



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB



نموذج كراسة الشروط والمواصفات (تقنية المعلومات)

المعتمد بموجب قرار وزير المالية رقم (1440) وتاريخ 1441/4/12هـ

اسم المنافسة: خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز الذكاء الاصطناعي NCAI-HPCCYB

رقم الكراسة:

تاريخ طرح الكراسة: 18/02/1446



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الفهرس

القسم الأول : مقدمة

- 1 تعريفات
- 2 تعريف عن المنافسة
- 3 قيمة وثائق المنافسة
- 4 المواعيد المتعلقة بالمنافسة
- 5 أهلية مقدمي العروض
- 6 السجلات والتراخيص النظامية
- 7 ممثل الجهة
- 8 مكان التسليم
- 9 نظام المنافسة

القسم الثاني : الأحكام العامة

- 10 المساواة والشفافية
- 11 تعارض المصالح
- 12 السلوكيات والأخلاقيات
- 13 السرية وإفشاء المعلومات
- 14 ملكية وثائق المنافسة
- 15 حقوق الملكية الفكرية
- 16 المحتوى المحلي
- 17 أنظمة وأحكام الاستيراد
- 18 تجزئة المنافسة
- 19 الإستهبعاد من المنافسة
- 20 إلغاء المنافسة وأثره
- 21 التفاوض مع أصحاب العروض
- 22 التضامن
- 23 التعاقد من الباطن
- 24 التأهيل اللاحق
- 25 عدم الالتزام بالتعاقد
- 26 الموافقة على الشروط



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز الذكاء الاصطناعي NCAI-HPCCYB

القسم الثالث : إعداد العروض**27 تأكيد المشاركة بالمنافسة****28 لغة العرض****29 العملة المعتمدة****30 صلاحية العروض****31 تكلفة إعداد العروض****32 الإخطارات والمراسلات****33 ضمان المعلومات****34 الأسئلة والاستفسارات****35 حصول المتنافسين على كافة المعلومات الضرورية****وزيارة موقع الأعمال****36 وثائق العرض الفني****37 وثائق العرض المالي****38 كتابة الأسعار****39 جدول الدفعات****40 الضرائب والرسوم****41 الأحكام العامة للضمانات****42 الضمان الابتدائي****43 مصادرة الضمانات****44 العروض البديلة****45 متطلبات تنسيق العروض****القسم الرابع : تسليم العروض****46 تقديم العروض****47 التسليم المتأخر****48 تمديد فترة تلقي العروض وتأجيل فتحه****49 الانسحاب****50 فتح العروض****القسم الخامس : تقييم العروض****51 سرية تقييم العروض****52 معايير تقييم العروض****53 تصحيح العروض****54 فحص العروض****55 الإعلان عن نتائج المنافسة****56 فترة التوقف****القسم السادس : متطلبات التعاقد****57 إخطار الترسية****58 الضمان النهائي****59 توقيع العقد**



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

القسم السابع : نطاق العمل المفصل

60 نطاق عمل المشروع

61 برنامج العمل

62 مكان تنفيذ الأعمال

63 جدول الكميات والأسعار

القسم الثامن : المواصفات

64 العمالة

65 المواد

66 المعدات

67 كيفية تنفيذ الأعمال والخدمات

68 مواصفات الجودة

69 مواصفات السلامة

القسم التاسع : متطلبات المحتوى المحلي

1 القائمة الإلزامية

2 اشتراطات المحتوى المحلي

القسم العاشر : الشروط الخاصة

القسم الحادي عشر : الملحقات



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

القسم الأول : المقدمة

1- تعريفات

المصطلح	التعريف
الجهة الحكومية	الهيئة السعودية للبيانات والذكاء الاصطناعي
المتنافس	مقدم العرض أو المشارك في المنافسة الراغب في تقديم العرض.
المنافسة	تشمل جميع إجراءات ووثائق طلب تقديم العروض من قبل الجهة ومقدمي العروض حتى الترسية.
النظام	نظام المنافسات والمشتريات الحكومية.
اللائحة التنفيذية	اللائحة التنفيذية لنظام المنافسات والمشتريات الحكومية.
المفردات والجمع	تدل الكلمات الواردة بصيغة المفرد على ذات المدلول بصيغة الجمع ويكون العكس صحيحاً أيضاً إذا تطلب النص ذلك.

2- تعريف عن المنافسة :

تعتبر المنافسة داعمة لقطاع التمكين الرقمي تتضمن متطلبات الهيئة السعودية للبيانات والذكاء الاصطناعي بالمملكة العربية السعودية لتسريع أعمال تطوير الذكاء الاصطناعي لمشاريع المركز الوطني للذكاء الاصطناعي المتعددة ودعم أصحاب المصلحة وتوفير الحوسبة اللازمة لتسهيل إنجاز الأعمال حسب جدول الكميات. يجب على مقدمي العروض الالتزام بتقديم أفضل وأحدث الحلول التقنية وفقاً لأعلى المعايير والمواصفات. كما ترغب الهيئة السعودية للبيانات والذكاء الاصطناعي بالتعاقد من مقاول في مسار الأمن السيبراني

3- قيمة وثائق المنافسة :

آلية الدفع	قيمة وثائق المنافسة
نظام سداد	خمسمائة ريال سعودي لا غير. 500.00

4- المواعيد المتعلقة بالمنافسة :

يتم اتباع كافة المواعيد المتعلقة بالمنافسة حسب الجدول أدناه. وفي حال تعطل البوابة لأسباب تقنية لمدة لا تزيد على ثلاث أيام متصلة فيتم تمديد مدة تنفيذ الإجراءات لمدة تماثل مدة تعطل البوابة وذلك على النحو المبين تفصيلاً بالبند ثالثاً من المادة الثامنة من اللائحة التنفيذية لنظام المنافسات والمشتريات الحكومية. وإن استمر العطل التقني لمدة تزيد على ثلاثة أيام وتعد على الجهة الحكومية أو المتنافس تنفيذ الإجراء بأي وسيلة بديلة. تعين تنفيذه بشكل ورقي، على أن ترفع الجهة ما تم عمله من إجراءات إلى البوابة فور زوال العطل.



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

المرحلة	تاريخ الاستحقاق
آخر موعد لإرسال الأسئلة والاستفسارات	22/03/1446
آخر تاريخ لتقديم العروض	29/03/1446 : 10:00 ص
تاريخ فتح العروض	29/03/1446 : 10:00 ص
الترسية	27/03/1446
بدء الاعمال	22/05/1446
مدة العقد	3 سنة

5- أهلية مقدمي العروض :

لا تحق المشاركة في المنافسة للأشخاص المشار إليهم فيما يلي:

1. موظفو الدولة ويستثنى من ذلك ما يلي:
 1. الأعمال غير التجارية إذا رخص لهم بمزاوتها.
 2. بشراء مصنعاتهم أو أي من حقوق الملكية الفكرية، سواء منهم مباشرة أو من خلال دور النشر أو غيرها.
 3. تكليفهم بأعمال فنية.
 4. الدخول في المزايدات العلنية، إذا كانت الأشياء المرغوب في شرائها لاستعمالهم الخاص.
2. من تقضي الأنظمة بمنع التعامل معهم بما في ذلك من صدر بمنع التعامل معهم حكم قضائي أو قرار من جهة مخولة بذلك نظاماً، وذلك حتى تنتهي مدة المنع.
3. المفلسون أو المتعثرون وفقاً لأحكام نظام الإفلاس، أو من ثبت إعسارهم، أو صدر أمر بوضعهم تحت الحراسة القضائية.
4. الشركات التي جرى حلها أو تصفيتها.
5. من لم يبلغ من العمر (ثمانية عشر) عاماً.
6. ناقصو الأهلية.

6- السجلات والتراخيص النظامية :

يجب أن تتوفر لدى المتنافسين وتعاقدتهم من الباطن الوثائق التالية وأن تكون هذه الوثائق سارية المفعول:

- السجل التجاري
- تصنيف المقاولين
- شهادة الزكاة
- شهادة الضريبة
- التأمينات الاجتماعية
- شهادة اشتراك الغرفة التجارية
- رخصة الاستثمار
- شهادة السعودية
- رخصة البلدية

7- ممثل الجهة :

يتم التواصل مع ممثل الجهة الحكومية المذكور أدناه في حال تعذر استخدام البوابة الإلكترونية أو الوسيلة البديلة.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

معلومات اتصال ممثل الجهة

الإسم	أخصائي منافسات
الوظيفة	أخصائي منافسات
الهاتف	0598131621
الفاكس	0598131621
البريد الإلكتروني	procurement@sdaia.gov.sa

8- مكان التسليم :

يتم تسليم العروض وجميع ما يتعلق بالمنافسة لممثل الجهة الحكومية في العنوان المذكور أدناه في حال تعذر تسليم العروض من خلال البوابة الإلكترونية أو الوسيلة البديلة.

مكان تسليم العروض

العنوان	الهيئة السعودية للبيانات والذكاء الاصطناعي
المبنى	مكتب إدارة البيانات الوطنية - سدايا
الطابق	الارضي
الغرفة / اسم الإدارة	الخدمات المشتركة لجنة فتح العروض
وقت التسليم	01:00 24/12/1445 م

9- نظام المنافسة :

تخضع هذه المنافسة لنظام المنافسات والمشتريات الحكومية ولائحته التنفيذية ولائحة تفضيل المحتوى المحلي والمنشآت الصغيرة والمتوسطة والشركات المدرجة بالسوق المالية في حال إصدارها من قبل مجلس الوزراء، ولائحة تنظيم تعارض المصالح، ولائحة سلوكيات وأخلاقيات القائمين على تطبيق النظام، في حال إصدارها من قبل مجلس الوزراء.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز الذكاء الاصطناعي NCAI-HPCCYB

القسم الثاني: الأحكام العامة

10- المساواة والشفافية

على الجهة الحكومية اطلاع كافة المتنافسين على المعلومات ذات العلاقة بنطاق العمل في المنافسة بما يمكنهم من تقييم الأعمال قبل الحصول على وثائق المنافسة، وتقديم الإيضاحات والبيانات اللازمة عن الأعمال والمشتريات المطلوب تنفيذها قبل ميعاد تقديم العروض بوقتٍ كافٍ وتلتزم الجهة بعدم التمييز بين المتنافسين في أي مما سبق. كما سيتم إخطار كافة المتقدمين للمنافسة بأي تغييرات تطرأ على المنافسة عبر البوابة الإلكترونية أو الوسيلة البديلة. وإن تعذر ذلك فعن طريق البريد الرسمي أو البريد الإلكتروني على النحو المبين بأحكام النظام واللائحة التنفيذية.

11- تعارض المصالح

يلتزم المتنافس والعاملون لديه والشركات التابعة له ومقاولوه من الباطن، وكل من له علاقة مباشرة أو غير مباشرة بتنفيذ وتأمين الأعمال والمشتريات المضمنة في نطاق هذه المنافسة، بإبلاغ الجهة الحكومية والإفصاح كتابة عن أي حالة تعارض ف المصالح أو أي مصلحة خاصة نشأت أو ستنشأ أو قد تنشأ عن أي تعامل يكون مرتبطاً بأنشطة الجهة الحكومية، وذلك وفق اللائحة تنظيم تعارض المصالح

12- السلوكيات والأخلاقيات

يحظر على المتنافس والعاملين لديه والشركات التابعة له ومقاوليه من الباطن، وكل من له علاقة مباشرة أو غير مباشرة بتنفيذ وتأمين الأعمال والخدمات التي تتضمنها هذه المنافسة، مخالفة الأحكام الواردة في لائحة تنظيم سلوكيات وأخلاقيات القائمين على تطبيق نظام المنافسات والمشتريات الحكومية وقواعد السلوك المهني وقواعد أخلاقيات المهنة وغيرها من القواعد التي نصت عليها الأنظمة المعمول بها أو المفروضة عليهم بموجب عضويتهم في أي منظمة مهنية أو هيئة ذات علاقة وفي الأحوال يلتزم بعدم الحصول أو محاولة الحصول على ميزة غير مستحقة بأي طريقة كانت أو تقديم أي هدية أو أي منفعة سواء مادية أو معنوية للحصول على معاملة تفضيلية من موظفي الجهة الحكومية في كافة مراحل تنفيذ المنافسة أو أي عقد ينتج عنها

13- السرية وإفشاء المعلومات

يلتزم المتنافسون بعدم إفشاء أي بيانات أو رسومات أو وثائق أو معلومات تتعلق بالمنافسة سواء كانت تحريرية أو شفوية أو استغلالها أو الإفصاح عنها. ويسري ذلك على كل ما بحوزته أو ما يكون قد اطلع عليه في العرض من أسرار وتعاملات أو شؤون تخص الجهة الحكومية، كما لا يجوز للمتنافسين نشر أي معلومة عن المنافسة وكل ما يتعلق بها عبر كافة وسائل الإعلام إلا بعد أخذ موافقة كتابية من الجهة الحكومية مسبقاً.

14- ملكية وثائق المنافسة

أولاً: تعود ملكية وثائق المنافسة وجميع نسخها للجهة الحكومية ويجب على المتنافسين إتلاف تلك الوثائق وجميع نسخها عند طلب الجهة الحكومية ذلك. والجهة الحكومية غير ملزمة بإعادة وثائق العروض.

ثانياً: حقوق الطبع والنشر لأي وثائق ومواد مقدمة من الجهة الحكومية ضمن هذه المنافسة مملوكة للجهة، وعلى ذلك لا يجوز نسخ هذه الوثائق والمواد، كلياً أو جزئياً، أو إعادة إنتاجها أو توزيعها أو إتاحتها لأي طرف ثالث أو استخدامها دون الحصول على موافقة كتابية مسبقة من الجهة الحكومية. وتجب إعادة جميع الوثائق التي قدمتها الجهة الحكومية فيما يتعلق بطلب تقديم العروض عند الطلب، دون الاحتفاظ بأي نسخ من قبل مقدم العرض أو أي شخص آخر.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

15- حقوق الملكية الفكرية

تعود حقوق الملكية الفكرية لجميع الوثائق والمواد والتقارير المقدمة من المتنافسين ضمن هذه المنافسة للجهة، كما يحل للجهة استعمالها بما تراه مناسباً لتحقيق المصلحة العامة.

16- المحتوى المحلي

يجب على المتنافسين الالتزام بلائحة تفضيل المحتوى المحلي والمنشآت الصغيرة والمتوسطة. والشركات المدرجة في السجل المالية الصادرة بقرار مجلس الوزراء رقم (245) وتاريخ 29/03/1441هـ

17- أنظمة وأحكام الإستيراد

يقر المتنافسون بأن أنظمة وأحكام الاستيراد والجمارك في المملكة العربية السعودية هي التي يتم تطبيقها على توريد وشحن أمنتجات أو أجزاء من أو إلى المملكة.

18- تجزئة المنافسة

المنافسة لا تتضمن تجزئة

19- الإستبعاد من المنافسة

حق للجهة استبعاد أي عرض اجتاز التقييم الفني بسبب تدني أسعاره بنسبة (25%) خمسة وعشرين بالمائة فأكثر عن التكلفة التقديرية والأسعار السائدة في السوق وذلك بعد أن تقوم لجنة فحص العروض بمراجعة الأسعار التقديرية ومناقشة صاحب العرض المنخفض وعدم اقتناعها بمقدرته على تنفيذ العقد بعد الطلب منه كتابياً تقديم تفاصيل للعناصر المكونة لعرضه وشرح أسباب انخفاضها.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

20- إلغاء المنافسة وأثره**أولاً:** للجهة الحق في إلغاء المنافسة قبل الترسية في الحالات الآتية:

1. وجود أخطاء جوهرية في وثائق المنافسة.
2. مخالفة إجراءات المنافسة لأحكام النظام واللائحة.
3. إذا اقتضت المصلحة العامة إلغاء المنافسة.
4. ارتكاب أي من المخالفات الواردة في الفقرة (3) من المادة (الحادية والخمسين) من النظام.
5. إذا لم تتمكن الجهة الحكومية من تخفيض أسعار العروض التي تتخطى أسعار السوق السائدة بشكل ظاهر أو تتجاوز المبالغ المعتمدة من خلال التفاوض.
6. ارتفاع أسعار العروض عن المبالغ المعتمدة.

ثانياً: تعاد قيمة وثائق المنافسة إلى أصحاب العروض إذا تم إلغاء المنافسة، في الحالات التالية

1. وجود أخطاء جوهرية في وثائق المنافسة.
2. مخالفة إجراءات المنافسة لأحكام النظام أو اللائحة.
3. إذا اقتضت المصلحة العامة إلغاء المنافسة.
4. ارتكاب أي من المخالفات، الواردة في الفقرة (3) من المادة (الحادية والخمسين) من النظام، وذلك لمن لا علاقة له بتلك المخالفات المتنافسين.
5. ارتفاع أسعار العروض عن المبالغ المعتمدة.

ولا تعاد قيمة وثائق المنافسة إذا كان الإلغاء بعد فتح المظاريف إلا لمن تقدم بعرضه للمنافسة. وفي حال تم تمديد تلقي العروض للمرة الثانية، وأبدى المشتري عدم رغبته في الاستمرار في المنافسة تعاد له قيمة وثائق المنافسة.

21- التفاوض مع أصحاب العروض**أولاً:** يحق للجهة التفاوض في حال ارتفاع أسعار العروض عن الأسعار السائدة في السوق بشكل ظاهر مع مراعاة ما يلي:

1. يحدد السعر المناسب بما يتفق مع الأسعار السائدة في السوق.
2. تتم الكتابة لصاحب العرض الفائز، بطلب تخفيض عرضه للسعر المحدد. وفي حال رفضه فإنه يتم الانتقال للعرض الذي يليه في الترتيب وهكذا.
3. تتم الترسية على صاحب العرض الذي يصل سعره إلى المبلغ المحدد أو المطلوب.
4. إذا لم يتم الوصول إلى السعر المحدد من قبل لجنة فحص العروض، يكون إلغاء المنافسة بتوصية من لجنة فحص العروض إلى صاحب الصلاحية بالإلغاء؛ والذي يتوجب عليه في تلك الحالة إلغائها.

ثانياً: يحق للجهة التفاوض في حال ارتفاع أسعار العروض عن المبالغ المعتمدة باتباع المرحلتين التاليين

1. يتم التفاوض بتخفيض الأسعار وفقاً لما ورد في الفقرة الأولى من هذه المادة.
2. في حال عدم قبول المتنافسين تخفيض أسعارهم يتم إلغاء أو تخفيض بعض البنود، بشرط ألا يؤثر ذلك على مراكز المتنافسين، وعلى الانتفاع من المشروع، وفي حال عدم الوصول للسعر المناسب، تلغى المنافسة.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

22- التضامن

يجوز للمتنافسين التضامن فيما بينهم لتقديم العروض على أن تتوافر الشروط الآتية:

1. أن يتم التضامن قبل تقديم العرض بموجب اتفاقية تضامن مبرمة بين المتنافسين ومصدقة من الغرفة التجارية ومن الجهات المخولة بالتوثيق
2. أن يحدد في الاتفاقية قائد التضامن كممثل قانوني أمام الجهة الحكومية لاستكمال إجراءات التعاقد وتوقيع العقد، ولأغراض المراسلات والمخاطبات.
3. أن يوضح في الاتفاقية الأعمال التي سيقوم بها كل طرف من أطراف التضامن.
4. أن تنص الاتفاقية على التزام ومسؤولية المتضامين مجتمعين أو منفردين عن تنفيذ كافة الأعمال المطروحة في المنافسة.
5. أن يُختم العرض وجميع وثائقه ومستنداته من جميع أطراف التضامن.
6. أن تقدم اتفاقية التضامن مع العرض وجميع وثائقه ومستنداته.
7. لا يجوز لأي طرف من أطراف التضامن التقدم للمنافسة بعرض منفرد أو التضامن مع منافس آخر.
8. لا يجوز تعديل اتفاقية التضامن بعد تقديمها إلا بموافقة الجهة الحكومية.

23- التعاقد من الباطن

مع مراعاة ما ورد في المادة (الحادية والسبعين) من النظام، يشترط في التعاقد من الباطن ما يلي:

- أ. أن يقدم المتنافس مع عرضه قائمة بأسماء المتعاقدين من الباطن لاعتمادهم من قبل الجهة الحكومية.
- ب. يجب أن تشمل العروض التي تتضمن متعاقدين من الباطن على الكميات الموكلة لهم واسعارهم وفقاً لمتطلبات وشروط ومواصفات الكراسة والعقد المرفق.
- ج. ألا يكون المتعاقد من الباطن من الأشخاص المشار إليهم في الفقرة (5) من هذه الكراسة، وأن يكون مرخصاً في الأعمال المتعاقد على تنفيذها من قبل المتعاقد الرئيس، أو أن يكون لديه مؤهلات كافية لتنفيذ الأعمال، ومصنفاً في المجال وبالدرجة المطلوبة إذا كانت الأعمال مما يشترط لها التصنيف، وأن يكون لديه المؤهلات والقدرات الكافية لتنفيذ تلك الأعمال.
- د. ألا تزيد نسبة الأعمال المسندة إلى المتعاقد من الباطن على (30 %) من قيمة العقد.
- هـ. يلتزم المتعاقد مع الجهة الحكومية بإعطاء الأولوية للمنتجات الوطنية -غير المدرجة ضمن القائمة الإلزامية- عند شراء ما يحتاجه من مواد أو أدوات وذلك باعتبار سعر المنتجات الأجنبية أعلى بنسبة 10 % من سعرها الأساسي ومقارنتها بسعر المنتج الوطني، كما يلتزم المتعاقد بذلك في عقود مع متعاقديه من الباطن. وفي حال عدم التزام المتعاقد مع الجهة الحكومية -أو مقاوليه من الباطن- ستوقع الجهة الحكومية غرامة مالية مقدارها 30% من قيمة المشتريات محل التقصير.
- و. يكون المتعاقد الرئيس مسؤولاً أمام الجهة الحكومية عن الأعمال المتعاقد على تنفيذها بعقود الباطن وفقاً للشروط والمواصفات.
- ز. لا يجوز للمتعاقد من الباطن القيام بالتعاقد مع أي متعاقد آخر من الباطن لتنفيذ الأعمال المتعاقد معه على تنفيذها.
- ح. يجب أن يقدم المتعاقد الرئيس اقراراً منه يسمح للجهة الحكومية أن تتولى صرف حقوق متعاقدي الباطن من مستحقات المتعاقد الرئيسي، في حال عدم قيامه أو تأخره بصرف حقوقهم عن الأجزاء التي قاموا بتنفيذها.
- ط. يجوز أن يتم التعاقد من الباطن لتنفيذ أعمال تزيد عن (30%) من قيمة العقد وتقل عن (50%) من قيمة العقد بشرط الحصول على موافقة مسبقة من هيئة كفاءة الإنفاق والمشروعات الحكومية وأن يتم اسناد تلك الأعمال إلى أكثر من متعاقد من الباطن يتم تأهيلهم لهذا الغرض.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

24- التأهيل اللاحق

أولاً: يجب على الجهة الحكومية إجراء تأهيل للاحق لصاحب العرض الفائز في الحالات التي لا يتم فيها إجراء تأهيل مسبق.

ثانياً: مع مراعاة ما ورد في المادة (العشرين) من النظام، والمادة (السادسة عشرة) من هذه اللائحة، على الجهة الحكومية إجراء تأهيل للاحق لصاحب العرض الفائز في المنافسة الذي سبق تأهيله تأهيلاً مسبقاً، متى كانت المدة بين إجراء التأهيل المسبق والترسية تزيد على (سنة)؛ وذلك للتأكد من استمرار مؤهلاته.

ثالثاً: عند عدم اجتياز صاحب العرض الفائز لمرحلة التأهيل اللاحق فيتم الانتقال لصاحب العرض الذي يليه في الترتيب وهكذا وتلغى المنافسة إذا لم يجتزه جميع المتنافسين.

رابعاً: يجب على الجهة الحكومية في حال إجرائها تأهيل للاحق للمتنافس الفائز أن تستخدم ذات المعايير التي تم استخدامها في مرحلة التأهيل المسبق.

خامساً: في حال قامت الجهة الحكومية بتأهيل سابق لمتنافس فيجوز لها عدم القيام بتأهيل ذلك المتنافس في الأعما والمشتريات المشابهة شريطة ألا يكون قد مضى أكثر من عام على التأهيل السابق

25- عدم الالتزام بالتعاقد

لا يجوز تفسير طلب تقديم العروض والاشتراك في هذه المنافسة وتقديم العروض بأي شكل من الأشكال على أنه التزام تعاقدى أو قانوني من طرف الجهة الحكومية طالبة العروض.

26- الموافقة على الشروط

يعتبر المتنافس موافقاً لكافة شروط ومواصفات وأحكام المنافسة من خلال مشاركته في عملية تقديم العروض. ويستتبع العرض المخالف لذلك إلا في الحالات التي تكون المخالفة شكلية وغير مؤثرة.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز الذكاء الاصطناعي NCAI-HPCCYB

القسم الثالث : إعداد العروض**27- تأكيد المشاركة بالمنافسة**

على المتنافسين الراغبين في المشاركة في هذه المنافسة إخطار الجهة الحكومية لتأكيد عدم وجود أي تعارض في المصالح وينتهم بتسليم العرض في المواعيد المحددة.

28- لغة العرض

يجب أن تقدم العروض باللغة العربية مع إمكانية تقديم بعض الوثائق أو جزء من العرض باللغة الإنجليزية، أو تقديم الوثائق الداعمة للعرض بإحدى اللغات الأجنبية عند الحاجة مع تقديم ترجمة لتلك الوثائق. مع العلم بأنه في حال وجد تعارض بين النص العربي والنص الإنجليزي للعروض فإنه يؤخذ بالنص الوارد باللغة العربية.

29- العملة المعتمدة

تعتبر العملة السعودية (الريال السعودي) العملة المعتمدة بكافة التعاملات المتعلقة بالمنافسة ما لم ينص في الشروط الخاصة على عملة أخرى. ويتم الصرف طبقاً للأنظمة واللوائح المالية المتبعة في نظام المنافسات والمشتريات الحكومية.

30- صلاحية العروض

يجب أن تكون مدة سريان العروض في هذه المنافسة (90) تسعون يوماً من التاريخ المحدد لتسليم العروض.

31- تكلفة إعداد العروض

يتحمل المتنافسين جميع التكاليف المرتبطة بالمنافسة، ولا تتحمل الجهة الحكومية أي مسؤولية لتغطية تكاليف المتنافسين في إعداد العروض، والتي تتضمن تلك التكاليف التي يتكبدها المتنافسين للقيام بالعناية الواجبة، والتكاليف المتعلقة بتقديم معلومات إضافية للجهة، بالإضافة إلى التكاليف المرتبطة بأي مفاوضات مع الجهة الحكومية. كما يجب على المتنافسين إمداد الجهة الحكومية بأي توضيحات مطلوبة طوال مدة المنافسة، دون إلزام الجهة الحكومية بتغطية التكاليف المرتبطة بذلك.

32- الإخطارات والمراسلات

تعد البوابة الإلكترونية أو الوسيلة البديلة هي الوسيلة المعتمدة لكافة الإخطارات والمراسلات المتعلقة بالمنافسة، وفي حال تعذر ذلك فيتم التواصل مع ممثل الجهة الحكومية المذكور في الفقرة 7 من هذه الكراسة.

33- ضمان المعلومات

تعتبر كافة المعلومات المقدمة في هذه الكراسة إرشادية فقط، ويقع على عاتق مقدم العرض وحده مسؤولية القيام بإجراءات لازمة للتحقق من دقة المعلومات المقدمة أو المستلمة فيما يتعلق بالمنافسة أو غير ذلك. كما يجب على المتنافسين أن يكونوا على دراية بجميع الأنظمة واللوائح والقرارات ذات العلاقة بنطاق عمل المنافسة وأخذها بعين الاعتبار عند تحديد الأسعار.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

34- الأسئلة والاستفسارات

يمكن للمتنافسين في حال وجود أي استفسارات عن المنافسة، أن يرسلوا استفساراتهم عن طريق البوابة الإلكترونية الوسيلة البديلة خلال (33) ثلاثة و ثلاثون يوماً من تاريخ طرح المنافسة. وتلتزم الجهة الحكومية بالرد على استفسارات المتنافسين عن طريق البوابة الإلكترونية أو الوسيلة البديلة خلال مدة لا تتجاوز (7) سبعة أيام من ذلك التاريخ، وفي حال تعذر ذلك فعلى الجهة الحكومية الرد عن طريق contracts@nic.gov.sa. وعلى الجهة الحكومية جمع كافة الاستفسارات المقدمة من المتنافسين والإجابة عليها ومشاركتها مع جميع المتنافسين دون الكشف عن هوية المتنافس مقدم الاستفسار عن طريق البوابة الإلكترونية أو الوسيلة البديلة. كما يمكن للجهة الحكومية تنظيم ورشة عمل لمناقشة كافة الاستفسارات المقدمة والإجابة عليها.

35- حصول المتنافسين على كافة المعلومات الضرورية وزيارة موقع الأعمال

على صاحب العرض المتقدم لتنفيذ الأعمال والمشتريات أن يتحرى قبل تقديم عرضه، عن طبيعة الأعمال المتقدم لها، والظروف المصاحبة للتنفيذ، ومعرفة بياناتها وتفصيلاتها على وجه الدقة، وما يمكن أن يؤثر في فئات عرضه ومخاطر التزاماته، وعليه بشك عام أن يسعى للحصول على كافة المعلومات الضرورية واللازمة لتنفيذ عطاءه وأن يقوم بفحص موقع الأعمال ومعاينته وكذلك الأماكن المحيطة به.

36- وثائق العرض الفني

يشمل العرض الفني المتطلبات التالية:

1. الخبرات السابقة
2. فريق العمل
3. تقديم عرض فني يشمل نطاق العمل وجدول الكميات المفصل مع تقديم المدة المستغرقة للتنفيذ
4. تقديم كامل الملفات التقنية لهيكلية الخدمة وطرق استخدامها
5. تقديم نموذج اتفاقية مستوى الخدمة للخدمات البنية التحتية كخدمة وخدمات برامج العمل
6. جدول مصفوفة الامتثال بنطاق العمل وجدول الكميات.
7. خطة المخاطر.
8. خطة التواصل.
9. السير الذاتية لفريق العمل

37- وثائق العرض المالي

يشمل العرض المالي المتطلبات التالية:

1. تسعير كامل كميات الجدول المدرج في منصة اعتماد.
2. الالتزام بالمدة المطلوبة في كراسة الشروط والمواصفات والنص عليها في خطاب التغطية.
3. ان تكون الأسعار المقدمة في منصة اعتماد متطابقة مع الأسعار المقدمة في عرض الشركة الورقي.
4. ان يكون العرض المالي الورقي مقدم باللغة العربية.
5. الالتزام بتسعير الكميات المطلوبة وعدم تقديم حلول بديلة للكميات المطلوبة.
6. عدم تقديم جدول دفعات مقترح من الشركات وفي حال تقديم جدول دفعات مقترح فلن يعتد به.
7. العرض المالي الورقي لابد من إيضاح ان المبالغ المقدمة شاملة قيمة الضريبة المضافة 15%.
8. يجب ان يكون اجمالي قيمة كل بند على حدة شامل قيمة الضريبة المضافة 15% في العرض المالي الورقي.
9. جدول الكميات شاملا الأسعار وجميع الضرائب والرسوم.
10. الضمان الابتدائي .



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

38- كتابة الأسعار

1. يجب على المتنافس تقديم سعره وفقاً للشروط والمواصفات، وجداول الكميات المعتمدة وألا يقوم بإجراء أي تعديل أو إبداء أي تحفظ عليها، كما يجب ألا يقوم بشطب أي بند من بنود المنافسة أو مواصفاتها، حيث أنه سيتم استبعاد العرض المخالف لذلك.
2. تدوين أسعار العرض الإفرادية والإجمالية في جداول الكميات رقماً وكتابة بالعملة المحلية، ما لم ينص على تقديمها بعملة أخرى.
3. لا يجوز لمقدم العرض التعديل أو المحو أو الطمس على قائمة الأسعار، ويجب إعادة تدوين أي تصحيح يجريه صاحب العرض عليها رقماً وكتابة والتوقيع عليه وختمه.
4. يجوز استبعاد العرض إذا بلغت فئات الأسعار التي جرى عليها التعديل أو المحو أو الطمس أكثر من (10%) من قائمة الأسعار، أو من القيمة الإجمالية للعرض.
5. لا يجوز لمقدم العرض ترك أي بند من بنود المنافسة دون تسعير إلا إذا أجازت شروط المنافسة ذلك.

39- جدول الدفعات

يقدم المتنافس جدولاً للدفعات يحدد فيه قيمة الدفعات المطلوبة ونسبتها من قيمة العرض ومرحلة استحقاقها. ويجوز للجهة الحكومية مراجعة جدول الدفعات وتعديله وفق ما تراه متوافقاً مع جدول المشروع.

40- الضرائب والرسوم

يجب أن تشمل جميع الأسعار المقدمة من قبل المتنافس كافة التكاليف من ضرائب ورسوم وغيرها من المصاريف، ولا تتحمل الجهة الحكومية أي مصاريف إضافية لم يتم ذكرها في عرض الأسعار.

41- الأحكام العامة للضمانات

يجب على المتنافس عند تقديم الضمانات مراعاة الشروط التالية:

1. يجوز أن يقدم الضمان من بنوك عدة، على أن يلتزم بموجبه كل بنك بأداء نسبة محددة من قيمة الضمان تكون محددة في خطاب الضمان المقدم من كل بنك بما يتساوى في قيمه المجتمعة بالضمان المطلوب كحد أدنى.
2. إذا قُدم الضمان من بنك أجنبي بوساطة أحد البنوك المحلية، يجب على البنك المحلي الالتزام بشروط وقواعد الضمانات البنكية المحددة في النظام واللائحة.
3. يكون الضمان واجب ومستحق الدفع عند أول طلب من جانب الجهة الحكومية، دون حاجة إلى حكم قضائي أو قرار من هيئة تحكيم.
4. يجب أن يكون الضمان غير مشروط، وغير قابل للإلغاء، وتكون قيمته خالية من أية حسومات تتعلق بالضرائب، أو الرسوم، أو النفقات الأخرى.
5. يجوز استبدال الضمانات البنكية من بنك لآخر، على ألا يفرج عن الضمان إلا بعد الحصول على الضمان البديل.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

42- الضمان الابتدائي

أولاً: على المتنافس تقديم الضمان الابتدائي بنسبة (1.00%) واحد بالمائة من القيمة الإجمالية للعرض مع مراعاة الأحكام العامة للضمانات أعلاه ووفقاً للشروط التالية:

- لا يجوز قبول العرض الذي يقدم بدون ضمان ابتدائي، ويجب على الجهة الحكومية قبول الضمان الناقص متى كانت نسبة النقص لا تتجاوز (10%) من قيمة الضمان المطلوب، وفي هذه الحالة، على لجنة فحص العروض- قبل التوصية بالترسية على مقدم الضمان الناقص- أن تطلب منه استكمال النقص في الضمان خلال مدة تحددها اللجنة لا تزيد عن (عشرة) أيام عمل، وإلا عُـد منسحباً ولا يعاد إليه الضمان الابتدائي.
- يُقدم أصل خطاب الضمان الابتدائي مع العرض، على أن يكون الضمان الابتدائي ساري المفعول مدة لا تقل عن (90) تسعين يوماً من التاريخ المحدد لفتح العروض، وفي حال كان الضمان ناقص المدة بما لا يتجاوز (ثلاثين) يوماً، تعين على لجنة فحص العروض- قبل التوصية بالترسية على مقدم الضمان الناقص- أن تطلب منه استكمال النقص في الضمان خلال مدة تحددها لجنة فحص العروض، وإلا يعد منسحباً ولا يعاد إليه الضمان الابتدائي، ولا يعد اليوم واليومين نقصاً في مدة الضمان.
- تقوم الجهة الحكومية بطلب تمديد الضمان الابتدائي لمن رست عليه الأعمال متى كان تاريخ انتهاء سريانه قبل تقديم الضمان النهائي.
- ترد الضمانات الابتدائية إلى أصحاب العروض التي لم يتم الترسية عليها بعد البت في الترسية، وكذلك في حال إلغاء المنافسة، أو بعد انتهاء الوقت المحدد لسريان العروض ما لم يبد صاحب العرض رغبته في الاستمرار في الارتباط بعرضه وفقاً لأحكام النظام واللائحة التنفيذية.
- وبخلاف ما ورد أعلاه وفيما لم يرد فيه نص يقتضي مصادرة الضمان الابتدائي، ترد الضمانات الابتدائية لأصحابها ويجوز للجهة الحكومية بناءً على تقديرها أو بطلب من أصحاب العروض الإفراج عن ضماناتهم الابتدائية قبل البت في الترسية، إذ تبين بعد فتح المظاريف وانكشاف الأسعار أن أسعار تلك العروض مرتفعة، أو مخالفة للشروط والمواصفات، بما يحول دون الترسية على أي منها.
- في حال تقديم العرض في ملفين إلكترونيين، يقدم الضمان الابتدائي في ملف العرض المالي.

ثانياً: يستثنى من تقديم الضمان الابتدائي وفقاً للحالات التالية :

- الشراء المباشر
- المسابقة
- تعاققات الجهات الحكومية فيما بينها، بشرط أن تنفذ الأعمال وتؤمن المشتريات بنفسها.
- التعاقد مع مؤسسة أو جمعية أهلية أو كيان غير هادف إلى الربح، بشرط أن تتولى بنفسها القيام بما تم التعاقد عليه.
- التعاقد مع المنشآت الصغيرة والمتوسطة المحلية
- الأعمال والمشتريات التي تنفذ خارج المملكة العربية السعودية.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

43- مصادرة الضمانات

أولاً على الجهة الحكومية عند توافر أسباب مصادرة الضمان البنكي، العرض على لجنة فحص العروض أو لجنة فحص عروض الشراء المباشر بحسب الحال؛ لدراسة الحالة وتقديم توصية مسببة إلى صاحب الصلاحية في الترسية. مع الأخذ في الاعتبار الآثار المترتبة على المصادرة ومدة سريان الضمان. ويجوز للجهة طلب تمديد الضمان مدة معقولة إذا كانت إجراءات اتخاذ قرار المصادرة تتطلب ذلك.

ثانياً : لا يجوز مصادرة الضمان إلا للأسباب التي تم تقديم الضمان لأجلها، ويكون طلب المصادرة مقتصرًا على الضمان الخاص بالعملية التي أخل المتعاقد فيها بالتزاماته، ولا يمتد إلى مصادرة الضمانات الخاصة بالعمليات الأخرى سواء كانت لدى جهة واحدة أو عدة جهات

ثالثاً : عند مصادرة الضمان الابتدائي في المنافسات المجزأة، تقتصر المصادرة على جزء من قيمة الضمان منسوبة إلى قيمة الأعمال التي تمت ترسيته على المتعاقد

رابعاً : إذا قررت الجهة الحكومية مصادرة الضمان، فتطلب مصادرته من البنك مصدر الضمان مباشرة وباستخدام عبارة "مصادر الضمان" بشكل صريح، وعلى البنك الاستجابة لطلب المصادرة فوراً.

44- العروض البديلة

الجهة الحكومية لا تتيح تقديم العروض البديلة في المنافسة.

45- متطلبات تنسيق العروض

يجب ان يكون حجم الخط مقاس 11 وجميع الملفات بصيغة PDF



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

القسم الرابع : تسليم العروض

46- آلية تقديم العروض

يقوم المتنافس بتقديم عرضه في الموعد المحدد من خلال البوابة الإلكترونية. وفي حال تعطل البوابة الإلكترونية لمدة تزيد عن ثلاثة أيام فيجوز تقديم العروض بشكل ورقي لممثل الجهة في المكان المحدد. يتم تقديم العروض على النحو الآتي:

1. تقدم العروض بواسطة مظهرين أو ملفين فني ومالي ويجوز للجهة الحكومية اشتراط ذلك في الأعمال والمشتريات التي تقل قيمتها عن (خمسة ملايين) ريال، وفق ما تراه محققاً للمصلحة
2. يقدم العرض إلكترونياً بعد أن يدخل المتنافس البيانات المطلوبة عبر البوابة في ملف مشفر، أو ملفين مشفرين إذا تطلب الأمر تقديم عرضين فني ومالي .
3. ويجوز للمتنافس تقديم عرضه مكتوباً على أوراقه الخاصة، وتكون العبرة في حال الاختلاف بما وضعته الجهة الحكومية من شروط وأحكام في نماذجها المختومة.
4. يقدم العرض بموجب خطاب رسمي يوقع من مقدمه أو ممن يملك حق التمثيل النظامي
5. يقدم العرض -وكافة مرفقاته التي تتطلب ذلك- مختوماً بختم مقدمه.
6. تقدم مع العرض الوثائق المذكورة في الفقرة 37 و 38 من هذه الكراسة
7. في حال تعذر تقديم العروض من خلال البوابة الإلكترونية لأسباب فنية، يتم تقديمها في مظاريف مختومة بواسطة البريد الرسمي، أو تسليمها للجهة الحكومية في المكان المحدد لاستقبال العروض، مع أخذ إيصال يبين فيه تاريخ وساعة التسليم، وعلى الجهة الحكومية رفع العروض التي تقدم ورقياً على البوابة لحفظها في سجلاتها، وذلك بعد فتحها من قبل لجنة فتح العروض
8. تعلن أسماء المتنافسين الذين تقدموا بعروضهم في البوابة، وذلك بعد انتهاء موعد تقديم العروض وفتحها، فإذا تعذر إعلانها في البوابة، تعلن في الموقع الإلكتروني للجهة الحكومية.

47- التسليم المتأخر

لا يعتد بكافة العروض التي يتم تسليمها بعد انتهاء المدة المحددة لتقديم العروض.

48- تمديد فترة تلقي العروض وتأجيل فتحها

أولاً: إذا لم تتمكن الجهة الحكومية من البت في الترسية خلال مدة سريان العروض، تعد محضراً توضح فيه أسباب ومبررات التأخير في البت بالترسية، وتُشعر أصحاب العروض برغبتها في تمديد سريان عروضهم لمدة لا تزيد عن (تسعين) يوم أخرى.

ثانياً: على من يوافق من أصحاب العروض على التمديد، أن يمدد ضماناته وأن يبلغ الجهة الحكومية بذلك خلال (أسبوعين) من تاريخ الإشعار بطلب التمديد. ومن لم يتقدم خلال هذه المدة، عُد غير موافق على تمديد عرضه، ويعاد له ضمانه الابتدائي في هذه الحالة.

ثالثاً: إذا مضت المدد المشار إليها في هذه المادة، لا يجوز للجهة الحكومية تمديد سريان العروض إلا بعد موافقة الوزارة بناءً على أسباب مبررة، وإلا تلغ المنافسة.

49- الانسحاب

يجوز لصاحب العرض أن يسحب عرضه قبل انتهاء المدة المحددة لتلقي العروض، وعلى الجهة الحكومية أن ترد له ضمانه الابتدائي. أما إذا قرر الانسحاب بعد انتهاء المدة المحددة لتلقي العروض، فيصادر الضمان الابتدائي. وإذا كان صاحب العرض من المنشآت الصغيرة والمتوسطة، يتوجب عليه عند الانسحاب دفع غرامة مالية للجهة الحكومية تساوي قيمة الضمان الابتدائي وذلك إذا قام بسحب عرضه قبل انتهاء مدة سريان العروض. وفي حال مرور (60) ستين يوماً من تاريخ سحب عرضه دون أن يدفع الغرامة المالية المقررة، يعاقب بمنعه من التعامل مع الجهات الحكومية لمدة سنة من تاريخ استحقاق الغرامة.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

50- فتح العروض

مع مراعاة الأحكام الواردة في المادة (الرابعة والأربعين) من النظام، تلتزم لجنة فتح العروض بالآتي:

أولاً: أن تفتح العروض في الساعة واليوم المحددين لذلك، ويجب أن يكون فتح العروض في موعد انتهاء مدة تلقي العروض. وفي العروض التي تتضمن ملفين إلكترونيين، تفتح اللجنة الملف الفني فقط بحضور من يرغب من أصحاب العروض.

ثانياً: في حال تقديم العرض في ملفين إلكترونيين، تحال العروض الفنية بعد فتحها، والعروض المالية قبل فتحها، ومحضر اللجنة إلى لجنة فحص العروض.

ثالثاً: إذا لم تتمكن لجنة فتح العروض من القيام بعملها لأسباب مبررة، يؤجل موعد فتح العروض المدة اللازمة والضرورية ويحدد له موعد آخر يُبلغ به المتقدمون للمنافسة. ولا يجوز في هذه الحالة قبول عروض جديدة أثناء فترة التأجيل.

رابعاً: في حال تقديم العرض في ملف إلكتروني واحد فتعلن لجنة فتح العروض اسم مقدم العرض وسعره الإجمالي وما ورد عليه من زيادة أو تخفيض في خطاب العرض الأصلي وكذلك ما إذا قدم جميع الوثائق المطلوبة والضمان الابتدائي وقيمتها، وفي حال تقديم العرض في ملفين إلكترونيين فتعلن لجنة فتح العروض اسم مقدم العرض فقط.

خامساً: لا يجوز للجنة فتح العروض أن تستبعد أي عرض أو أن تطلب من أصحاب العروض تصحيح الأخطاء أو تلافي الملاحظات الواردة في عروضهم، كما لا يجوز لها استلام أي عروض أو مظاريف أو خطابات أو عينات يقدمها لها أصحاب العروض أثناء جلسة فتح العروض.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

القسم الخامس : تقييم العروض

51- سرية تقييم العروض

تلتزم الجهة الحكومية بعدم إفشاء أي بيانات أو رسومات أو وثائق أو معلومات تتعلق بتقييم العروض المستلمة، سواءً كان تحريرياً أو شفوياً، أو استغلالها أو الإفصاح عنها إلى أي شخص كان، ويسري ذلك على كل ما بحوزتها أو ما يكون قد اطلع عليه في العروض من أسرار وتعاملات وصفقات أو شؤون تخص المتنافسين.

52- معايير تقييم العروض

تتم الترسية على العرض ذو التكلفة /السعر الأفضل من العروض التي اجتازت التقييم الفني للجهة الحكومية. يلتزم المتنافسون بتقديم نسبة المحتوى المحلي المستهدفة لاجتياز التقييم الفني، وفي حال عدم تقديم نسبة المحتوى المحلي المستهدفة، فيتم استبعاد المتنافس من المنافسة. يقيم العرض -المجتاز للتقييم الفني- بحيث يكون وزن العرض المالي عند التقييم بنسبة (60%) (وزن السعر)، وتكون أوزان كل من خط الأساس ونسبة المحتوى المحلي المستهدفة وكون الشركة مدرجة في السوق المالي عند التقييم بنسبة (40%)، ويكون التقييم وفقاً للمعادلة التالية: نتيجة التقييم المالي = (سعر أقل عرض متأهل فنياً (بالريال) سعر العرض للمتنافس المراد تقييمه (بالريال)) $\times 60\% +$ (نسبة المحتوى المحلي المستهدفة $\times 50\% +$ خط الأساس $\times 50\%$ $\times 5\%$ نقاط للشركة المدرجة) $\times 40\%$. تتم الترسية على المتنافس الحاصل على أعلى تقييم، على ألا يتجاوز الفارق نسبة (10%) بين السعر الوارد في عرض المتنافس الحاصل على أعلى تقييم نهائي وبين أقل سعر وارد في عرض أي من المتنافسين المؤهليين، وفي حال تجاوز الفارق في السعر هذه النسبة فيتم الانتقال للمتنافس الذي يليه في التقييم.

53- تصحيح العروض

أولاً: على لجنة فحص العروض مراجعة جداول الكميات والأسعار الواردة في العرض -سواء في مفرداتها أو مجموعها- وإجراء التصحيحات الحسابية اللازمة في العرض.

ثانياً: إذا وجد اختلاف بين السعر المبين كتابةً والسعر المبين بالأرقام، يؤخذ بالسعر المبين كتابةً. وإذا وجد اختلاف بين سعر الوحدة وسعر مجموعها، فيؤخذ بسعر الوحدة.

ثالثاً: إذا وجدت دلائل تؤكد عدم صحة السعر وفقاً لأسلوب التصحيح الوارد في الفقرة (2) من هذه المادة، فيحق للجنة فحص العروض -بعد التأكد من التوازن المالي لأسعار البنود ومقارنة السعر مع أمثاله في العروض والعروض الأخرى وسعر السوق والأسعار التقديرية- الأخذ بالسعر الوارد في العرض الذي يثبت لها صحته، ويستبعد المتنافس عند رفضه لهذا السعر.

رابعاً: يجوز للجنة فحص العروض التوصية باستبعاد العرض إذا تجاوزت الأخطاء الحسابية في الأسعار بعد تصحيحها وفقاً لأحكام هذه المادة أكثر من (10%) من قائمة الأسعار أو إجمالي قيمة العرض زيادةً أو نقصاً.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

54- فحص العروض

تلتزم لجنة فحص العروض، عند تحليل العروض بمعايير التأهيل ومعايير التقييم وشروط المنافسة، مع الأخذ بعين الاعتبار ما يلي:

أولاً: تفتح لجنة فحص العروض ملف الأسعار التقديرية، كما تقوم بفتح العروض المالية للعروض الفنية المقبولة في الموعد المحدد لذلك بعد إشعار أصحاب العروض الفنية المقبولة بذلك، وتعلن الأسعار للحاضرين من أصحاب العروض.

ثانياً: إذا لم يقدم صاحب العرض أيّاً من الشهادات المطلوبة والمنوه عنها تفصيلاً في الفقرة (6) من هذه الكراسة أو كانت الشهادات المقدمة منتهية الصلاحية، فيمنح صاحب العرض مدة تحددها لجنة فحص العروض على ألا تزيد على (عشرة) أيام عمل لاستكمال تلك الشهادات فإن لم يقدمها في الوقت المحدد يستبعد من المنافسة ويصادر الضمان الابتدائي.

ثالثاً: إذا أغفل المتنافس وضع أسعار لبعض البنود جاز للجنة فحص العروض استبعاد عرضه أو اعتبار البنود غير المسعرة محملة على القيمة الإجمالية للعرض. ويعتبر المتنافس موافقاً على هذا الشرط عند تقديمه للعرض.

رابعاً: يعتبر المتنافس كأن لم يقدم عرضاً بالنسبة إلى الأصناف غير المسعرة، ويستبعد عرضه إذا لم تجز شروط المنافسة التجزئة.

خامساً: في حال عدم تنفيذ المتنافس للبنود المحملة على إجمالي قيمة العرض يتم تنفيذها على حسابه، أو يحسم ما يقابل تكلفتها من العرض؛ وذلك بحسب متوسط سعر البند لدى المتقدمين للمنافسة، أو السعر الذي تقدره لجنة فحص العروض في حال العرض الواحد أو عدم تسعير البنود المغفلة من المتنافسين .

سادساً: إذا عدلت الجهة الحكومية عن تنفيذ أي بند من البنود المحملة على إجمالي قيمة العرض يُحسم ما يقابل تكلفتها بحسب متوسط سعر البند لدى المتقدمين للمنافسة، أو السعر الذي تقدره لجنة فحص العروض في حال العرض الواحد أو عدم تسعير البنود المغفلة من المتنافسين.

سابعاً: إذا تساوى عرضان أو أكثر في التقييم الكلي، فتتم الترسية على أقل العروض سعراً فإذا تساوت في ذلك، فتقوم الجهة الحكومية بتجزئة المنافسة بين العروض المتساوية، متى كانت شروط ومواصفات المنافسة تسمح بذلك، وإذا لم ينص على التجزئة، فتكون الأولوية في الترسية للمنشآت الصغيرة والمتوسطة المحلية، وتجرى منافسة مغلقة بين العروض المتساوية في حال تعذر ذلك.

ثامناً: للجنة فحص العروض إعادة تسعير البنود، إذا تبين لها أنها وضعت بشكل غير مدروس ولا تمثل السعر الحقيقي للبنود على ألا يؤثر ذلك في السعر الإجمالي للعرض. فإذا رفض المتنافس إعادة التسعير، يستبعد من المنافسة ويرد له ضمانه .



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

55- الإعلان عن نتائج المنافسة

أولاً: تعلن الجهة الحكومية عن العرض الفائزة في المنافسة في البوابة أو الوسيلة البديلة وتبلغ صاحبه بذلك، ويتضمن الإعلان المعلومات الآتية بحد أدني :

أ. صاحب العرض الفائز.

ب. معلومات عن المنافسة.

ج. القيمة الإجمالية للعرض الفائز.

د. مدة تنفيذ العقد ومكانه.

ثانياً: يُبلغ المتنافسون الآخرون بنتائج المنافسة، وأسباب استبعادهم بما في ذلك الدرجات الفنية لعروضهم.

ثالثاً: تنشر البوابة نتائج وبيانات المنافسات والمشتريات التي تزيد قيمتها على (مئة ألف) ريال، وذلك خلال (ثلاثين) يوماً من التعاقد بحد أقصى، على أن تنشر معلومات كل عقدٍ على حدة، وأن تشمل تلك المعلومات ما يلي:

أ. اسم المتعاقد وعنوانه ونوع العقد.

ب. مدة العقد وقيمه ومكان تنفيذ.

ج. تاريخ تسليم الأعمال.

56- فترة التوقف

يجب على الجهة الحكومية الالتزام بفترة توقف بعد إخطار المتنافسين بنتائج المنافسة، وذلك وفقاً للضوابط الآتية:

أولاً: تلتزم الجهة الحكومية بفترة التوقف (5) أيام عمل من تاريخ إعلان نتائج المنافسة، وتلتزم الجهة الحكومية بالإعلان عنها في البوابة الإلكترونية أو الوسيلة البديلة .

ثانياً: في حال تعذر الإعلان في البوابة أو موقع الجهة الحكومية أو الوسيلة البديلة لأسباب فنية، يبلغ المتنافسين بذلك عبر البريد الإلكتروني.

ثالثاً: مع مراعاة ما ورد في المادة (السابعة والثمانين) من النظام، تستقبل الجهة الحكومية التظلمات على قرار الترسية أو إجراء من إجراءاتها من خلال البوابة أو الوسيلة البديلة.

رابعاً: لا يجوز للجهة الحكومية أن تقبل أي تظلم بعد انتهاء فترة التوقف.

خامساً: لا يعد قرار الترسية نافذاً حتى تنتهي فترة التوقف، ويتم البت في التظلمات إن وجدت.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

القسم السادس: متطلبات التعاقد

57- إخطار الترسية

تقوم الجهة الحكومية بإرسال خطاب الترسية للمتنافس / المتنافسين الفائزين عن طريق البوابة الإلكترونية أو الوسيلة البديلة، ويتضمن الخطاب نطاق العمل، والقيمة، وتاريخ بداية العقد، وأن قرار الترسية لا يرتب أي التزام قانوني أو مالي على الجهة الحكومية إلا بعد توقيع العقد من جميع الأطراف.

58- الضمان النهائي

أولاً: يجب على من تتم الترسية عليه تقديم ضمان نهائي بنسبة (5.00%) من صافي القيمة الحالية للعقد، وذلك خلال (خمس عشر) يوم عمل من تاريخ إبلاغه بالترسية. ويجوز للجهة الحكومية تمديد هذه المدة لمدة مماثلة واحدة، وأما في الأعمال والمشتريات التي تنفذ خارج المملكة العربية السعودية: ويجوز للجهة تمديد تلك المدة لمدد مماثلة بما تراه محققاً للمصلحة.

ثانياً: إذا كان صاحب العرض من المنشآت الصغيرة أو المتوسطة يتوجب عليه دفع غرامة مالية إلى الجهة الحكومية تساوي قيمة الضمان الابتدائي، إذا لم يقدم الضمان النهائي في حال تمت الترسية عليه، وفي حال مرور (60) ستين يوماً من تاريخ انتهاء مهلة تقديم الضمان النهائي دون أن يقوم بدفع الغرامة المالية المقررة يعاقب بمنعه من التعامل مع الجهات الحكومية لمدة (سنة).

ثالثاً: يجب على الجهة الحكومية الاحتفاظ بالضمان النهائي إلى أن يفي المتعاقد معه بالتزاماته ويستلم المشروع استلاماً نهائياً وفقاً لأحكام العقد وشروطه.

رابعاً: مع مراعاة المادة (الحادية والستون) من النظام، لا يلزم تقديم الضمان النهائي في الحالات الآتية:

- أ. إذا كانت قيمة الأعمال والمشتريات لا تتجاوز (مائة ألف) ريال.
- ب. التعاقد بين الجهات الحكومية.
- ج. التعاقد مع مؤسسة أو جمعية أهلية أو كيان غير هادف إلى الربح.
- د. التعاقد مع الشركات التي تملك الدولة فيها نسبة لا تقل عن (51%) من رأس مالها.
- هـ. إذا كُلف المتعاقد بأعمال إضافية.
- و. الأعمال والمشتريات التي تنفذ خارج المملكة العربية السعودية.

59- توقيع العقد

مع مراعاة الفقرة (2) من المادة (الخامسة والخمسين) من النظام، لا يجوز البدء في تنفيذ الأعمال المتعاقد عليها قبل توقيع العقد، وتحدد الجهة الحكومية موعداً لتوقيع العقد بعد تقديم الضمان النهائي، وأما في الحالات التي لا يلزم فيها تقديم الضمان النهائي بموجب البند (رابعاً) من الفقرة (58) من هذه الكراسة فيكون تحديد موعد توقيع العقد بعد صدور قرار الترسية والإعلان عنه، فإن تأخر عن الموعد المحدد دون عذر مقبول، يتم إنذاره بذلك، فإذا لم يحضر لتوقيع العقد خلال (15) خمسة عشر يوماً من تاريخ إنذاره، يلغى قرار الترسية وذلك دون إخلال بحق الجهة الحكومية في الرجوع على صاحب العرض الفائز للتعويض عما لحق بها من ضرر، وتزود اللجنة المنصوص عليها في المادة (الثامنة والثمانين) من النظام بنسخة من القرار؛ للنظر في هذه المخالفة.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

القسم السابع: نطاق العمل المفصل



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

60- نطاق عمل المشروع

HI]HT HGLAV,U

الهدف:توريد وتركيب الانظمة السيبرانية

وصف الهدف:توريد الاجهزة المشار اليها في جدول الكميات وتركيبها وضبطها في احد مراكز البيانات الخاصة بالهيئة السعودية للبيانات والذكاء الاصطناعي

الهدف:توفير خدمات مدارة لمركز مراقبة عمليات الامن السيبراني SOC as service

وصف الهدف:توفير خدمات مركز عمليات الامن السيبراني لمراقبة الانظمة على مدار الساعة (24*7*365) حسب جدول الكميات على ان يتم الالتزام بالضوابط والتشريعات الخاصة بالامن السيبراني في المملكة العربية السعودية في تنفيذ هذه الخدمات

الهدف:توفير اختبارات الامن السيبراني

وصف الهدف:توفير الاختبارات اللازمة وتشمل اختراق الانظمة وتقييم الثغرات السيبرانية للتأكد من سلامة الانظمة ومأمونيته حسب جدول الكميات و على ان يتم الالتزام بالضوابط والتشريعات الخاصة بالامن السيبراني في المملكة العربية السعودية ف تنفيذ هذه الخدمات

الهدف:توفير إدارة وتشغيل للخدمات والانظمة الأمنية السيبرانية

وصف الهدف:تشغيل الخدمات والبرامج التقنية على مدار الساعة لحماية المنصة الوطنية للذكاء الاصطناعي من الاختراقات والهجمات السيبرانية حسب جدول الكميات

الهدف:الحد من المخاطر السيبرانية

وصف الهدف:تطبيق الضوابط الأمنية اللازمة ودعم أصحاب المصلحة وتوفير الحوسبة اللازمة لتسهيل إنجاز الأعمال حسب المتطلبات خلال أعمال مشاريع المركز الوطني للذكاء الاصطناعي المتعددة

الهدف:حماية البنية التحتية

وصف الهدف:رفع مستوى الامتثال لمعايير الأمن السيبراني التنظيمية و تحقيق الأهداف الاستراتيجية للأمن السيبراني بمر المعلومات الوطني

أهداف المشروع

الهدف:

تأمين كافة مكونات الحاسب فائق الأداء وأجهزة التخزين فائق الأداء وأجهزة معالجة البيانات ضد تهديدات الامن السيبراني.

وصف الهدف:

سوف يتم تركيب متحكمات الامن السيبراني شاملة الأجهزة و البرامج و مكدراتها و تقديم الخدمات اللازمة لتشغيلها مراقبتها لحماية المنصة و متعلقاتها.

وصف نطاق العمل

يجب أن تعمل كافة أجهزة الامن السيبراني بكامل طاقتها بما في ذلك الأجهزة والشبكات والمتحكمات والبرمجيات.

يجب أن تتضمن أجهزة الامن السيبراني كافة خدمات التركيب والصيانة ل ٣ سنوات تبدأ من تاريخ تركيب الأجهزة وبعد موافقة وقبول المستخدم. يقصد بالمستخدم الهيئة السعودية للبيانات والذكاء الاصطناعي.

3. سيتم استخدام المعدات لتأمين وتوفير الارشادات اللازمة لمنصة الذكاء الاصطناعي و تحتوي على الأجهزة حسب جدول الكميات مع الأخذ بالإعتبار دراسة مطابقة الأنظمة و الضوابط لمنصة الذكاء الاصطناعي المستهدف من خلال عمل دراس اثبات جدوى (POC) وفي حال عدم تكامل الحل مع الأنظمة فالهيئة الحق بإلغائها البند أو استبداله.

كيفية تنفيذ الاعمال والخدمات

يجب على المورد تسليم الأنظمة خلال فترة ٤ شهور من استلام امر الشراء ويتضمن ذلك جميع مكونات الأجهزة كما ذكره بجدول الكميات

يجب على المورد تقديم مخطط تفصيلي للمشروع وإطار زمني لتنفيذ منصة مراقبة الامن السيبراني SOC. يجب على المورد توفير عدد كاف من المهندسين المؤهلين لإكمال التثبيت وإجراء نقل المعرفة.

يجب أن تكون جميع القوى العاملة الداعمة متوفرة في الموقع لبدء التركيب عند تسليم النظام.

يجب على المورد إكمال أي متطلبات لوائح التصدير، إذا لزم الأمر. في غضون أسبوعين (2) من تاريخ التعاقد.

يجب على المورد تضمين تراخيص جميع البرامج المرخصة في عرضه. يجب على المورد أيضًا تضمين نسخ من أي اتفاقيات ترخيص برمجيات أو نماذج تنظيم التصدير أو أي مستندات قانونية تكمّلها الهيئة السعودية للبيانات والذكاء الاصطناعي جنبًا إلى جنب مع العرض الفني.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز الذكاء الاصطناعي NCAI-HPCCYB

سيتم اعتبار المعدات قد تم تسليمها فقط عندما يتم تسليم جميع المكونات إلى مركز البيانات المعين المختار من قبل الهيئة السعودية للبيانات والذكاء الاصطناعي. يجب على المورد اكمال توصيلات الأجهزة وتشغيل الأنظمة وتكوينها وقياس الأداء وقبول المستخدم للأنظمة في غضون ثلاثة (3) أسابيع من التسليم.

يجب على مقدم خدمات الأمان المُدارة توفير خدمات الكشف والاستجابة المُدارة (مراقبة التهديدات المباشرة) على مدار 24 ساعة في اليوم وطوال أيام السنة، بالاشتراك السنوي بما يصل إلى 70 جيجابايت بما في ذلك التراخيص

يجب أن تغطي الأصول التالية وليست حصراً على : Active Directory Microsoft، وأجهزة سطح المكتب Microsoft Windows وخوادم Windows Microsoft، وخوادم Linux Linux، وجدار حماية الحدود (8)، وجدار حماية مركز البيانات (4)، ونظام الكشف والاستجابة (EDR)، وجدار حماية تطبيقات الويب، ونظام التحكم في الوصول (NAC) وإدارة الوصول المسيطرة (PAM).

يجب على مزود خدمات الأمان المُدارة توفير جمع السجلات، وتحليلها، وترابطها، وتحليل البيانات، ويجب أن تتم تخزين البيانات في موقع المؤسسة وفقاً للامتثال التنظيمي.

يجب على مزود خدمات الأمان المُدارة توفير رؤية مستمرة على مدار 24 ساعة في اليوم للتهديدات والثغرات والهجمات، بالإضافة إلى خدمة الاستجابة للحوادث مع خدمات التحسين

يجب على مقدم خدمات الأمان المُدارة توفير خدمة الكشف والاستجابة المُدارة التي تعزز عملية الاستجابة للحوادث الحالية للعمليات، وتوفر رؤية وخبرة تساعد على التعرف على حاجتهم لاتخاذ إجراءات استجابة، وتقييم المخاطر وتحديد النهج الأكثر فعالية لمعالجة الحادث.

يجب على مقدم خدمات الأمان المُدارة الامتثال لجميع التشريعات المتعلقة بأمن المعلومات.

يجب أن توفر خدمات الأمان المُدارة نموذج التشغيل الذي يعرف الأدوار والمسؤوليات بين المزود والمؤسسة، وكيفية التفاعل مع فريق الأمن السيبراني وإدارة المخاطر والامتثال في المؤسسة، وكذلك معايير خدمة مستوى الأداء (SLAs) وإجراءات الاستجابة للحوادث

يجب على مزود خدمات الأمان المُدارة توفير خدمات استخبارات التهديدات المُدارة باستخدام مصادر مفتوحة وتغذيات استخبارات التهديدات بهدف فهم أحدث التهديدات السيبرانية الناشئة في أقرب وقت ممكن بناءً على مخاطر الأعمال والموقف الأمني.

61- برنامج العمل

المخرجات

اسم المخرج: المخططات التصميمية

وصف المخرج: توفير الوثائق التصميمية (HLD & LLD) و مخططات التوزيع لأجهزة و الاتصال البيني و الخارجي

مرحلة المخرج: إيصال جميع الأجهزة

اسم المخرج: اتفاقية مستوى التشغيل

وصف المخرج: مستند يوضح بنود اتفاقية مستوى التشغيل بين مزود الخدمة والموردين

مرحلة المخرج: الاتفاقيات

اسم المخرج: تقرير حالة التشغيل

وصف المخرج: وثيقة دورية (شهرية - ربعي) بحالة تشغيل بنية الامن السيبراني و تشمل تفاصيل حالة الاستخدام و مشاكل التشغيل و مسبباتها و حلولها

مرحلة المخرج: التشغيل الفعلي

اسم المخرج: طلب إطلاق التيار والتشغيل المبدئي

وصف المخرج: وثيقة طلب إطلاق التيار والتشغيل المبدئي

مرحلة المخرج: توصيل الكهرباء وتنصيب الاجهزة

اسم المخرج: القبول المبدئي للأجهزة والبرمجيات

وصف المخرج: وثائق الاختبار للقبول المبدئي

مرحلة المخرج: إجراءات القبول

اسم المخرج: وثيقة تقديم فريق العمل

وصف المخرج: تقرير بأسماء الفريق و اسناد مهام التشغيل

مرحلة المخرج: تقديم وتجهيز فريق العمل التشغيلي

اسم المخرج: اتفاقية مستوى الخدمة

وصف المخرج: مستند يوضح بنود اتفاقية مستوى الخدمة تفصيليا

مرحلة المخرج: الاتفاقيات



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز الذكاء الاصطناعي NCAI-HPCCYB

اسم المخرج: استلام وتركيب الأجهزة

وصف المخرج: وثيقة بتأكيد استلام وتركيب الأجهزة في مراكز البيانات

مرحلة المخرج: إيصال جميع الأجهزة

المراحل

اسم المرحلة: التشغيل الفعلي

الوصف: التشغيل الفعلي لأجهزة الامن السيبراني

شهر/يوم

شهر

المدة التقديرية

36

اسم المرحلة: الاتفاقيات

الوصف: يقوم المتنافس على توفير و توقيع الاتفاقيات اللازمة بين الموردين، كذلك توفير اتفاقية مستوى الخدمة التي تتوافق م مسودة اتفاقية الخدمة

بالكراسة

شهر/يوم

شهر

المدة التقديرية

1

اسم المرحلة: تقديم وتجهيز فريق العمل التشغيلي

الوصف: تقديم فريق العمل وتفعيل امكانياته للبدء بالعمل التشغيلية

شهر/يوم

شهر

المدة التقديرية

1

اسم المرحلة: إجراءات القبول

الوصف: القيام بعمل إجراءات القبول والتأكد من مطابقة سرعة الحاسب الجمعي وجهاز التخزين

شهر/يوم

يوم

المدة التقديرية

7

اسم المرحلة: توصيل الكهرباء وتنصيب الأجهزة

الوصف: توصيل الكهرباء وتنصيب الأجهزة والشبكات وأجهزة التخزين

شهر/يوم

شهر

المدة التقديرية

1

اسم المرحلة: إيصال جميع الأجهزة

الوصف: يقوم البائع بإيصال جميع الأجهزة المطلوبة

شهر/يوم

شهر

المدة التقديرية

1



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

62- مكان تنفيذ الأعمال

• منطقة الرياض

◦ الرياض



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

63- جدول الكميات والأسعار



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

تقنية معلومات المواد

اسم الجدول



رقم الكراسة :

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التسلسلي	البنية التحتية	الخدمة	الوصف	المواصفات	ملاحظات
1	خدمة	خدمة	شبكة	يجب على مقدمي خدمات الأمن المُدارة توفير خدمات الكشف والاستجابة المُدارة وخدمات الاستشارة بشأن التهديدات. يجب على مقدمي خدمات الأمن المُدارة توفير حلول مجمعة تشمل الحوسبة والتخزين والشبكة. يجب على مقدمي خدمات الأمن المُدارة توفير الكشف المستمر للثغرات باستخدام أدوات الضعف والتكامل مع حلول منصة الكشف والاستجابة المُدارة. يجب على مقدمي خدمات الأمن المُدارة تقديم تقارير أسبوعية أو شهرية للمنظمة بشأن الخدمات المشتركة مع مقدمي خدمات الأمن المُدارة. يجب على مقدمي خدمات الأمن المُدارة توفير ثلاثة مهندسين في الأمن السيبراني لإدارة الضوابط الأمنية المقترحة في الطلب. يجب على مقدمي الخدمات الأمنية المُدارة إجراء تحقيقات عميقة واستجابة للحوادث.	لا
36	خدمة	خدمة	شبكة	يجب على مقدمي خدمات الأمن المُدارة توفير خدمات الكشف والاستجابة المُدارة وخدمات الاستشارة بشأن التهديدات. يجب على مقدمي خدمات الأمن المُدارة توفير حلول مجمعة تشمل الحوسبة والتخزين والشبكة. يجب على مقدمي خدمات الأمن المُدارة توفير الكشف المستمر للثغرات باستخدام أدوات الضعف والتكامل مع حلول منصة الكشف والاستجابة المُدارة. يجب على مقدمي خدمات الأمن المُدارة تقديم تقارير أسبوعية أو شهرية للمنظمة بشأن الخدمات المشتركة مع مقدمي خدمات الأمن المُدارة. يجب على مقدمي خدمات الأمن المُدارة توفير ثلاثة مهندسين في الأمن السيبراني لإدارة الضوابط الأمنية المقترحة في الطلب. يجب على مقدمي الخدمات الأمنية المُدارة إجراء تحقيقات عميقة واستجابة للحوادث.	لا



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	الصفة	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				قبل مزود الخدمة المتعاقد مع		
				هـ		
				د		
				مع		
				الم		
				ب		
				ش		
				ر		
				اليه		
				في		
				جدو		
				ل		
				الك		
				ميا		
				ت		



رقم الكراسة :

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	التمسيد	البنس	وحدة القياس	وصف البنس	المواصفات	ملاحظات
				على ان تكون مدة كل خدمة شهر في مقر الهيئة السعدو دية للبيانا ت والذ كاء الا ص		



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	الغرض	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
						طنا عي



رقم الكراسة :

إسم الإدارة :

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التسلسلي	الصفة	الحد الأدنى	الحد الأقصى	الوصف	المواصفات	الرقم التسلسلي
1	لا			تركيب ووضع بطاقات أمن الحاويات containers security لتأمينها على البيئة السد	Bidder should do the configuration and installation	2



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	الصفة	البند	وحدة القياس	وصف البند	المواصفات	ملاحظات
				حاجبة		
				الخاصة		
				بالمركز		



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	الرقم المميز	الرقم التسلسلي	المواصفات	وصف البند	وحدة القياس	البند	الرقم	الرقم
1		لا	General . • Must be a cloud native platform architecture capable of being deployed on different architectures i.e. container, serverless or public cloud. • Must support a non-intrusive deployment i.e. No appliances or Agents. • Supports automated deployments tools and can leverage APIs for onboarding. • "Supports RBAC model for separation of duties and data - Read Only. - Role for adding cloud accounts.. - Limit access to specific accounts or account groups. Support integration of SSO and Federation providers via industry standard protocols i.e. SAML. • "Capability to feed alerts to 3rd party workflow tools in addition to visualising in the Prisma dashboard • Capability to tune alerts generated and customise the type of alerts that are sent to the relevant workflow tools and teams. • Solution provides an industry standard RESTFUL API. . • Containers (K8 - Managed/Unmanaged) Docker + others. • "Deploy out as a cloud native solution without requiring any agents or additional layers being added to container images or underlying cluster.. • Support deployment on multiple container platforms including:. . - Kubernetes (Cloud hosted EKS, AKS and GKE). - Other variants (Openshift, Pivotal etc). - Docker (stand alone and Swarm). - ECS". • Management platform flexibility to allows hosted SaaS or customer hosted container based management console. • "Kubernetes Deployment options:. . - Scripted. - Deployment manifest YAML. - Helm charts". . . . • Provide protection for cloud functions, deploy into the function.. •	لاضافة طلبقة الحدماية السببرانية للحاويات	عدد	أمن بن الحاويات containers security	3	ذ د م ة



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				Discover cloud functions and vulnerabilities via cloud provider APIs. . • Hosts (Linux, Windows). . • "Deploy out as a cloud native solution that supports a deployment on multiple host platforms including:. . - Windows. - Linux". • Management platform flexibility to allows hosted SaaS or customers self hosted management console. . . Vulnerability Assessment Requirement. General . . • Provides high level visualisation on any vulnerabilities that exist . • Filter based on severity of vulnerability. • Capability to export vulnerability assessment information via API, CSV or integration with other platforms . • Allows filtering of vulnerabilities based on specific criteria i.e. CVE number. • Automatic updating of vulnerability feeds without operational overhead. • Where possible, provide mappings against well known vulnerability standards bodies and metrics i.e CVE and leverage common scoring mechanisms i.e. CVSS. . IAC. . • Capability to scan in the CI phase prior to deployment of instances i.e. Terraform , Cloud Formation . . • Containers (K8 - Managed/Unmanaged) Docker + others. . • Ensure that any vulnerability scanning doesn't require changes to be made to the container image via insertion of agents or similar mechanism. • Capability to scan all container images for vulnerabilities irrespective of whether they are deployed in Public Cloud , On-Premise, Hybrid or air gapped environments. • "Perform Vulnerability assessment at the CI (Continuous Integration) phase of the DevOps build pipeline by plugging into well known build platforms i.e.. - Jenkins. - CircleCi.	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنية	وحدات القياس	وصف البنود	المواصفات	ملاحظات
					- Azure DevOps , AWS codepipeline and others. . • Perform integration capability for other lesser known build platforms.. • Where possible, provide vulnerability metrics directly within the build platform and the option to fail the build if vulnerabilities of a given severity are discovered". • Allow developers to scan a stand alone container image prior to checking into a registry, build pipeline or running. • "Capability to scan container registries to ensure ongoing health of container image, examples include:. • Azure Container Registry. - Docker Hub. - Google Container Registry. - AWS EC2 container registry. - Nexus Sonar. - JFrog . . • Many more providing they are Docker Registry 2.0 compliance". • Capability to discover vulnerabilities in running container images within the environment. • Platform provides the capability to concisely visualise vulnerabilities at the Build, Deploy and Run. • Capability to drill down on each container image and visualise the exact layer(s) where vulnerabilities exist, enable fast feedback via integration with DevOps workflows. • "Capability to understand each vulnerability in-depth and threat vectors that may raise the risk profile in the environment.. • Ease of attack. - Threat Vectors i.e. Network based. - If a fix is available and how long has the vulnerability existed.. - Traits of running containers that elevate risk. - Detailed CVE information and remediation details.. • Understand which containers and hosts the vulnerability exist on.. - Impacted packages/ frameworks.. - Percentage of environment impacted". • The capability to define your own custom



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				vulnerability checks. • "Configure proactive policies to alert on or prevent deployment of vulnerable images into a production environment.. • Policies should be tunable based on the severity level, labels, images and other factors". • In high security environments that are air-gapped, provide a mechanism to update vulnerability signatures. • Vulnerability managemnt should cover Git Repo including Java , Python & ode repositories on git. . • Serverless - Lambda, Azure, GCP Functions. . • Automatically discover vulnerabilities for Serverless functions including any vulnerabilities in function libraries. • ""Capability to understand each vulnerability in-depth and threat vectors that may raise the risk profile in the environment.. - Ease of attack. - Threat Vectors i.e. Network based. - If a fix is available and how long has the vulnerability existed.. - Detailed CVE information and remediation details.. - Impacted packages/ frameworks.. • Hosts (Linux, Windows). . • Capability to scan all supported hosts for vulnerabilities irrespective of whether they are deployed in Public Cloud , On-Premise, Hybrid or air gapped environments. • Capability to discover vulnerabilities in running hosts within the environment as well as AWS AMI. • "Capability to understand each vulnerability in-depth and threat vectors that may raise the risk profile in the environment.. - Ease of attack. - Threat Vectors i.e. Network based. - If a fix is available and how long has the vulnerability existed. - Detailed CVE information and remediation details. - Understand which containers and hosts the vulnerability	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

اسم الإدارة :

إسم النموذج: خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المؤسسة	القطاع	الخدمة	المواصفات	وصف البند	وحدة القياس	البند	الغرض	الرقم التتبعي
			exist on. - Impacted packages/ frameworks.. - Percentage of environment impacted". • The capability to define your own custom vulnerability checks. • "Configure proactive policies to alert on or prevent deployment of vulnerable hosts into a production environment (Linux hosts only).. • Policies should be tunable based on the severity level, labels, images and other factors". • In high security environments that are air-gapped, provide a mechanism to update vulnerability signatures. • Have the ability to apply vulnerability rules when when vendor fixes are available. . • Customer specific use cases. . . Compliance Requirement. General . . • Provides high level visualisation on any compliance violations across the environment for the different architectures i.e. Public Cloud, Container or Serverless. • Filter based on severity of compliance failure. • Capability to export compliance violation events via API, CSV or integration with other platforms i.e Slack, SOAR (Demisto), Jira, Email. • Allows for filtering and searching for specific compliance checks via name, resource impacted or severity plus other metrics i.e. cloud accounts, labels.. • Automatic updating of vulnerability feeds without operational overhead. • Where possible leverage well known compliance standards and regulatory frameworks i.e. NIST, CIS, GDPR PCI, ISO. • Ensure continuous and automatic scanning for compliance without the operators having to manually set and schedule scans. . . • Containers (K8 - Managed/Unmanaged) Docker + others. . • Ensure that any compliance scanning doesn't					



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
					require changes to be made to the container image via insertion of agents or similar mechanism. • Capability to scan all container images for compliance violations irrespective of whether they are deployed in Public Cloud , On-Premise, Hybrid or air gapped environments. • "Provide out of the box baselining against well know standards and frameworks for container images, runtime and kubernetes configuration. - CIS (Docker & Kubernetes). - NIST 800-190. - PCI. - GDPR". • "Perform compliance audit at the CI (Continuous Integration) phase of the DevOps build pipeline by plugging into well known build platforms i.e.. - Jenkins. - CircleCi. - Azure DevOps and others. . • Perform integration capability for other lessor know build platforms.. • Where possible, provide vulnerability metrics directly within the build platform with the option to fail the build if compliance violations of a given severity are discovered". • Allow developers to scan a stand alone container image prior to checking into a registry, build pipeline or running. • "Capability to scan container registries to ensure ongoing compliance of images, examples include:. - EC2 container registry. - Nexus Sonar. - JFrog . . • Many more providing they are Docker Registry 2.0 compliance". • Capability to discover compliance violations in existing running containers within the environment. • Platform provides the capability to concisely visualise compliance violations at the Build, Deploy and Run. • The capability to define your own custom compliance checks. • "Configure proactive policies to alert on or prevent deployment of



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البند	وحدة القياس	وصف البند	المواصفات	ملاحظات
				non-compliant images into a production environment.. . • Policies should be tunable based on the severity level, labels, images and other factors". • In high security environments that are air-gapped, provide a mechanism to update compliance signatures. • Capability to only allows the use of "Trusted images". • "Understand what images are running in the enviroment and allow only ""Trusted Images"" to run.. . - Control via registry. - Repo. - Individual Image. - Base layers of image". . • Serverless - Lambda, Azure, GCP Functions. . • "Automatically discover compliance violations for Serverless functions including:. . - Embedded Private keys and passwords. - Overly permissive access. - Broad resource access. - Unused services that the function can access. - Suspicious function actions". • ""Capability to understand each compliance failure.. . - Ease of attack. - Threat Vectors i.e. Network based. - If a fix is available and how long has the violation existed.. - Impacted functions. • ". • Hosts (Linux, Windows). . • Capability to scan all container images for compliance violations irrespective of whether they are deployed in Public Cloud , On-Premise, Hybrid or air gapped environments. • "Provide out of the box baselining against well know standards and frameworks for hosts including Windows, Lunix, Docker host/ daemon/ security ops, Kubernetes master/worker/ federation:. . - CIS (Docker & Kubernetes). - NIST 800-190. - PCI. - GDPR". • Capability to discover compliance violations in existing running hosts within the environment. • The capability to define your own custom	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البند	وحد القياس	وصف البند	المواصفات	ملاحظات
				compliance checks. • In high security environments that are air-gapped, provide a mechanism to update compliance signatures. • Perform checks look at the Windows host's configuration of the Windows Firewall, Windows Defender / anti-malware, and Windows Update configuration. • Ability to implement security around files and directories in your monitoring profile for changes - File Integrity Monitoring (FIM). • Customer specific use cases. • Incident Response and Protection Requirement. General . . • Provide dashboarding detailing any incidents or anomalies along with criticality. • Support different types of threat detection capabilities including static signature, learning and behavioural analysis. • Capability to export compliance violation events via API, CSV or integration with other platforms • Allows for filtering and searching for specific incidents via name, resource impacted or severity plus other metrics i.e. cloud accounts, labels. • Automatic updating of threat intelligence feeds. • Behavioural and learning based models must be automatic without requiring the operator to manually setup thresholds etc. . . • Containers (K8 - Managed/Unmanaged) Docker + others. . • "The platform can baseline container images and their expected behaviours via a combination of static analysis of dockerfiles and deployment manifest combined with dynamic analysis of a running container, this should include:. - Network activity. - Processes. - File System. . • Container capabilities i.e. Does it have elevate access". • Capability to relearn baseline . • "Capability to report when there is	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				a deviation or abnormal activity compared to the baseline i.e. . . - New process spawned. - Network comms that differs from the baseline. - Exec access to containers". • "Leverages threat intelligence to spot malicious or abnormal behaviour i.e. . . - Crypto Mining. - Malware. - Communication with high risk domains/destinations. - Lateral Movement". • Capability to drill down on incidents and perform forensic investigation and capture/export information related to the incident. • Allows proactive protection against certain incidents including the capability to prevent rogue processes and network activity or in extreme cases to terminate a running container, this should be possible through a flexible policy that can be tailored based on container images, namespace or labels. • The platform automatically maps and learns network activity between the container images in the environment. • Provide a zero trust architecture by implementing microsegmentation to limit lateral movement . • "Provide layer 7 Web application protection for containers hosting web apps, protection should include, protections should include:. - CSRF Protection. - XSS Protection. - Clickjacking protection. - SQL Injection protection. - Attack Tool protection . - Malformed request protection. . . . • Serverless - Lambda, Azure, GCP Functions. . • "Automatically discover compliance violations for Serverless functions which could lead to incidents including:. - Embedded Private keys and passwords. - Overly permissive access. - Broad resource access. - Unused	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				services that the function can access. - Suspicious function actions". • "Capability to protect functions including:. - Network. - Process. • ". • Hosts (Linux, Windows). . • "The platform can baseline hosts and their expected behaviours, this should include:. - Network activity. - Processes". • Capability to relearn baseline learned behaviours. • "Capability to report when there is a deviation or abnormal activity compared to the baseline i.e. . . - New process spawned. - Network comms that differs from the baseline. - Exec access to containers". • "Capability to report when there is a deviation or abnormal activity compared to the baseline i.e. . . - Network comms that differs from the baseline. - App Capabilites. - Application Control / Whitelisting. - Log Inspection. - User, Application and Application Activites. - File Integrity Monitoring". • Capability to drill down on incidents and perform forensic investigation and capture/export information related to the incident. • Allows proactive protection against certain incidents including the capability to alert on rogue applications on hosts, this should be possible through a flexible policy. • The platform automatically maps and learns network activity between hosts in the environment. • Provide a zero trust architecture by implementing microsegmentation to limit lateral movement . • "Provide layer 7 Web application protection for hosts withweb apps, protection should include, protections should include:. - CSRF Protection. - XSS Protection. - Clickjacking protection. - SQL	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	الخدمة	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
					Injection protection. - Attack Tool protection . - Malformed request protection. • Customer specific use cases	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	الرقم الفني	المواصفات	وصف البند	وحدة القياس	البند	الكمية	الرقم التتبعي
100	لا	Encryption Key Management - Hardware Security Modules . Certificate-Based Authentication for outside developers	Encryption Key Management - Hardware Security Modules . Certificate-Based Authentication for outside developers	عدد	Encryption Key Management	خ.د.م.ة	4



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	الغرض	البنية	وحدة القياس	وصف البنود	المواصفات	ملاحظات
				ed Aut hen tica tio n for out sid e dev elo per s		



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التام	الرقم الفرعي	الوصف	المواصفات	ملاحظات	الرقم التام
5	خ د م ا	خ د م ا	خ د م ا	خ د م ا	خ د م ا
36	لا	لا	• يتطلب من مقدم العطاء استخدام الأدوات والخبرات التقنية للبيئات السحابية من خلال خبراء ذات خبرة عملية في هذا المجال ويشمل نطاق العمل عمل تقييم ومراجعة الإعدادات للأنظمة السحابية بما يشمل:- مراجعة الاعدادات الأمنية للأنظمة البيئية السحابية المختلفة مع التدقيق على قياس مدى الالتزام بالمعايير والضوابط الامنية. - يلتزم مقدم الخدمة بالتأكد من تطبيق افضل ممارسات الامنية المعتمدة من الشركات الأم بالإضافة الى . - الكشف عن الثغرات الأمنية بشكل اوتوماتيكي باستخدام أدوات الاختبارات الأمنية لمكونات البيئة السحابية مثل المنصات السحابية والخوادم وأجهزة الشبكة. - مراجعة التصميم التقنية للمكونات السحابية والأنظمة المستضافة بالإضافة الى فحص الاعدادات والقواعد المطبقة. - انشاء وتطوير المراجع الأمنية المعتمدة لجميع المكونات السحابية -Minimum Security Baseline المعتمدة وتعزيز المتطلبات الأمنية بتطوير الخدمات السحابية Standards والتطبيقات المقدمة من خلال منصات الاتمة السحابية Cloud Management Platform. - التطوير وتعزيز المعايير الأمنية لنظم إدارة الحاويات السحابية (Kubernetes & Containers) بما يدعم أنشطة التطوير ونشر الحاويات على الخوادم المتعددة		



رقم الكراسة :

الذكاء الاصطناعي NCAI-HPCCYB

[illegible]



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الغرض	البنية	وحدة القياس	وصف البنية	المواصفات	ملاحظات	الرمز	الكمية
6	اجهزة	Internet Switch	عدد	لربط الشبكات والأجهزة الداخلية	• 24 x RJ45 10/100/10000Mb auto- sensing ports, SFP+ ports, 1x PSU included. . • 8 x RJ45 10/100/1000Mb auto- sensing ports, SFP+ ports, 1x PSU included. . • Support for minimum of 8 switches per stack for 24 port and 48 port switches . • Must support Comprehensive enterprise-class Layer 2/3 feature set on 24/48 port switches . The switch (24/48) must support Layer 3 routing and must be offered with its highest available licensing model . • Switch must be compliant . • Switch should be SDN Open Flow ready . Standards Support . • 802.3 - 10 Base-T . • 802.3u - 100 Base-T . • 802.3ab - 1000 Base-T . • 802.3ac - VLAN Tagging . • 802.3ad - Link Aggregation . • 802.3ae - 10 GigE . • 802.1D - Spanning Tree, GARP and GVRP . • 802.1S - Multiple Spanning Tree . • 802.1W - Rapid Spanning Tree . • 802.1Q - Virtual LANs with Port-based VLANs . • 802.1v - Protocol-based VLANs . • 802.1p - Ethernet Priority with User Provisioning and Mapping . • 802.1X - Port-based Authentication . • 802.2 . • 802.3x - Flow Control . • 802.1AB - LLDP . • 802.1p . • SNMP v1/v2/v3 . • IGMP snooping v1/v2V3 . • IGMP Snooping Querier . • For 24 and 48 port switches, should support routing static capabilities.. • The proposed switch must have 3 years vendor support with 7x24 service. . • The Quantity for the 48 port switches must be 1. . • The Quantity for the 24 port switches must be 2. . • The Quantity for the 8 port switches must be 1	لا	2	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	الرقم الفني	الوصف	الكمية	الوحدة القياسية	المواصفات	ملاحظات	الرقم التتبعي
7	اجهزة	DM Z Switch	عدد	لربط الشبكات والأجهزة الداخلية	• 24 x RJ45 10/100/10000Mb auto- sensing ports, SFP+ ports, 1x PSU included. . . 8 x RJ45 10/100/1000Mb auto- sensing ports, SFP+ ports, 1x PSU included. . . Support for minimum of 8 switches per stack for 24 port and 48 port switches . . Must support Comprehensive enterprise-class Layer 2/3 feature set on 24/48 port switches . . The switch (24/48) must support Layer 3 routing and must be offered with its highest available licensing model . . Switch must be FreshAir compliant . . Switch should be SDN Open Flow ready . . Standards Support . . 802.3 - 10 Base-T . . 802.3u - 100 Base-T . . 802.3ab - 1000 Base-T . . 802.3ac - VLAN Tagging . . 802.3ad - Link Aggregation . . 802.3ae - 10 GigE . . 802.1D - Spanning Tree, GARP and GVRP . . 802.1S - Multiple Spanning Tree . . 802.1W - Rapid Spanning Tree . . 802.1Q - Virtual LANs with Port-based VLANs . . 802.1v - Protocol-based VLANs . . 802.1p - Ethernet Priority with User Provisioning and Mapping . . 802.1X - Port-based Authentication . . 802.2 . . 802.3x - Flow Control . . 802.1AB - LLDP . . 802.1p . . SNMP v1/v2/v3 . . IGMP snooping v1/v2/v3 . . IGMP Snooping Querier . . For 24 and 48 port switches, should support routing static capabilities.. . The proposed switch must have 3 years vendor support with 7x24 service. . . The Quantity for the 48 port switches must be 1. . The Quantity for the 24 port switches must be 2. . The Quantity for the 8 port switches must be 1	لا	2



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	الرقم الفني	الوصف	المواصفات	الكمية	الوحدة	البنية	الرقم
1000	2114	زحمة	FC Cables LC-LC, LC-MC• Fiber Optic SFP Single mode 1Gig/10Gig• Length 3 mtr• Single mode, 8 core - Fiber Optic Cable. • Fiber Optic Patch Panel: Single Mode Duplex LC Fully Loaded 8/16 port. • Fiber Optic LC Duplex Patch chords 3mtrs• Heat Shrink Sleeves, Pigtailed, Alcohol Pads, Labelling and all other required accessories for splicing.	8	اجزة	FC Cables LC LC MC	
1000		لا	UTP Cat7 Patch Chords 3mtrs •	9	اجزة	UTP Cables Cat 7	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

اسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التسلسلي	الوصف	الكمية	الوحدة	المواصفات
10	اجهزة الـ MG MT Switch	عدد	جهاز	• 24 x RJ45 10/100/1000Mb auto-sensing ports, SFP+ ports, 1x PSU included. . • 8 x RJ45 10/100/1000Mb auto-sensing ports, SFP+ ports, 1x PSU included. . • Support for minimum of 8 switches per stack for 24 port and 48 port switches . • Must support Comprehensive enterprise-class Layer 2/3 feature set on 24/48 port switches . The switch (24/48) must support Layer 3 routing and must be offered with its highest available licensing model . • Switch must be FreshAir compliant . • Switch should be SDN Open Flow ready . • Standards Support . • 802.3 - 10 Base-T . • 802.3u - 100 Base-T . • 802.3ab - 1000 Base-T . • 802.3ac - VLAN Tagging . • 802.3ad - Link Aggregation . • 802.3ae - 10 GigE . • 802.1D - Spanning Tree, GARP and GVRP . • 802.1S - Multiple Spanning Tree . • 802.1W - Rapid Spanning Tree . • 802.1Q - Virtual LANs with Port-based VLANs . • 802.1v - Protocol-based VLANs . • 802.1p - Ethernet Priority with User Provisioning and Mapping . • 802.1X - Port-based Authentication . • 802.2 . • 802.3x - Flow Control . • 802.1AB - LLDP . • 802.1p . • SNMP v1/v2/v3 . • IGMP snooping v1/v2V3 . • IGMP Snooping Querier . • For 24 and 48 port switches, should support routing static capabilities.. • The proposed switch must have 3 years vendor support with 7x24 service. . • The Quantity for the 48 port switches must be 1. . • The Quantity for the 24 port switches must be 2. . • The Quantity for the 8 port switches must be 1



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الرقم الفني	الرمز	المواصفات	وصف البند	وحدة القياس	البند	الكمية	الرقم التمسلي
2	لا		System information. License Capacity . • 500-4,000 users. . Hardware Specifications. • 8 GB. Management. • HTTP/S, SSH, CLI, SNMP, Console RJ45. . Network Interfaces . • 4x GE RJ45. Storage. • 4 TB (2 TB x2) Hard Disk. Power Supply . • Single (Optional Dual). Form Factor. • 1U Appliance. Input Voltage . • 100-240V, AC 60-50 Hz. Power Consumption . (Average / Maximum) 120 W / 151 W. Maximum Current. • 100V/5A, 240V/3A. Heat Dissipation. • 550 BTU/h. Operating Temperature . • 32-104°F (0-40°C). Storage Temperature. • -13-158°F (-25-70°C). Humidity. • 5-95% non-condensing. FEATURES SUMMARY. . System. . • Wide range of deployment options:. • Inline, Forward Proxy, Explicit proxy, WCCP/PBR. • Hardware or virtual appliance. • IPv4 and IPv6 address support. • Application Support including HTTP/S. • HA available as active-active and active-backup with. • session synchronization . . Authentication. . • Support for various authentication modes including Radius,. • SAML, LDAP, NTLM, Kerberos. • Password. • In-built authentication requiring no additional device. . . Threat Protection. . • Integration with threat intelligence services for real-time threat updates. • Integration with cloud sandbox to detect advanced threats. • In-built security services requiring no additional appliance. • DNS and Web-Filtering. • Dynamic categorization of websites. • Blocking of malicious and suspicious domains and URLs. • Static blacklists and whitelists. • Application Control. • Granular web application	يعمل على توفير الحماية من كشف العذر وانخفاض به وف	عدد	تقنية الوسي	زخم	11



رقم الكراسة :

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التسلسلي	الصفة	البند	وحدة القياس	وصف البند	المواصفات	ملاحظات	الرموز	الرمز
				ص الترا في ك الدا خل / الخا رج من الى/ الالة رنت وة طبير ق بع خض السد يا سا ت الخا صة ت	control for social websites. • Support for 3000+ applications. • Antivirus, bonet and DLP. • Content Analysis. • Multiple ICAP servers support. • IPS signature and filters. • Web Rating Override. • SSL/SSH Inspection. • Custom Application Signature. . . Advanced Caching. . . Web and video caching. • Reverse web cache. • Traffic Shaping and QoS policies to prioritize Apps. • Dynamic adaptive streaming over HTTP. • Dynamic adaptive streaming over RTP and RTMPT. . . WAN Optimization. . • Protocol Optimization - support HTTP, MAPI, CIFS, FTP,. • and TCP. • Secure tunneling over across WAN. • Wan Optimization peers. . Management and Reporting. . • Support Syslog server. • Granular role based access. • Reporting and Logging. • Policy tests for ease of deployment			



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

رقم التسمية	البنية	وحدة القياس	وصف البنية	المواصفات	ملاحظات
12	اجهزة	عدد	لربط الشبكة والأجهزة الداخلية	Up to 6.4 Tbps switching capacity with up to 2 Bpps of . forwarding performance.. - Up to 36 MB of unified buffer per ASIC.. - Intel 2.4-GHz x86 CPU with up to 120 GB of USB 3.0 or up to 960 GB of SATA SSD storage for container-based application hosting.. - Up to 32 nonblocking 100 Gigabit Ethernet QSFP28 ports.. - Up to 32 nonblocking 40 Gigabit Ethernet QSFP+ ports.. - Up to 48 nonblocking 25 Gigabit Ethernet SFP28 ports.. - Up to 48 nonblocking 10 Gigabit Ethernet SFP+ ports.. - Scalable Layer 3 routing (IPv4, IPv6, and multicast) tables and Layer 2 switching tables.. - Hardware support for Application Hosting (e.g. with Cisco ThousandEyes Enterprise Agent).. 802.1ba AV Bridging (AVB) built in to provide a better AV experience through improved time synchronization and QoS.. - Precision Time Protocol (PTP; 1588v2) provides accurate clock synchronization with sub-microsecond accuracy, making it suitable for distribution and synchronization of time and frequency over the network.. - Support for both static and dynamic NAT and Port Address Translation (PAT)	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الغرض	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات	المرجع	التمديد	م
13	إجهزة حدة الحماية	جهاز حدة الحماية	عدد	لحم اية الشبكة وف حوص حزم الببانات حزم الببانات الداخلة والخارجة من البنية التحتية	General Specification . • Should be provided with Next . . Generation Firewall licenses for IPS, Advanced Malware Protection and Application Control Service, URL and DNS filtering. • The device should support both Explicit Proxy and Transparent Proxy along with all NGFW features simultaneously on the same appliance without any compromise.. • The solution should support advanced SDWAN features to aggregate multiple WAN interfaces, measure application performance among the links and selecting best exit interface for traffic using measured SLAs without additional license. • The SDWAN feature shall fully support IPv4 as well as IPv6. • The SDWAN feature should support both passive WAN health measurement through synthetic transactions and active WAN health measurement through monitoring application session information. • Should support both SSL certificate inspection and full SSL inspection. Solution should support TLS 1.1, 1.2 and 1.3 deep inspection. • The solution must support native integration with similar products to form a fabric to share visibility, share threat intelligence and automate response.. • The device must have APIs.. • It should have inbuilt feature of Two-Factor Authentication (2FA) for SSL-VPN and for Admin login, without needing a separate software/hardware to deploy the solution.. • The system must have the ability to integrate with external threat feeds and IP reputation sources from both public and private sources . • The proposed system shall provide robust	لا		2	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

اسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التسلسلي	الوصف	الوحدة القياسية	البنود	المواصفات
1	واجهة المستخدم	واجهة	واجهة	visibility GUI panels and dashboards. Should support HTML5 based Web UI. The Web UI should not have any Java, Flash or ActiveX components as these components can pose considerable security threats due to frequent-vulnerabilities and end-of-support notices.. • The proposed system shall provide administrators ability to assign arbitrary score given based on the perceived risk of certain events such as visit to malicious websites and malware detection. . • Should be able to send logs simultaneously to existing Centralized logging appliance, multiple Syslog servers and SIEM solutions. • The proposed solution should be leader in last Gartner Network Firewall.. • The proposed solution should be leader in last Gartner WAN Edge Infrastructure.. • The proposed solution should be integrated with any authentication and identification platform and support at minimum; Active Directory, LDAP, RADIUS, TACACS+.. • 8x 100GE/40GE QSFP28 slots and 18x 25GE/10GE SFP28 slots, 2 x GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, 2x 2TB storage and 2 AC power supplies. • 3 Year Advanced Threat Protection (IPS, Advanced Malware Protection Service, Application Control). • 3 Year Secure RMA Service



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الرقم الفني	الوصف	المواصفات	ملاحظات	الكمية	الوحدة	الاسم	الرقم
14	اجزة	Intermedia Switches	لربط الشبكات والأجهزة الداخلية	• 24 x RJ45 10/100/10000Mb auto- sensing ports, SFP+ ports, 1x PSU included. . • 8 x RJ45 10/100/1000Mb auto- sensing ports, SFP+ ports, 1x PSU included. . • Support for minimum of 8 switches per stack for 24 port and 48 port switches . • Must support Comprehensive enterprise-class Layer 2/3 feature set on 24/48 port switches . The switch (24/48) must support Layer 3 routing and must be offered with its highest available licensing model . • Switch must be FreshAir compliant . • Switch should be SDN Open Flow ready . • Standards Support . • 802.3 - 10 Base-T . • 802.3u - 100 Base-T . • 802.3ab - 1000 Base-T . • 802.3ac - VLAN Tagging . • 802.3ad - Link Aggregation . • 802.3ae - 10 GigE . • 802.1D - Spanning Tree, GARP and GVRP . • 802.1S - Multiple Spanning Tree . • 802.1W - Rapid Spanning Tree . • 802.1Q - Virtual LANs with Port-based VLANs . • 802.1v - Protocol-based VLANs . • 802.1p - Ethernet Priority with User Provisioning and Mapping . • 802.1X - Port-based Authentication . • 802.2 . • 802.3x - Flow Control . • 802.1AB - LLDP . • 802.1p . • SNMP v1/v2/v3 . • IGMP snooping v1/v2/v3 . • IGMP Snooping Querier . • For 24 and 48 port switches, should support routing static capabilities.. • The proposed switch must have 3 years vendor support with 7x24 service. . • The Quantity for the 48 port switches must be 1. . • The Quantity for the 24 port switches must be 2. . • The Quantity for the 8 port switches must be 1	2	لا		



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الغرض	البنود	وحدة القياس	وصف البنود	المواصفات	ملاحظات	الرمز	الكمية
15	زخام	حماية نظم أمن الحاسبات	عدد	خدمة تقوية أمن الحاسبات	• The bidder should propose a solution which contain dedicated secure internal DNS and DHCP physical/virtual servers across one datacentre with an overall optimal capacity of 45K DNS QPS and 300 DHCP LPS. • The proposed solution should contain dedicated secure caching DNS with an overall optimal capacity of 23K DNS QPS. • The proposed DNS security solution should contain a dedicated hardware /virtual reporting & analytics server in the main datacentre with total indexing daily capacity of 500MB. • The proposed solution must for 1 and 3 yrs.. • The bidder should propose the below for the SDAIA cloud datacentre. • The proposed solution should contain dedicated secure internal DNS and DHCP virtual servers across one datacenter with an overall optimal capacity of 75K DNS QPS and 450 DHCP LPS . • The proposed solution should contain dedicated secure caching DNS with an overall optimal capacity of 45K DNS QPS. • The proposed solution should contain dedicated external DNS with an overall optimal capacity of 23K DNS QPS. • The proposed DNS security solution should contain a dedicated virtual reporting & analytics server in the main datacentre with total indexing daily capacity of 5GB. • The proposed solution must for 1 and 3 yrs.. • The proposed solution DNS Firewall solution should leverage on-premises DDI platforms to run the DNS Firewall service.. • The proposed solution should offer internal authoritative DNS, DHCP and hybrid DNS firewalling . • The proposed solution should contain on-		لا	1



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	الرقم	البنية	الوصف	المواصفات	ملاحظات
				premises VM based platforms and should cover 1x datacenters capable of running the DNS Firewall service.. • The proposed DNS Firewall license should be used as a hybrid DNS FW that can support cloud-based DNS Firewalling and on-premises DNS Firewalling at the same time. The on-premises DDI solution and Hybrid DNS FW should both be provided from the same technology vendor. . • The proposed DDI solution should offer flexible licenses that can be moved to/from HW platforms to/from virtual based platforms and vice versa.. • The proposed solution should be capable of integrating thru DNS over TLS with on-premises DDI solution deployed in the network. The DDI solution should be available and produced from the same DNS Firewall vendor.. • The proposed solution should be offered from a technology vendor/manufacturer who is able to offer cloud-based DNS FW for protection against Data Exfiltration over DNS.. • The proposed DNS FW solution should offer support for DNSSEC validation.. • The proposed solution must offer DNS Context-aware Security.. • The proposed solution should be offered from a technology vendor/manufacturer that can support Threat Intelligence from same vendor for DNS based Firewalling.. • The proposed solution should be offered from a technology vendor/manufacturer that should support Threat Intelligence data/loCs sharing with SIEM and NGFWs thru WAPI calls.. • The proposed solution should be offered from a technology vendor/manufacturer that can offer DNS Firewalling to provide	ن ص ح ة الم علو مة نف س ها (لم يتم تغي يره أ العب ث بها) و س خد م بين الذ طا



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الرقم الفني	الوصف	المواصفات	ملاحظات
		قادت التي تخدم نف س اسد م الذ طا ق لتبا دل الما فا ت بيذ ها	protection against DNS based tunneling, DGA, fast-flux and data exfiltration and infiltration threats.. • The proposed solution should be offered from a technology vendor/manufacturer that can offer DNS Firewalling that should support Behavioral based analytics and detection for DNS based threats.. • The proposed solution should be able to offer DNS Firewalling without any change on the setup leveraging threat intelligence and streamlined behavioral analytics thru machine learning.. • The proposed solution should be capable of integrating with 3rd party security eco-systems from NGFWs and SIEM solutions.. • The proposed solution should be capable of protecting users on-premise behind the network and roaming users or users located in branches that don't have direct connectivity to the datacenter(s).. • The proposed cloud DNS firewall solution should support DNS caching for better application performance.. • All provided components of the solution including internal DNS, DHCP and hybrid DNS FW should be provided from the same technology vendor.. • The proposed solution must offer cloud based and on-premise based protection against Data Exfiltration over DNS.. • The proposed solution should offer DNS FW leveraging threat intelligence and streamlined behavioral analytics thru machine learning.. • The proposed DNS FW solution should offer support for DNSSEC validation.. • The proposed solution must offer DNS Context-aware Security.. • The proposed solution should support Threat Intelligence based DNS	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				Firewalling.. • The proposed solution should offer Threat Intelligence Data Exchange (TIDE) platform support Threat Intelligence data/loCs sharing with SIEM and NGFWs thru RESFul WAPI.. • The proposed solution should support cloud based and on-premises based Behavioral based analytics and detection for DNS based threats.. • The proposed solution should be capable of integrating with 3rd party security eco-systems including NGFWs (PaloAlto & Fortinet), Vulnerability Management Systems (Tenable/Qualys/FortiGate/PaloAlto/ServiceNow/Rapid7) and SIEM solutions.. • The secure DDI solution should offer the ability to leverage security eco-system and orchestration using outbound restful API calls and notifications to enable triggering actions and automation across 3rd party systems. . • The secure DNS caching solution should offer the ability to leverage outbound restful API calls and notifications upon DNS security events. Solutions that don't support outbound API calls will be discarded.. • The proposed solution should be capable of protecting users on-premise behind the network and roaming users or users located in branches that don't have direct connectivity to the DCs.. • The proposed cloud DNS firewall solution should support DNS caching for better application performance.. • The secure DDI solution should offer DNS firewalling leveraging DNS RPZ threat intelligence that should contain multiple categories of RPZ security feeds. Solutions with single security RPZ feed will be discarded. . • The secure DDI solution should offer be able to offer	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				DNS firewalling with threat intelligence from the same technology vendor that should contain as minimum all below RPZ security feeds:.. • Base hostnames: The base hostnames RPZ feed is required to enable protection against known hostnames that are dangerous as destinations and are sources of threats, such as APTs, bots, compromised host/domains, exploit kits, malicious name servers and sinkholes.. • Anti-malware: This RPZ feed enables protection against hostnames containing known malicious threats, such as malware command and control (C&C), malware download and active phishing site.. • Ransomware: This RPZ feed enables protection against hostnames containing malware that restricts access to the computer system it infects and demands a ransom for the removal of the restriction. • Bogon: This RPZ feed enables should contain the source addresses of DDoS attacks and is an informal name for an IP packet on the public Internet that claims to be from an area of the IP address space reserved, but not yet allocated or delegated by an Internet Authority or Registry. Bogons are usually the result of accidental or malicious misconfiguration.. • DHS AIS_IP and DHS AIS_Hostname (2 feeds): AIS is a part of the Department of Homeland Security's (DHS's) effort to create an ecosystem in which, as soon as a company or federal agency observes an attempted compromise, the indicator is shared with AIS program partners.. • DHS AIS NCCIC Watch list Hostnames and Domains and DHS AIS NCCIC Watch list IPs (2 feeds): Indicators contained in these feeds appear on the watch	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				list from the National Cybersecurity and Communications Integration Center (NCCIC)	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الغرض	البنية	وحدة القياس	وصف البنية	المواصفات	ملاحظات
16	اجهزة	خوا	عدد	خوا دم لاسد تضافة البرامج للامن السدي	Chassis Chassis with up to 16x2.5" Drives. • Trusted Platform Module Trusted Platform Module 2.0 V3. • Chassis 2.5" Chassis with up to 16 SAS/SATA Drives, 2 CPU. • CPU Gold 6330 2G, 28C/56T, 11.2GT/s, 42M Cache, Turbo, HT (205W) DDR4-2933. • CPU Gold 6330 2G, 28C/56T, 11.2GT/s, 42M Cache, Turbo, HT (205W) DDR4-2933. • Memory Type 3200MT/s RDIMMs. • Memory Type 32GB RDIMM, 3200MT/s, Dual Rank, 16Gb BASE x8. • HDD 2.4TB 10K RPM SAS ISE 12Gbps 512e 2.5in Hot-Plug Hard Drive. • Power Supply Dual, Hot-Plug, Power Supply Fault Tolerant Redundant (1+1), 800W, Mixed Mode. • Rack Power Cord Rack Power Cord 2M (C13/C14 10A). • NIC Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM. • NIC Ethernet X710 Quad Port 10GbE SFP+, OCP NIC 3.0. • BOSS-S2 controller card BOSS-S2 controller card + with 2 M.2 240GB (RAID 1). • SFP SFP+ SR Optic, 10GbE, for all SFP+ ports except high temp validation warning cards. • OS VMware ESXi 7.0 U3 Embedded Image (License Not Included). • OS Licenses VMware vSphere 7 Standard for 1 CPU, up to 32 cores, 1YR VMware SNS. • Warranty Warranty 12Months, 12 Month(s). • Support Support and Next Business Day Onsite Service, 12 Month(s). . • Chassis Chassis with up to 16x2.5" Drives. • Trusted Platform Module Trusted Platform Module 2.0 V3. • Chassis 2.5" Chassis with up to 16 SAS/SATA Drives, 2 CPU. • CPU Gold 6330 2G, 28C/56T, 11.2GT/s, 42M Cache, Turbo, HT (205W) DDR4-2933. • CPU Gold 6330 2G, 28C/56T, 11.2GT/s, 42M Cache, Turbo, HT (205W)	لا



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

رقم التسمية	البنية	وحدة القياس	وصف البند	المواصفات	ملاحظات
				DDR4-2933. • Memory Type 3200MT/s RDIMMs. • Memory Type 32GB RDIMM, 3200MT/s, Dual Rank, 16Gb BASE x8. • HDD 2.4TB 10K RPM SAS ISE 12Gbps 512e 2.5in Hot-Plug Hard Drive. • Power Supply Dual, Hot-Plug,Power Supply Fault Tolerant Redundant (1+1), 800W, Mixed Mode. • Rack Power Cord Rack Power Cord 2M (C13/C14 10A). • NIC Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM. • NIC Ethernet X710 Quad Port 10GbE SFP+, OCP NIC 3.0. • BOSS-S2 controller card BOSS-S2 controller card + with 2 M.2 240GB (RAID 1). • SFP SFP+ SR Optic, 10GbE, for all SFP+ ports except high temp validation warning cards. • OS VMware ESXi 7.0 U3 Embedded Image (License Not Included). • OS Licenses VMware vSphere 7 Standard for 1 CPU, up to 32 cores, 1YR VMware SNS. • Warranty Warranty 12Months, 12 Month(s). • Support Support and Next Business Day Onsite Service, 12 .Month(s)	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الغرض	البنية	وحدة القياس	وصف البند	المواصفات	ملاحظات
17	نظم	نظم	عدد	توريد	On-Premise solution that is compliance with all local laws and - regulations in Saudi Arabia - Integrated Active Directory, Exchange and Office 365 management - One-click AD, O365, and Exchange user creation - Bulk management of AD objects via CSV import - 200+ pre-packaged, actionable reports - Automation for routine tasks such as AD cleanup - OU-based help desk delegation - Template-based user provisioning - Protect against data loss disasters with AD backup and recovery - Integration with popular SIEM, HR management, and helpdesk software - iOS and Android mobile apps, and much more - Create users in AD, Exchange, Office 365, Google Apps, and Skype for Business (Lync) in a single step - Create or modify AD objects (users, groups, contacts, OUs, and computers) in bulk via CSV import - Perform AD tasks such as password reset, account unlock, clean up, and more - Streamline the management of AD objects such as users and OUs with customizable templates - Assign, replace, or revoke Office 365 licenses in bulk. Manage shared, remote, room, and equipment mailboxes - Create backups of AD objects and restore all attributes of an object or only specific attributes - Generate and schedule more than 200 preconfigured, granular reports on AD, Exchange, Office 365, and Google Apps - View inactive users, locked out users, disabled computers, and more in just few clicks - Create custom AD reports to obtain the exact data that you require - Export to a number of formats including HTML, PDF, XLS,	لا



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				XLSX, CSV, and CSVDE - Mention specific users or computers in a CSV file for generating their important details - Generate compliance reports to meet regulatory standards such as SOX, HIPAA, and more - Granularly delegate AD, Office 365, and G-Suite tasks to help desk technicians for specific Ous - Delegate tasks such as resetting passwords, creating users, and more - Delegate without elevating technicians' privileges in Active Directory - Automate routine Active Directory tasks such as AD clean up - Configure a review-approval workflow to execute AD tasks with a structured flo - Exercise control over automated tasks by using workflow with automation - Manage users from anywhere- Reset passwords; unlock, enable, disable and delete accounts - View reports on locked out, disabled, password, expired and inactive users - View, manage, and execute AD workflow requests - Audit Windows file servers, failover clusters, NetApp, and EMC storage to document changes to files and folders - Track changes across Windows servers, printers, and USB devices with a summary of events - Leverage advanced statistical analysis and machine learning techniques to detect anomalous behavior and defend against cyber attacks - Monitor, report, and alert on domain controllers in real time - Utilize over 200 detailed, event-specific GUI reports - Track changes to Group Policy and all AD objects - Track logons and logoffs to workstations - View and schedule graphical reports - Report on employee attendance, total active and idle time - Monitor activity on terminal services - Track file	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنية	وحدتها	وصف البند	المواصفات	ملاحظات
				creation, modification, and deletion - Get forensics on security and permission changes - Monitor network shares AD45 Utilize file integrity monitoring (FIM) - Also monitor, alert and report on AD FS, AD LDS, LAPS, DNS, NAS devices, scheduled tasks and processes, Windows security log and other system events - Track all changes to Windows AD objects including users, groups, computers, GPOs, and OUs. - Achieve AD monitoring with a single, correlated view of all the activities - Monitor every user's logon and logoff activity, including every successful and failed logon attempt across network workstations - Audit Windows file servers, failover clusters, NetApp, and EMC storage to document changes to files and folders - Audit file access - Monitor system configurations, program files, and folder changes to ensure file integrity - Audit removable storage devices. Audit print servers - Monitor RADIUS logons	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التسمية	البنية	وحدة القياس	وصف البن	المواصفات	م
18	اجهزة	خادم server	عدد	خوا دم لحف ظ وتو فير التق اريبر دور ية ولا مرا قبة بش كل عام	م
				M640 Chassis - 2.5". • 2 x Gold 5220 -2.2Ghz - 16 Core. • 8x 16GB • DDR4 2666Mhz RDIMM. • 16 x 900 GB 15K SAS drives. • PERC H330 Mini Blade Controller (RAID 0/1/5/10/50). • 2 x Pass Through Mezz Adapter - VRTX. • Intel X520 10GbE DP KR NDC. • IDSDM with 2 x . 16GB SC cards. • Dell iDRAC9 License Enterprise	م



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الغرض	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات	الرمز	الكمية
19	اجهزة	نظام	عدد	توريد	"يجب توريد وتركيب نظام ادارة صلاحيات دخول مسؤول النظام PAM الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: The product should be deployed in a variety of footprints including a physical appliance, a VMware virtual appliance, , and provide equivalent capabilities in each.. The product provides a bastion-host gateway to broker - as proxy - user access to managed target devices (*NIX, Windows, etc.) with a zero-trust posture.. The solution must be based on a fully featured Appliance, with at least Open Authentication, Zero-Trust model, Password DB, Discovery, Access Control policies, Session Recording, VMware management, Cloud Applications Management, Command Broker hosted on the same Appliance without the need of additional modules or components. The Solution must provide Load Balancing (VIP configuration, algorithms and management) and High Availability (Clustering and Disaster Recovery) capabilities within the Appliance, without the need of any 3rd party software or licenses.. The High Availability Architecture must be able to support One or Multiple Datacenters installation (WAN) without the need of 3rd party software or licenses.. The preferred PAM High Availability is Active-Active, and the Internal Password Database must natively provide a complete Replication Architecture without the need of 3rd party software or licenses. . The High Availability Architecture	لا	50	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	الرقم المميز	الرقم المتتالي	المواصفات	وصف البند	وحدة القياس	البند	الرقم التتبعي
			must be able to support Active-Active and Active-Passive Disaster Recovery installations without the need of 3rd party software or licenses. In case of Multiple Datacenter (WAN) installation, the High Availability Architecture must be able to provide the capability to use any of the PAM Sites to recover (for DR or any other unavailability scenarios) the main Production Site, without the need of 3rd party software or licenses.. The PAM Solution supports an upgrade process in-place, using the provided GUI and based on patch/payload files.. The product's Appliance is highly scalable, supporting (for example) 3000 concurrent SSH sessions, 1500 concurrent RDP sessions, or 2000 concurrent connections of mixed SSH and RDP regardless of which form factor (physical or virtual) is used and with Session Recording active. The product adds scale by simply adding new appliance to a cluster.. The PAM solution must be accessed via a dedicated "PAM Client" to be installed on the Users' Desktops/Laptops. The Session Recording capability must provide a Primary Storage and a Failover Storage, with the possibility to disable completely the Access to the managed devices when the Session Recording storage is not available/mounted. The product supports a variety of authentication methods including LDAP v3 compliant directories including AD, OpenLDAP, RHDS, Novell eDirectory, etc., RADIUS and MFA solutions that integrate with RADIUS, x.509 certificate (browser or Smartcard-based), RSA SecurID, SAML 2.0 as a Relying Party, as well as combined authentication such as LDAP + RADIUS..				



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الرقم الفني	الوصف	المواصفات	ملاحظات
			The product includes an internal user store for maintaining product administrator's identities, to ensure independence from an external directory for protecting privileged operations.. The product logs all activity including administrative operations and user activity. User Activity attributes actions to the named user.. The PAM Solution must provide proof of compliance with the following Certifications: 23 NYCRR 500, FISMA, HIPAA, NERC, NRC, PCI/DSS, GDPR. The PAM Solution must provide proof of compliance with the Common Criteria certification with a NIAP approved Enterprise Security Management Protection Profile (NIAP- Preferred Protection Profile). The Solution must provide a Target Connector Framework, enabling to easily build custom Connectors for remote targets that are not supported with out-of-the-box Connectors.. The PAM Solution can provide an add-on for reporting any suspicious behavior with privileged access and proactive remediation actions.. This Behavioral Analysis add-on must be based on an Appliance and specifically designed, configured and specialized for collecting and elaborating the PAM data.. 2FA Solution - 2nd Factor Authentication Credentials (i.e. Mobile OTP, Soft Token, etc.) should be generated on a Mobile App and without the need of any connection or network access for the mobile device.. 2FA Solution - 2nd Factor Authentication Credentials (i.e. Mobile OTP, Soft Token, etc.) must support also Push Notification and SMS as alternative methods to receive/consume the second factor credential.. 2FA Solution - 2nd	



رقم الكراسة :

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التسلسلي	الصفة الوصفية	المواصفات	وصف البند	وحدة القياس	البند	القيمة	الرمز
		Factor Authentication Credentials technology must be patented by the vendor and must not require any kind of user password being in transit on the network . The PAM Solution controls access to many different endpoint types such as UNIX/Linux via SSH or Telnet, Windows and RDP Published Apps, Databases, Mainframes via TN3270 or TN5250, Network devices via SSH or telnet, web-based apps via http/https/SAML, etc.. The product controls user access to managed systems through the appliance using a "Zero Trust" model that prevents access that is not explicitly granted.. Provides in-line command filtering using white lists/black lists for SSH, network devices and Mainframe command line operations. No endpoint agent needed.. Can detect when violations of the white list/black list rules occur and can automate action as a result including warning the user, logging off the session, or disabling the user's account within the product as well as alerting when the event occurs.. The product provides highly efficient integrated video session recording with low storage requirements. Videos are fingerprinted to ensure they have not been tampered with. Violations of policies are highlighted in the videos. Video Session Recording is supported for RDP, Telnet, SSH (via CA PAM applet and Windows Putty client), HTTP, HTTPS, TN3270 and TN5250 sessions.. The product allows administrators to terminate active sessions from within the product's Web interface.. Provides a socket filtering capability to prevent unauthorized outbound TCP/IP connections on managed systems					



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
					including *NIX and Windows.. The product supports using RDP to published applications in which the user can be confined, rather than requiring RDP to a full desktop.. The product allows local/desktop applications to be invoked for connecting to the managed devices via the appliance.. The product supports logging in to the managed applications using SAML 2.0, with the product as the IdP.. The product provides fine-grained control over AWS console features so that administration of AWS can be secured, delegated and managed. The product uses AWS APIs to manage all access to AWS. New instances of AWS servers are automatically detected and managed.. The product controls and audits access to privileged accounts in VMware vCenter. New Virtual systems are automatically detected and managed.. The product provides fine-grained control over VMware NSX so that administration of NSX can be secured, delegated and managed.. The product Controls and Audits administrative access to MS Office 365.. The product can be deployed as an MS Azure instance and can Control and Audit administrative access to MS Azure. Kerberos Authentication for RDP sessions when users are logged in with PIV/CAC smart cards (PIV pass-thru).. The product controls access to high-privileged accounts such as *NIX root and Windows Administrator, sa, etc.. The product provides automated login to managed endpoints using privileged credentials, without revealing the credentials to the user.. The product supports password management for privileged accounts, to rotate passwords after it



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				has been used or viewed, and/or at scheduled intervals. Password composition and view policies can be customized.. The product supports SSH Key management for managed endpoints across the hybrid enterprise, including on-prem, private or hybrid cloud, and IaaS-based devices for authentication of privileged accounts and rotation of SSH keys.. The product allows secondary authentication (such as to sudo, databases or other targets that require a second authentication) to be invoked by authorized users and optionally supplies the privileged account credential when it is required.. The product allows "Learn Mode" to build transparent login configurations to acquire credentials when using RDP published applications.. The product uses a simple "Learn Mode" to acquire credentials of web-based apps by allowing users to map the applications credentials to the fields of the product.. The product can require an approval by designated users as a condition of accessing the credentials for managed accounts.. The product can validate that a Ticket exists as a condition of granting access to a privileged credential using the customers help desk including CA Service Desk Manager, BMC Remedy, HP Service Manager, ServiceNow, and Salesforce Service Cloud.. This integration must be provided out-of-the-box. The product provides tools/APIs for enabling applications that require access to privileged accounts to access credentials programmatically, eliminating the need to "hard code" credentials into the script or application. Password can be rotated	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				automatically.. The product should be able to manage passwords stored in plain, hardcoded in system files or user-defined files, JDBC definitions, etc. including within application configuration files, code or scripts.. In addition the solution must provide a JDBC driver wrapper for addressing the J2EE applications use case.. The A2A capability must support at least the following languages: Java, Perl, C, C++, C#, Korn Shell, C Shell, PHP, Python, PowerShell, Visual Basic, Visual C++, VB Script, and JavaScript.. The product should have capabilities to provide credentials for authenticating applications/scripts at run-time and using batch processes.. The A2A capability must operate with a full secured process, as follows:.. · The Account must be classified as A2A. · The Account must have an "alias" so the programmers don't need to know the credential. · PAM must verify the agent/client who's asking the credentials. · PAM must verify the name of the alias. · PAM must verify the script or program invoking the request. · PAM must verify the user ID invoking the request. · PAM must verify the path of the calling program. · PAM must verify the hash of the calling program من تاريخ التشغيل.. . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة .	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التسمية	البنية	وحدتها	وصفها	المواصفات	ملاحظات
20	اجهزة	خوادم	خوادم	Chassis 8x2.5 Front Storage. • Trusted Platform Module Trusted Platform Module 2.0 V3. • Chassis 2.5" Chassis with up to 8 Hard Drives (SAS/SATA), 3 PCIe Slots, 2 CPU. • CPU Gold 5317 3G, 12C/24T, 11.2GT/s, 18M Cache, Turbo, HT (150W) DDR4-2933. • CPU Gold 5317 3G, 12C/24T, 11.2GT/s, 18M Cache, Turbo, HT (150W) DDR4-2933. • Memory Type 3200MT/s RDIMMs. • Memory Type 32GB RDIMM, 3200MT/s, Dual Rank, 16Gb BASE x8. • HDD 960GB SSD SAS ISE Read Intensive 12Gbps 512 2.5in Hot-plug AG Drive, 1 DWPD,. • HDD 1.92TB SSD vSAS Read Intensive 12Gbps 512e 2.5in Hot-Plug AG Drive SED, 1DWPD,. • Power Supply Dual, Hot-plug, Power Supply Fault Tolerant Redundant (1+1), 800W, Mixed Mode. • Rack Power Cord Rack Power Cord 2M (C13/C14 10A). • NIC Ethernet X710 Quad Port 10GbE SFP+, OCP NIC 3.0. • OS VMware ESXi 7.0 U3 Embedded Image (License Not Included). • OS VMware vSphere 7 Standard for 1 CPU, up to 32 cores, 1YR VMware SNS. • Warranty Parts Only Warranty 12Months, 12 Month(s). • Support ProSupport and Next Business Day Onsite Service, 12 Month(s)	3



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	الرقم الفني	الوصف	البنية	البنية	البنية	البنية	البنية
2	لا	"يجب توريد وتركيب نظام الكشف و الاستجابة لأنظمة الشبكة NDR الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: . The solution should be available as hardware appliance or virtual appliance or as a software . The solution should provide all the required functionalities in one box only that consumes a maximum of 2U Rack Space without the need to add more boxes Support out-of-band management. Built in GUI for system management. Management interface must be accessible from any standard browser and work on any standard OS. (Windows, MacOSX, Linux, Firefox, Safari, Chrome, Internet Explorer). Solution should not require the installation of any client (thick or thin) . Support up to 200 individual users accounts for management. Support at least 10 unique users logged in simultaneously. Support LDAP based authentication for management access. Support separate management roles for administration and users. Support encrypted session for all management functions (SSL, SSH). Support an integrated database and reporting engine that does not require user-configuration, maintenance, or tuning. . Support an audit log of management activities. Support safe downloading of reconstructed artifacts, either individually or as an archived collection. Support sending system alerts and events to an external syslog and log aggregators. Support SNMP v2 & v3	توريد	عدد	نظ	ز	21



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التسمية	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				queries for system health and status. Support sending SNMP traps for system alerts and events. Support sending Email notifications for system alerts and events. Support an API for extended attribute extraction and protocol classification. Ability to revoke a user's access. Support central management for at least 35 remote capture devices. Support encrypted communications between the central manager and all remote capture devices. Support interacting with and configuring all remote capture devices simultaneously from the central manager. Support federated queries to all devices under management from the central manager.. The communication between the central manager and the remote devices should not utilize more than 3% of a 1 Gbps link. Support out-of-band passive deployments. Support a VM based deployment. Support a VM deployment that can regenerate intra-guest VM traffic from a virtual switch to a physical network segment. Support a bare metal install on approved provided hardware. Support cluster mode deployments for enhanced throughput and processing. Support Direct Attached Storage to increase forensic retention beyond internal storage. Support capturing and retaining regenerated traffic from, aggregation TAPs, SPAN ports, and mirror ports. Support efficient capture on multiple interfaces simultaneously. Support both optical and copper connections for capture. Support a minimum of 4x 10 Gbps copper connections for capture. Support capturing inbound and outbound data concurrently. Support full Berkley Packet Filter	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	الرقم القياسي	المواصفات	وصف البند	وحدة القياس	البند	الرقم القياسي	الرقم التتبعي
		(BPF) functionality for inclusive/exclusive packet capture per capture interface. Support processing, capturing, and recording packets at a sustained 5 Gbps for 6 hours with 99.999% data capture rate.. Support network links that can burst up to 10 Gbps. Support capture and processing of traffic that is 802.1Q tagged. Support data storage solutions and scale up to 800TB per appliance . Support capture and query of both IPv4 and IPv6 traffic. Support exporting RAW PCAP data from query results. Support real-time regeneration of traffic flows to secondary capture or analysis solution.. Support playback of historical traffic based on specific time frames to secondary capture or analysis solution. Support the following classes of reputation services: virus scanner, domain reputation, URL reputation, hash reputation, and file analysis integration.. Solution should provide automated workflows and instant reports deliver complete forensic details, contextual awareness and actionable intelligence about breaches—including root-cause exploration and reconstruction of breach activity for fast time-to-resolution.. Support extracting files/artifacts from flows in common network protocols (HTTP, SMRTP, SMB, IM, etc.). Support an integrated solution to preview artifacts/files that have been extracted from flows.. Support interpreting JavaScript to discover obscured content or exploits. Support geo location for identifying the sources of communications by country. Support storing meta-data for 3x longer than capture data. Support efficient DPI					



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				inspection regardless of the number of protocol classifiers instantiated. Support alerts for any indexed metadata. Support real-time alerting for reconstructed files . Support a hashing mechanism for extracted file types.. Support near real-time verdict tracking via automated threat intelligence, reputation services AND malware detonation platforms.. Support user configurable dashboards. Support reporting on any and all flows for a predetermined time frame. Support alerting on any single or combination of metadata attribute(s) in near real-time. Support reconstruction of multiple platform file types, including Windows executables and archives (zip, exe, dll, PE, etc.), Mac .pkg and .dmg files, Android .ap files, etc.. Support extraction of large files, i.e. there should be no restriction on the file size of the artifacts being extracted.. Ability to save reports for later use.. Easy configuration of reporting tools.. Support classification and indexing of traffic within nested (tunneled, encapsulated) protocols at least 10 layers deep.. Support Active Directory Integration so it can perform mapping between users and all related attributes such as IP addresses. Support report caching for consecutive queries of the same data. Support integration with other network tools via REST or other API.. Support integration with external firewalls. Support integration with external IPS solutions. Support integration with external SIEM solutions. Support integration with external malware analysis solutions . Support integration with external endpoint forensics	



رقم الكراسة :

اسم الإدارة :

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التسلسلي	الوصف	الوحدة	الميزانية	المواصفات	ملاحظات
					solutions. Support session flow . Support to discard the row data and keep only meta data . توفير الدعم الفني والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لا يندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة .



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التسلسلي	الصفة	البند	وحدة القياس	وصف البند	المواصفات	ملاحظات	الرمز	الاسم	الرقم
22	نظام	نظام	عدد	توريد وتركيب نظام حفظ وسائط الحزم عبر الشبكة TAP الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: . Support tap the links set up with TAPs (and/or SPANs), even if the traffic is not under continuous monitoring.. -Network packet broker with 40 GBE tap feature or more based on the network infra. -Must support captures, aggregates, and distributes network traffic for monitoring nd analysis purposes . port configuration multiple 40GbE ports for connecting to network links, switches, or routes, . -Support packet filtering, load balancing, packet slicing and protocol decapitation . توفير الدعم الفني والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لا يندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة .		لا	1		



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	الرقم الفني	البنية التحتية	البنية التحتية	وصف البنود	المواصفات	ملاحظات
23	نظام	نظام	نظام	توريد	"يجب توريد وتركيب أجهزة فك التشفير عبر الشبكة SSL Broker الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: SSL/TLS visibility. Provides SSL/TLS decryption and encryption, strong cipher support, and flexible deployment.. Dynamic service chaining. Provides service insertion, service resiliency, service monitoring, and load balancing.. Context-based intelligence. Scales with high availability. Granular control والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة	لا



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج: خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم	الوصف	البنية	البنية	البنية	البنية	البنية
24	يجب توفير وتركيب نظام حماية تسريب البيانات Data loss prevention الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: . Detect sensitive corporate operations documents (Governance, Procedures) . Detect sensitive corporate business documents (Legal, M&A, Marketing). . Detect sensitive design documents (Drawings, Project Plans). . Management console supports two-factor authentication for user authentication.. . All communications from different modules with the management console must be encrypted. . Supporting security logging and auditing of administrative actions.. . The solution must support policy tuning workflow and automation, centralized policy, system events, and incidents from management console . . All DLP modules (email, web, network, servers, storage, Cloud, and endpoints) must be managed by a single management console.. . The solution must have one unified policy applied on all DLP modules (email, web, network, servers, storage, Cloud, and endpoints).. . Supporting multiple concurrent administrators.. . Measure risk reduction and demonstrate compliance by using the reports generated from the management console. . Ability to integrate with classification tool. . Accommodating the following content-aware detection techniques: partial and exact document matching, images, structured data fingerprinting, statistical analysis, extended regular expression matching, and conceptual	نظام حماية تسريب البيانات	نظام حماية تسريب البيانات	نظام حماية تسريب البيانات	نظام حماية تسريب البيانات	نظام حماية تسريب البيانات



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				and lexicon analysis using the following detection technologies: vector machine learning, indexed document matching, remote EDM indexer, and exact data matching. • Includes predefined policies or templates to cover standard regulations and best practices. • Policies can be created using user authentication directory services (LDAP), utilizing user group and username information. • Policies can be created based on IP, email address or domain (both as source and destination). • Policies can be created based on method of data transfer (protocol, USB devices, etc.). • Policies can be created based on port. • Policies can be created using combinations of data elements of structured or unstructured data. • Exceptions can be built into rules to minimize false positives. • New rules can be created by copying an existing rule. • All incidents (gateway, endpoint and discovery) report to a central management console. • All policies (gateway, endpoint and discovery) can be managed from a central management console. • Incident details retain source IP address, destination IP address, protocol, and port. • Incident details retain sender e-mail address, recipient e-mail address, and SMTP headers. • Incident details retain all content in the transaction, not just the content that violated policy. • The solution should be capable of defining DLP Policy based on user risk score and response based on user risk score.. • The solution should be capable of protecting and building policies based on Zero trust users regardless of whether the user is authorized or non-authorized to use the data.. • Incident details	



رقم الكراسة :

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التسلسلي	البنية	الوصف	البنية	البنية	البنية	البنية
	المواصفات					
	retain all attachments in the transaction, not just the attachment that violated policy. • Provides for pre-registration (fingerprinting) of known sensitive data . • Provides pre-registration in the form of fingerprinting both structured and unstructured data . • Structured data fingerprinting method provides for specifying which combination of data fields constitute a match on a per-policy basis . • Database fingerprinting process allows for direct connection via ODBC (name each supported database) . • Supports detection based on document type, even if file extension has been changed . • Supports sensitive content in file types of any kind . • Supports recursive review of archived files . • Supports inspection and detection of files of any format (note how many file formats). . • Incidents can be assigned automatically to reviewers . • Incidents can be sorted by severity level . • Incidents can be sorted by sender, recipient, source, destination, protocol, and content type . • Incidents can display and highlight a summary content that violated the policy . • Incident views can be customized based on content pertinent to the reviewer's role and preferences . • Incidents can be grouped by sender, recipient, source, destination, etc., for easy management . • Incident views can be created and saved for easy recall . • Incident reporting can be shared with SYSLOG compatible systems . • Multiple incidents can be assigned to a case for further investigation and remediation . • Cases can be reassigned to different owners after creation . • Case content can be exported with full content and					



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				attachments for review by an external reviewer . . . Interfaces with MTAs to provide for SMTP blocking . . Interfaces with web proxies using ICAP standard for HTTP/FTP blocking . . Supports analyzing SSL traffic using compatible ICAP proxies . . Supports blocking of SSL traffic using compatible ICAP proxies . . Supports notification of policy violation to end user (violation) for email violations . . Supports notification of policy violation to end user (violation) for violations using protocols other than email (HTTP, FTP, etc.) . . Supports notification of policy violation to management . . End user notification is customizable . . End user notification is customizable based on type or severity of violation . . Event reporting includes an explanation of which policy was violated and which portion of the content caused the violation . . Supports "coach mode," notifying user of pending infraction and allowing them to correct or provide justification to proceed. . . Restrict access to specific policy violations based on company role (Compliance, HR, Legal, Finance, etc.) . . Restrict access to policy violations on a per user and per group basis . . Restrict access to actionable functions within policies based on role (Reviewer, Policy Writer, Investigator) . . Limit access to incident details and attachments based on role . . Mask PII or PCI information contained in match summary display based on role . . Restrict access to after-the-fact search capabilities based on role . . Restrict access to case creation, reviewing, modification, or deletion based on role . . Integrate with LDAP for unified user	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				authentication . • Integrate with LDAP groups for unified role definition . • Audit and securely store all user transactions . • Granular access controls to separate system maintenance functions from sensitive information access . • Secure access to the management console using HTTPS . • Secure remote maintenance access to the console using SSH . • Secure storage of local account passwords . • Security hardening measures to remove unnecessary services and network protocols to the DLP systems . • All access to device is logged for an audit trail . • All changes to device configuration or policies are logged . • Audit log is protected from access and manipulation (even via command line or accessing the backend of the device). • Supports centralized reporting for multiple network devices in a single reporting console . • Supports reporting on gateway, endpoint and discovery in a single reporting console . • Provides executive dashboard . • Allows for custom report creation . • Custom reports can be saved (memorized) and re-run . • Reports can run automatically on daily, weekly or monthly basis . • Generate reports in PDF or CSV format . • Develop reports built around stakeholder requirements . • Develop reports based on top (X) policy violations, senders, content type, protocol, etc. . • Build reports from GUI based on current view attributes (columns, content filters, view, etc.) . • Build detailed reports based on historical traffic/content analyzed . • Export historical records for archiving or external review/analysis . • Purpose built appliance . •	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				Turn-key installation and deployment . • DLP system, databases, and assets can be managed by a single department in an enterprise environment . • Single data-at-rest inspection device can analyze and index all sensitive content for data stores up to xxx TB . • Supports sustained bandwidth of up to xxx Mbps with bursts to xxx Mbps . • Supports high availability . • Supports fail over . • Supports network attached storage . • Supports offline archiving of data (in what format) . • Supports encryption of sensitive data fields within the database for PCI compliance . • Supports encryption of entire database . • Provides backup and restore capability of event log data, policies and profiles and system configuration . • Supports load balancing of multiple inspection devices without third-party load balancing devices . • Multiple inspection devices can be managed from a central console (single interface) . • Settings, policies and configurations are automatically replicated across multiple inspection devices . • Capable of monitoring both inbound and outbound connections . • Manages event expiration log as storage limits are met . • . توفير الدعم الفني والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل . . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة .	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

اسم الإدارة :

إسم النموذج: خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	الهدف	البنية	الحدود	الوصف	المواصفات	ملاحظات
25	نظام	نظام	عدد	توريد	"يجب توريد وتركيب نظام حماية وامن دخول الشبكة Network access control الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: . Monitor endpoint status on the network in real-time.. 4 medium network appliances . • Enforce granular policies for access control and endpoint compliance. • Address security operations with automated network security remediation. • Act as an integration hub to share data with other cybersecurity tools. . Solution Must support Centralized Management with a Centralized License. The proposed solution must support Enterprise management via Virtual Machine or Appliance to manage all the appliances from a single admin console when multiple Appliances/Virtual Machines are used to cover the solution. Solution Must support High Availability for the Enterprise Management. Solution Must Support Interactive Dashboard for the Visibility and the Compliance Status. Solution Must support Asset inventory Dashboard. Solution Must support up to 10 Endpoint Appliances Configuration management. Proposed Solution must have two appliances in the main DC with the following Specs to manage the solution and for centralized license.. Proposed solution should be capable of supporting 10,000 endpoints and managing up to 200 Layer-2/Layer-3 network devices.. Proposed Solution should provide Visibility & Control into (Campus Network, Data Center, Cloud, OT and IoT)..	لا



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				Proposed Solution must be scalable for Future expansion without requiring major Architecture changes.. Proposed Solution must support continuous monitoring and assessment for the endpoints while connected to the Network Infrastructure (Periodic reassessment). Proposed Solution must support Windows, Linux, and Mac OS Operating systems, and must support legacy Windows Operating Systems.. Proposed Solution should be capable to block the access of endpoints which are connected on unmanaged network (I.e Unmanaged Switch).. Proposed solution should be capable of identifying IOT devices such as: IP Cameras, VOIP, Projectors, HVAC devices, etc.. Proposed solution must support IoT credential assessment (Default Credentials, Default SNMP Communities, Default Factory Credentials ..Etc.). Proposed Solution must support passive and active check for well known Vulnerabilities and IOC's. Proposed Solution must support open ports and map it to the devices.. Proposed Solution must support IP to MAC Mapping on wired connected devices based on Switch IP and Switch port.. Proposed Solution must support Data Center Visibility including and not limited to VMware, ACI and all components related to it.. Proposed Solution should have the capabilities to check if VMware Tools are installed on a virtual machine. Such as: . • Tools installed and up to date . • Tools installed but upgrade recommended . • Tools installed but need to be updated . • Tools installed but VM is not managed . • Tools not installed . Proposed Solution should have the capabilities to check	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
					if the ESXi host profile is compliant, non-compliant or unknown.. Proposed Solution should have the capabilities to classify different types of VMware virtual machines and servers, such as: . • Virtual Machines . • ESXi Servers . • vCenter Server. Proposed Solution should have the capabilities classifying virtual machines based on VMWare NSX security groups or based on NSX security tags. . Domain, Domain User, Domain Member, OS-Class, IP of the connected switch, Switch Port, Switch Port VLAN, Switch Port Status, Switch Vendor, Access status.. Proposed Solution must support Passive discovery with DPI for IT and IoT protocols.. Proposed Solution must support Passive discovery with SPAN port traffics analysis. .. Proposed Solution should support Access Restriction Based on encryption. Proposed Solution should support Access Restriction Based on patches . Proposed Solution should support Access Restriction Based on AV . Proposed Solution should support Access Restriction Based on Managed Device . Proposed Solution should support Access Restriction Based on AD/LDAP account . Proposed solution should be capable of support/integrating with wide variety of Network switching vendors such as Cisco, Juniper, Arista, Huawei, Brocade / Foundry, etc. without making any change on the existing setup or requiring upgrade to this infrastructure elements.. Solution provided shall provide unrestricted number of Virtual Appliances Licenses to cover our requested total IP Endpoints.. Proposed Solution appliance should support (centralized, distributed and hybrid)



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				architecture.. Proposed Solution should not require any network architecture change . Proposed solution should be deployed without requiring 802.1X for Access Control features. Proposed Solution must integrate with infrastructure devices by using SNMP, CLI. Proposed Solution should support visibility to all the IP enabled devices connected in the network (agentless using Passive and Active Fingerprinting techniques) for both Traditional Endpoints and Industrial IoT Devices. . Proposed solution should not require an agent to perform endpoint profiling, posture Assessment & baselining for full NAC solution features (for managed devices). Agent can be used for managed AD-member Windows endpoints. . Proposed solution should provide information regarding the endpoint connected to the network, such as IP Address, MAC Address, NetBIOS Name, NetBIOS . Proposed solution should support Device tracking (What, Where, Who, When and how). Proposed solution should be capable to provide Post-connect monitoring in an agentless manner. . Proposed Solution Should capable to achieve all feature & functionality with agentless, Agent based & Dissolvable agent mode deployment.. Proposed Solution should provide Visibility & Control into Data Center virtual-machines and its virtualized infrastructure. Proposed solution must support hardware-based and virtual appliance.. Proposed solution should be scalable of supporting 1M+ IP endpoints and managing Layer 2 / Layer 3 devices in non-dot1x mode.. Proposed Solution should support	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				high-availability and clustering.. Proposed solution should allow administrators to review events, do searches, and run reports from a Web UI. . Proposed solution must support the following reporting capability:.. 1- Automatically generate reports on scheduled basis.. 2- Administrators should update or define custom reports.. 3- Ability to run certain reports based on security role. 4- Support scheduled reports be delivered via e-mail. Proposed solution should support event logging via severity. For forensic and faster network troubleshooting, the solution should log each & every session/ all important events that pass through and provide simple graphical and statistical reports. & Logs should be exportable to external log server.. The solution should provide real time alerts via eMail.. Proposed solution should support Role Based Access Control for management. Proposed support alert notification. Proposed solution should support report generation in csv, xls or pdf. Proposed Solution should support creation of custom reports. Proposed Solution should support helpdesk notification. Proposed solution must support non-disruptive, out-of-band model (with all feature & functionality) to ensure network keeps functioning even if the solution goes down for whatever reason.. Proposed solution must support built-in configuration wizards and customizable policy templates for rapid time-to-value.. Discuss how can the proposed solution prevent end-stations failing to meet policy from accessing the network and the alternatives for quarantining and/or fixing computers out of	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				compliance.. Proposed solution quarantine method should not rely on specialized hardware or software.. Proposed solution should support VLAN restriction, Switch port block, Dynamic ACL, Endpoint ACL, Port based ACLs and virtual firewalling.. Proposed solution should support performing Pre and Post admission check, policy recheck. Proposed solution should support Compliance and Remediation abilities. Proposed solution should support Guest Management without requiring additional license.. Describe proposed solution policy configuration options: those configured out of the box (best practices) and the flexibility for the state to customize the solution (status checking methods, breadth of status checking options).. Proposed solution should support automatically detecting new endpoint connected to the network. Please describe how this can be done with proposed solution.. Proposed solution should be cable of identifying virtual versus physical hosts. The solution should be able to identify the vendor of the NIC of endpoints. The solution should be able to identify the switch name and the port on the switch to which and endpoint is connected. Proposed solution should be able to identify the user, email address and IP address of managed devices without requiring an agent through integration with existing LDAP server.. Proposed solution should be able to identify on managed the presence/absence of (without requiring an agent):. Windows Services. Windows process. Open ports. External devices. Dual Home. P2P application.. IM application..	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				Proposed solution should provide IOC scanning to discover and mitigate threats from infected endpoints.. The Solution should be able to identify and classify the Operating System and patch levels installed on managed devices without requiring an agent.. Proposed Solution should support the following User Directory Servers:.. • Active Directory. • eDirectory.. • Sun Directory Server.. • Notes.. • Open LDAP Server.. • Radius Protocol Server.. Proposed solution should support the following Widows OS:.. • Windows10. • Windows 8. • Windows 7. • Windows vista. • Windows 2000. • Windows XP. • Windows Server 2016 Technical Preview. • Windows Server 2012. • Windows Server 2008. • Windows Server 2003 . Proposed solution should support the following MAC OS:.. • OS X 10.6 (Snow Leopard). • OS X 10.7 (Lion). • OS X 10.8 (Mountain Lion). • OS X 10.9 (Mavericks). • OS X 10.10 (Yosemite). • OS X 10.11 (El Capitan). • Mac OS 10.12 (Sierra). • Mac OS 10.13.x (High Sierra). • Mac OS 10.14.x (Mojave). • Mac OS 10.15.x (Catalina). Proposed solution should support the following Linux OS:.. • CentOS. • Debian . • Fedora . • Kali. • Mint. • Red Hat Enterprise Linux. • Red Hat Enterprise Desktop. • Red Hat. • Open Suse. • Suse Enterprise. • Ubuntu. • IGEL. Proposed Solution should support posture assessment of Mac and Linux endpoints while providing an inventory of applications, processes and open ports on an endpoint. In addition, solution should include remediation actions such as kill processes, run scripts, set registry keys or disable dual-homed device adaptors. . Proposed solution should Integrate with	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				LDAP/AD. Proposed Solution should provide built-in method to identify IoT (SNMP / SSH / Telnet) weak and default credentials with ability to add custom credentials to the posture assessment engine. Proposed solution should support Integration with SCCM without requiring creation of any SQL queries (integration should be simple, and out of the box). Proposed solution should support both copper and fiber interfaces (1G/10G).. The solution should support bi-directional information sharing and workflow automation with security technologies such as Advanced Threat Detection (ATD), Vulnerability Assessment (VA), Enterprise Mobility Management (EMM), Next-Gen Firewalls, Endpoint Protection Platforms (EPP) and Security Information and Event Management (SIEM) tools help accelerate system-wide response and achieve operational efficiencies. The OEM should provide a list of all the currently supported integrations.. The Configuration of the solution must be from the vendor by a certified professional service engineer .. توفير الدعم الفني والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لا يندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة .	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	الرقم المميز	الرقم المتتالي	المواصفات	وصف البنود	وحدة القياس	البنود	الرقم التتبعي	الرقم المميز
500	لا	لا	توريد وتركيب الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. توريد وتركيب الرخص اللازمة (150 للخوادم (350خادم). توريد وتركيب الرخص اللازمة للأجهزة الطرفية (150 جهاز). The technology shall support the application whitelisting . and advance threat protection . The techonolgy shall support host firewall . Desktop firewall to control network traffic and protect against attacks. Central management console to monitor and manage endpoints. Antivirus and spyware to scan and remove malicious software. Intrusion prevention to prevent unauthorized access and exploits. Suggested solution must support below client operating systems:. • Android, Apple IOS.. • Windows on Arm devices, Windows in S Mode.. • Windows Vista (32-bit, 64-bit) . • Windows 7 (32-bit, 64-bit; RTM and SP1) . • Windows Embedded 7 Standard, POSReady, and Enterprise (32-bit, 64-bit) . • Windows 8 (32-bit, 64-bit) . • Windows Embedded 8 Standard (32-bit and 64-bit) . • Windows 8.1 (32-bit, 64-bit), including Windows To Go . • Windows 8.1 update for April 2014 (32-bit, 64-bit) . • Windows 8.1 update for August 2014 (32-bit, 64-bit) . • Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (32-bit, 64-bit) . • Windows 10 (32-bit, 64-bit) . • Windows 10 Fall Creators Update (version 1709) (32-bit, 64-bit) . • Windows 10 April 2018 Update (version 1803) (32-bit, 64-bit). • Windows 10 Oct 2018 Update (Version 1809) (32-bit, 64-bit). • Windows 10 June 2019 Update (Version 1903) (32-bit, 64-bit). • Windows 10 Des 2019 Update	توريد د وتر كي ب نظا م مكا فد ة المل فا ت الخ ث Ant ivir us	عد د مكا فد ة الم لفا ت الخ بيث ة	نظ ام مكا فد ة الم لفا ت الخ بيث ة	رذ ص ة	26



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	الوصف	المواصفات	ملاحظات
				(Version 1909) (32-bit, 64-bit). • Windows 10 May 2020 Update (Version 2004) (32-bit, 64-bit). • Windows Server 2008 R2 (32-bit, 64-bit; R2, SP1, and SP2) . • Windows Small Business Server 2011 (64-bit) . • Windows Server 2012 . • Windows Server 2012 R2 . • Windows Server 2012 R2 update for April 2014 . • Windows Server 2012 R2 update for August 2014 . • Windows Server 2016. • Windows Server 2019. • Mac OS X 10.10, 10.11, 10.12, 10.13, 10.14 (including 10.14.5), 10.15. • Amazon Linux 1, 2.. • CentOS 6.X, 7.x, 8.x ; 32-bit and 64-bit. • Debian 6.0.5 Squeeze, Debian 8 Jessie; 32-bit and 64-bit . • Fedora 16, 17; 32-bit and 64-bit . • Oracle Linux (OEL) 6U2, 6U4, 6U5, 7, 7.1, 7.2, 7.3 . • Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U4 , 8. • SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12, 12 SP1 - 12 SP3, 15 64-bit . • SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12 SP3, 64-bit . • Ubuntu 12.04, 14.04, 16.04, 18.04; 32-bit and 64-bit". "Suggested solution must support below Virtual Environments:. • Microsoft Azure . • Amazon Workspaces . • VMware WS 5.0, GSX 3.2 or later, ESX 2.5 or later . • VMware ESXi 5.5 - 6.7. • Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016 Hyper-V, 2019. • Citrix XenServer 5.6 or later . • Virtual Box by Oracle". Solution should able to Detects and blocks malicious software in real time, including viruses, worms, Trojan horses, spyware, Adware, and RootKit.. Endpoint solution technology should include a behavioral based technology apart from providing the signatures for known threats, vulnerability add	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البند	وحدة القياس	وصف البند	المواصفات	ملاحظات
				heuristic based approach. It should be able to score both good and bad behaviors of unknown applications, enhancing detection and reducing false positives without the need to create rule-based configurations to provide protection from unseen threats i.e. zero-day threats.. Solution firewall engine should have option to allow or block support of network protocols, including Ethernet, Token Ring, IPX/SPX, AppleTalk, and NetBEUI. Can block protocol drivers (example: VMware, WinPcap) and should have Adapter specific rules - e.g. Ethernet, Wireless, VPN. Proposed IPS solution should allow customer to edit and create the IPS signature using snort-based format if required.. Solution should able to block devices based on Windows Class ID and should include USB, Infrared, Bluetooth, Serial, Parallel, fire wire, SCSI and PCMCIA.. Solution should also be able to block and give read/write/execute permission for mentioned devices.. Solution should provide application analysis, process control, file and registry access control, and module and DLL control.. "Proposed Solution should be able to deploy flexible and different security policies depending upon the AND/OR relationship of following network triggers:.. • IP address (range or mask). • DNS Server. • DHCP Server. • WINS Server. • Gateway Address. • TMP Token Exists (hardware token). • DNS Name Resolves to IP. • Policy Manager Connected. • Network Connection (wireless, VPN, Ethernet, dialup)". Proposed IPS solution should combines NIPS (network) and HIPS (host) both with Generic Exploit Blocking (GEB) for one signature to	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				proactively protect against all variants, Granular application access control and behavior-based technology mentioned above.. Proposed Anti Spyware solution should be able to bypass Windows File System and should have Direct Access to NTFS Volume to provide raw Disk Scan for superior RootKit protection.. System Lock Down - it should be able to “Locks down” the system by fingerprinting every executable file on the system. It can then monitor all running applications and terminate any application for which the agent does not have a matching fingerprint.. Denial of service detection and protection - Should Protects the system from multiple forms of anomalous network behavior that is designed to disrupt system availability and/or stability.. Anti-spoofing - Should Protects the transmission of data from being sent to a hacker system who has spoofed their IP or Mac Address. Agent has the ability to detect and block process execution chains. It is able to detect when a malicious application tries to execute a trusted application, and then use the trust privileges of that application to access the network.. Anti-application hijacking - Should prevent hackers and web sites from identifying the operating system and browser of individual computers.. Code insertion attack prevention - Prevent malicious applications from inserting code into trusted application to bypass outbound application fire walling.. Protocol adapter attack prevention - Prevent malicious applications from using their own protocol adapter to bypass outbound fire walling.. Anti-Virus Solution	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
					proposed should not have failed Virus Bulletin 100 award ever and should have won the same more than 41 times continuously.. Proposed Personal firewall solution should be on the top on Gartner magic quadrant.. Antivirus and Antispyware policy can have options by default to choose High Security and High performance to have a right balance while deployment in the production network.. Antivirus schedules scans should get delayed/rescheduled while laptops are running on batteries.. Antivirus should have behavior-based technology to scan for Trojans, worms and key stroke loggers to protect from zero-day threats. Sensitivity level of this should get adjusted with customized scanning frequency.. Antivirus Solution should have internet browser protection and home page should be configurable if security risk changes that.. The proposed solution should have email plugin scans attachments, including zip files, removing malware before it reaches the inbox and able to Scan POP 3 email traffic including email clients Microsoft outlook, lotus notes and outlook express.. Desktop Firewall rules should be configurable depending upon the adapters including Ethernet, wireless, Dialup, VPN (Microsoft PPTP, Nortel, Cisco.. Desktop Firewall rules should be configurable depending upon the state of screen saver "ON" & "Off".. Desktop Firewall Policies should be configurable depending upon the time and day.. Product should have readymade policies including -To Make all removable drives read only, to block program from running from removable drives,



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	الرقم المميز	الرقم المتتالي	المواصفات	وصف البند	وحدة القياس	البند	الرقم التتبعي
			protect clients files and registry keys, log files written to USB drives, block modifications to host files. Management server should have the capabilities to add multiple domains if required for the different locations to assign the different administrators for other locations. Each domain should share the same management server and database & This separation prevents administrators in one domain from viewing data in other domains. These administrators can view and manage the contents of their own domain, but they cannot view and manage the content of other domains.. To conserve the network bandwidth clients should be configurable to upload the maximum records of logs to the management server.. Product should have a security setting to block all traffic until the firewall starts and after the firewall stops except initial DHCP & NetBIOS Traffic.. The proposed AV solution should have the capability to detect the files through number of users using that file across the globe.. Browser intrusion prevention: AV should be capable enough to block the malicious downloads thorough browsers.. The proposed AV solution should rank the files based on the digital signature, age of the file, prevalence like attributes. The proposed AV client should have a visible indication whenever it connected to the AV console.. AV console should have a threat con which indicates the virus status on the Public network. The Proposed solution should have the deception feature as part of the Endpoint Agent. The Proposed Solution should have Memory exploit mitigation as a				



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنية	وحدتها	وصف البنود	المواصفات	ملاحظات
				part of the same agent. The proposed solution should have EDR feature using same agent. The proposed solution should be a part of Gartner leader quadrant. The proposed solution should have endpoint deception as a part of the single agent. The proposed solution should have Host Integrity identifies and remediates non-compliant or out-of-date endpoints.. The proposed solution should have effective Advance machine learning in file analysis and behavioral analysis.. The proposed solution should have Host IPS can block and detect internal or outbound network attacks and communications and threats at the browser and network level before they make it to the disk and are executed.. Endpoint agent protected from tampering or disabling.. The proposed solution should have a cloud management console as optional. "Endpoint Detection and Response should Detect, hunt, isolate, and eliminate intrusions across all endpoints using AI-driven analytics, investigation playbooks, and unequaled threat intelligence, and it should be integrated with Endpoint Protection as a single agent. EDR Should have the below features:. Detect and Expose - Reduce time to breach discovery and quickly expose scope . • Apply Machine Learning and Behavioral Analytics to expose suspicious activity, detect and prioritize incidents . • Automatically identify and create incidents for suspicious scripts and memory exploits . • Expose memory-based attacks with analysis of process memory . Investigate and Contain - Increase incident responder productivity and ensure threat containment . •	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسك	البنود	وحدات القياس	الوصف	المواصفات	ملاحظات
				Ensure complete incident playback with continuous recording of endpoint activity, view specific endpoint processes . • Hunt for threats by searching for indicators of compromise across all endpoints in real-time . • Contain potentially compromised endpoints during investigation with endpoint quarantine . Resolve - Rapidly fix endpoints and ensure the threat does not return . • Delete malicious files and associated artifacts on all impacted endpoints . • Blacklist and whitelist files at the endpoint . • Enhanced reporting allows any table to be exported for incident resolution reports . Integrate and Automate - Unify investigator views, orchestrate data and work flows . • Easily integrate incident data and actions into existing SOC infrastructure including Splunk and ServiceNow. • Replicate the best practices and analysis of skilled investigators with automated incident playbook rules. • Gain in-depth visibility into endpoint activity with automated artifact collection ". Respondent should have as part of the platform an End Point solution that allows for detection, validation, and quarantine. All functionality must work on or off of the corporate network and without a requirement for VPN back to the corporate network. The proposed platform must be able to support multiple detection and protection technologies within their solution and should include a signature base engine that leverage on database of known files and their behavior to determine if the file is malicious, without additional payload on file detonation to detect zero day and unknown threats. The	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

اسم الإدارة :

إسم النموذج: خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم	الوصف	البنية	البنية	البنية	البنية	البنية
1	المواصفات	وصف البنية	وحدات القياس	البنية	البنية	البنية
2	المواصفات	وصف البنية	وحدات القياس	البنية	البنية	البنية



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				different network location.. The solution must be able to pass Indicators of Compromise (IOCs) such as file hash, to the endpoint solution so that the endpoint solution could block current and future detection of similar files. Solution should be able to detect Kernel level rootkits. Solution should be able to handle reflective DLL injection. The solution should be able to identify across endpoints if the malicious file presents with different names . The solution must provide a single view of suspicious or malicious files across the endpoints . The solution must provide file reputation based on Intelligence information gathered across the globe to aid remediation and investigation processes. The solution must provide the administrator the ability to submit files for Dynamic Malware analysis. . The solution must provide the ability to whitelist or blacklist files across endpoints . The endpoint agent must support file reputation lookup to EDR servers. The endpoint agent must support blocking, deletion and quarantine of threats. The endpoint agent must not impact the performance of the agent.. The endpoint agent must provide host-based intrusion prevention capabilities to protect against network threats targeting endpoints. The endpoint agent shall provide browser-based intrusion prevention capabilities to the endpoints. The endpoint solution must support a deep environment search for IOCs from all endpoints for files and registry keys as well as domains and URLs. The endpoint solution must be able to blacklist and erase malicious files from a single control plane. The solution	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	الرقم المميز	المواصفات	وصف البند	وحدة القياس	البند	الرقم التتبعي
		must be able to quarantine endpoints from a single control plane to prevent further infection . The endpoint solution must correlate threat and malware information with the existing anti-malware solution and prioritize or de-prioritize EDR incidents based on protection status by the anti-malware solution. The proposed APT solution must also have support for current Endpoint protection as part of the platform that allows for detection, validation, containment and remediation of the Endpoint.. The endpoint agent should integrate with the endpoint protection and not require any new agent to be installed on the endpoint. . The endpoint EDR Solution should be able to remediate the endpoint using the existing Endpoint protection or its own tools.. The endpoint EDR solution should be able to detect the unknown malicious malware and should be able to submit the malware for virtual execution from endpoints independent of the Network EDR solution. . The endpoint EDR solution should be able to detect, validate, contain and remediate the endpoints when the user is on or off of the corporate network and without a requirement for VPN back to the corporate network.. The proposed solution should support containment of the endpoints and containment operations should support role-based Administrators.. The endpoint EDR solution should be able to accept IOC's and threat intelligence dynamically from the devices performing Virtual execution analysis on the network (e.g. Integration with Network and Email based EDR solution). The				



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				proposed solution should have IoC and Threat Hunt queries on clients directly at scale. The endpoint EDR solution must be able to integrate with SIEM.. The endpoint EDR solution must be able to detect the presence of files that have been written to a system but have not been executed.. The endpoint EDR solution may not interfere with normal user and business operations on the endpoint no matter how busy the system becomes.. The endpoint EDR solution must provide regular updates of threat intelligence to include indicators involving highly advanced threat groups in state-sponsored targeted attacks.. The endpoint EDR solution upgrades must be supported by standard enterprise software deployment mechanisms as well as the ability to perform upgrades to endpoints within the solution itself.. The Solution provider should allow the submission of suspicious sample for analysis at the click of a button from the solution to avoid Potential False positive . The solution should support the bare-metal and virtual execution sandbox to detect the virtual aware new gen threats.. The implementation of the solution should not add any new agent and should be part of the endpoint protection to the endpoint machine.. The Proposed solution should support flight data recorder . The proposed solution should comprehensive App discovery and inventory to scan and inventories all the apps and files collected from all the endpoints in the environment and provides detailed information about each app and file, including the name, risk score, vulnerability score,	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البند	وحد القياس	وصف البند	المواصفات	ملاحظات
				publisher, reputation, number of devices it is seen on, and so on.. The proposed solution should comprehensive application control policy and easy Policy Creation with Logical View to add any application from discovered App to white or black list.. Endpoint App Control enables trust in apps, based on a variety of app attributes, allowing or blocking apps based on one or a combination of any number of static (e.g. hash, path, publisher and certificate) and dynamic (e.g. risk and reputation score) attributes.. The App Control policy should enable rule creation on a broad range of parameters that include app name, path, and hash, reputation, publisher, user, user group, and command-line parameters.. The App Control policy should have an option to enforced in “monitor only” mode.. The proposed solution should analyze the difference between what the applications allowed in the environment and what applications run in the environment. . The proposed solution should enable to define trusted updaters which can be from discovered apps or new apps, publisher, directory, files, users, and user groups, that can install or update the software on the endpoints.. The proposed solution should prevent trusted apps from being exploited and prevent untrusted apps from infecting systems.. "The proposed solution should have application behavior Isolation rules capabilities to protect our devices and these rules allow or block certain application behavior, as the following isolation types. . • Browser isolation (Google Chrome, Firefox, Internet Explorer, Microsoft Edge). •	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

اسم الإدارة :

إسم النموذج: خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم	الوصف	البنية	البنية	البنية	البنية	البنية
1	المواصفات	وصف البن	وحد القياس	البن	البن	البن
2	Office isolation. • PDF Renderer isolation. • Platform isolation policy, which includes the following: - o OS settings. - o Generic jail settings (high, medium, and low isolation). The isolation provides rules to protect the following: • Registry protection. • File protection. • Process interaction protection. • Process execution protection. • Network access protection. • System call protection". The proposed solution should detects any suspicious files in our network based on the intensity levels and enable us to add the detected files to whitelist or blacklist and enable us to isolate a suspicious application with a Platform Isolation policy.. The proposed solution should have ability to discover, inventory and isolate portable applications based on risk rating.. The proposed solution should have deception feature with deploying a wide variety of 'bait' - fake files, credentials, network shares, cache entries, and endpoints - throughout your environment.. The proposed solution should have endpoint deception as a part of the single agent. The proposed solution should have utilize deception techniques to monitor and notify of malicious application behavior.. The proposed solution should be supporting IOS and Android Devices. The proposed solution should prevent attacks on mobile devices running iOS and Android.. The proposed solution should proactively protecting the mobile devices from malware, network threats, and app/OS vulnerability exploits, with or without an Internet connection.. The proposed solution should have capability to enable us to take faster reaction and constant					



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				protection, even when devices are disconnected from the Internet.. The proposed solution should Proactively thwart attacks, immediately and automatically when a threat is detected.. The proposed solution should target the exact threat without impacting other resources or processes, and kick in on-demand.. The proposed solution should have protection action against risky apps threats including but not limited to (blocking communication, preventing installation, blocking communication with malicious command-and-control (c&c) servers, and blocking access to sensitive resources). The proposed solution should have protection action against network threats including but not limited to (network automatic launch of VPN tunnel when network threat is detected, blocking access to sensitive corporate resources, and blocking access to fake corporate wi-fi hotspots).. The proposed solution should have protection action against content threats including but not limited to (tunnelling all traffic through a secure web gateway, blocking access to unwanted content, and blocking SMS phishing messages).. The proposed solution should have protection action to automatically disconnect malicious VPNs. The proposed solution should have VPN technology can be implemented in always-on or on-demand mode.. "The VPN technology in the proposed solution should have the capability to operate in two ways: . 1. as an encrypted tunnel through which traffic passes securely between the device and a network.. 2. as a selective traffic blocker. (specific traffic passing	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				through the VPN is dropped and never leaves the device).. Each of these implementations can be always-on or on-demand.". The proposed solution should have Multi-layered mobile defence against known, and zero-day attacks across every mobile threat vector.. The proposed solution should have protection from suspicious networks, apps and behaviors before they can do harm.. The proposed solution should protect privacy and productivity without negatively impacting mobile experience or battery life.. The proposed solution should have automated IT policy enforcement and built-in integrations with all major existing enterprise EMM/ MDM, SIEM, email servers and VPNs.. The proposed solution should have capabilities to integrate with many security solution including but not limited to WSS, CASB, DLP and Endpoint protection. The proposed solution should easy to deploy, adopt, maintain and update.. The proposed solution should zero impact on productivity, experience, privacy and deep analysis of suspicious apps.. The proposed solution should have real-time response and protection against various known, unknown and targeted malware attacks from any suspicious apps and networks.. The proposed solution should have automated corporate asset protection when under attack.. The proposed solution should have a reputation check capability with machine learning for apps, networks and OS.. The proposed solution should have comprehensive activity logs for integration with any SIEM solution.. The proposed solution should have app analysis	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				capability based on signature, static/dynamic analysis, behavior, structure, permissions, source and more.. The proposed solution should have detection, blocking and remediation of malicious IOS profiles.. The proposed solution should have capability to identify Man-in-the-Middle, SSL downgrading and content manipulation attacks without violating privacy.. The proposed solution should have capability to monitoring devices for unpatched known vulnerabilities and uncovering zero-day vulnerabilities in apps and operating systems.. The proposed solution should provides mobile threat defense for modern operating systems without relying on a 3rd party. The proposed solution should addressing stealthy attacks or APTs with effective Active Directory defense from the endpoint to provide autonomous breach containment, incident response, and domain security assessment.. The proposed solution should autonomously capability to learn the organization's Active Directory structure in its entirety (servers, endpoints, applications, users, branches, naming conventions, configurations, attributes etc.). The proposed solution should able to create an authentic and unlimited obfuscation.. The proposed solution should able runtime evaluation of processes, context and Active Directory activity is evaluated.. The proposed solution should have a high-fidelity alert and the capability to is automatic to blocking the attack.. The proposed solution should provide a real-time forensics reporting that captures actual reconnaissance, credential theft, and lateral movement phases that were	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البند	وحد القياس	وصف البند	المواصفات	ملاحظات
				performed by the attacker and documenting the attacks chain.. The proposed solution should able to automatic mitigation stops the malicious process on the endpoint to contain the breach in real-time, removing its ability to spawn another process, overwrite another part of memory, run reconnaissance commands, or communicate out to the network.. The proposed solution should have the capability to continuously probes for domain misconfigurations, vulnerabilities, and persistence, and present the domain from the attacker's perspective, and allowing for immediate risk mitigation.. The proposed solution should prevent lateral movement with AD protection and ML based deception technology. The proposed solution should have an automated assessment process uses attack simulations to gather in-depth information about the configuration of the domain, privileged accounts, security settings, GPO, endpoints, domain controller, and Kerberos.. The proposed solution should have autonomously analyzes every component of the domain and Active Directory structure for misconfigurations and backdoors in AD and the entire domain environment.. Solution should be deployed, administered and updated in a single agent package and update mechanism. There should not be any need for multiple deployment of agent & to get the updates to achieve the all product functionality required above. . The proposed solution should have cabapilty to deployment in Cloud, On-Prem, and Hybrid options. Find unmanaged endpoints and deploy single	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البند	وحدة القياس	وصف البند	المواصفات	ملاحظات
				lightweight agent for complete protection.. Security and compliance check both should be managed by a single administration management server and console.. Solution should provide integration with RSA for management console authentication addition to the user credential authentication if required and also should get integrated with LDAP, Syslog, and Active Directory.. The Management servers installed at different locations should have the ability to replicate data, logs and content at defined interval in Multi-Server Architecture with Policy and Log Replication.. The agent should be able to password protect uninstall, password for disabling service and password to open the client GUI so that users will not be able to uninstall the agent.. Agent should have the ability to protect the service from being stopped, even if an administrator logs on.. Update mechanism should include client content updates from management server, internal update servers, external vendor update servers, also from the client that acts as a proxy between a management server and clients in the group and using Third-party tools like Microsoft SMS.. Proposed AV solution should have . . . a single and the same agent for physical and Virtual clients الدعم الفني لا يندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) . . . توفير ورش عمل لنقل ومشاركة المعرفة لتشغيل وتركيب النظام..	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الغرض	البنية	وحدة القياس	وصف البند	المواصفات	ملاحظات	الرمز	الاسم	الرقم
27	نظام جدار حماية التطبيقات	نظام	عدد	توريد وتركيب أجهزة حماية تطبيقات الويب WAF الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: 9. Solution must provide analytics capability for device groups in synchronization with improvement in management and visibility with stats notification.. 10. Solution must be able to define and control how traffic is distributed across links, based on real-time traffic flows and throughput.. 11. Solution must be able to automatically build different policies for different applications and rapid deployment based on detected traffic with combined detection and prevention techniques.. 12. Solution must be able to update all signatures and protection mechanisms and licensing in totally isolated environment. 13. Solution must provide automatic self-learning and creation of security polices with versioning capability of the configured policies and rollback.. 14. Solution must provide SSL offloading capability with storing private keys in secure mechanism with capability for tuning SSL parameters.. 15. Solution must provide session tracking mechanisms that enhanced enforcement and reporting capabilities that take into account user sessions and application user names within the application.. 16. Solution must provide request and response logging that support profile by enabling configuration log entries to be reported when requests/responses are received.. 17. Solution must provide protection of AJAX-enabled applications	لا	2			



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البند	وحد القياس	وصف البند	المواصفات	ملاحظات
				including those that use JSON for data transfer between the client and the server. 18. Solution must provide virus checking on HTTP file uploads and SOAP attachments. Support to Anti-Virus via ICAP communication channel.. 19. Solution must provide XML Web Services access restriction methods defined via Web Services Description Language (WSDL) or XML Schema format (XSD). 20. Solution must provide XML Parser Protection, limit recursions to thwart DoS conditions, limit the numbers of elements, lengths of elements, attack signatures enforcement.. 21. Solution must be able to perform information display masking/scrubbing on requests and responses.. 22. Solution must be able to perform restrictions and filtering based on values and lengths of URL, filetype, parameters, methods, encoding in headers and response, cookies, and body content for all type of HTTP protocols.. 23. Solution must be able to monitor latency of Layer 7 (application layer) traffic to detect the spikes and anomalies in the typical traffic pattern.. 24. Solution must be able to integrate with vulnerability management tools and provide virtual patching capability.. 25. Solution must be able to provide protection based on all OWASP defined vulnerabilities . توفير الدعم الفني والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لا يندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	الرقم الفني	الوصف	المواصفات	ملاحظات	الرقم التتبعي
28	ظام	نظام	توريد وتركيب نظام كشف الملفات المتقدم عبر الشبكة Host Sandboxing الحلول مع كامل مستلزماتها . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: يجب ان يكون للجهاز القدرة على الوصول الى الملفات و فحصها من خلال البرتوكولات التالية: - - NFS. - CIFS WebDAV. - Secure WebDAV . يجب ان يكون الجهاز بالمواصفات التالية: - - Hard Disk 4 x 2 TB HDD, 3.5" RAID 10. 2RU rack mount. - Up to 50,000 Network Interface Ports:2 x Gigabit Ethernet ports. - Up to 50,000 files per day .توفير الاشتراك في scanning content on file servers and sharepoint servers . توفير الدعم الفني والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة	لا	2



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الغرض	البنود	وحدة القياس	وصف البنود	المواصفات	ملاحظات	الرمز	الترتيب
29	زخام	نظام	عدد	توريد	"يجب توريد وتركيب نظام كشف الملفات المتقدم عبر الشبكة Network Sandboxing الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: . يجب ان يكون للجهاز القدرة على العمل . . Network . توريد وتركيب عدد 4 نظام حماية الشبكات. Signature-less Detection Capability using Virtual Machine Based Dynamic Analysis. . The. proposed solution should have IPS capabilities. . The proposed solution should have Riskware. detection capabilities. . The solution must detect Zero-Day and APT attacks.. . The solution. should support IPMI. . It should support two management ports. . The proposed solutions should. be certified by the US Department of Homeland Security SAFETY Act Certification. . The. solution must utilize custom Virtual Machine (on-premise) technology to positively identify. malware, including zero-hour vulnerability exploits, polymorphic payloads, and obfuscated javascript.. The virtualization solution must not be detectable by malware in order to avoid evasion.. They Hypervisor must not be an OEM solution such as from VMWare or others. . The solution. has to be capable of automatically downloading threat intel from an intelligence cloud. . all static. analysis will occur in the appliance including: IPS, custom signature, Riskware, CnC rule. matching and others. . The solution should support inline monitoring and blocking (not only TCP. Reset). . The solution OS software must but capable of being automatically updated	لا		2



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

اسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتالي	المواصفات	وصف البند	وحدة القياس	البند	الفترة	المرجع
١	from the. Web management GUI. · The solution must be able to run multiple Micro Tasks in a single VM. (e.g. run sample across multiple versions of Adobe Acrobat in a Single VM Execution). · The. solution must be administered through a web-based console that doesn't require the installation of. additional software.. · The solution must allow the creation of accounts with different roles used. to administer the solution, or just monitor the alerts.. · The solution must allow the authentication. to the console by using authentication services like RADIUS, TACACS+, LDAP and LDAPS.. · . The solution should support remote administration using CLI and GUI (Web Console). · The. solution must be able to detect and report web exploits by using multiple versions of web. browsers and plug-ins.. · The analysis must be performed runtime in order to detect all the. malware actions, even the ones that fail in the virtual environment but might be successful on a. client workstation. Before and after differential Comparison or VM state is not acceptable.. · For. the list of applications supported in the VM's the Vendor must have a method for pushing updates. to the list of applications dynamical to the appliance without requiring a full OS or solution. upgrade.. · The solution must allow the configuration of an ACL to control access to the. management interface. · The solution must be able to utilize NetBIOS and DNS for hostname. resolution when generating alerts.. · IPS Detection of Reconnaissance Activity. · IPS Detection of. Brute Force Attacks. · IPS Uses Dynamic Analysis Engine (VM) for IPS alert validation					



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البند	وحد القياس	وصف البند	المواصفات	ملاحظات
				and. correlation. · The solution should support remote administration using ssh and https. · The. solution must be able to detect and report malware downloaded by users, or downloaded in the. context of a web exploit by using multiple client operating systems with multiple service pack. levels running on both x64 and x86 architectures.. · completely unknown vulnerabilities across. protocols and applications.. · The solution must be able to detect all three stages of the modern. malware's attack lifecycle, while highlighting every stage of the attack: Exploit, Dropper & Data. Exfiltration. · Solution should use customized hypervisor and should include instrumentation. running within itself for run-time detection analysis. · Solution should be able to handle reflective. DLL injection. · Solution should be able to detect Kernel level rootkits. · Solution should be able. to handle packed payloads. · Solution should be able to deal with VM evasion techniques. ·. Solution should have the ability to remain fully effective when configured to share no data,. events, nor any information with vendor or the vendors network.. · Solution should have the. ability to detect client-side EXPLOITS prior to any complex malware being downloaded to the. systems; complex malware is defined as malware with complex abilities such as key-logging,. data-stealing, encrypting, migrating, and installing additional complex malware.. · The solution. must be capable of blocking reliably outgoing communications to CnC servers in order to. conserve data integrity on hosts including out of band infections. · The solution	



رقم الكراسة :

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التسلسلي	الوصف	البنية	البنية	البنية	البنية	البنية
1	المواصفات	وصف البنية	وحدة القياس	البنية	البنية	البنية
2	المواصفات	وصف البنية	وحدة القياس	البنية	البنية	البنية



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	الرقم	البنية	الوصف	المواصفات	ملاحظات
30	د	م	تقويم مستوى نضج الامن السيبراني اعتمادا على مرجعية هيكلية الامن السيبراني للذكاء الاصطناعي متوافق مع متطلبات العمل الاتية: . a.Conduct gap and maturity level assessment (CMMI Maturity Levels) and define the As-Is and To-Be states on the AI Cybersecurity Architecture covering each building block.. b.Provide recommendations on how to fill the gap between current and target state and ensure flexibility and robustness for .all new technologies	خد ما ت است شارة	1



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التسلسلي	الفئة	البند	وحدة القياس	وصف البند	المواصفات	ملاحظات
31	زخم	نظام الحقن من نزهة المفاصل لتزامم	عدد	توريد وتركيب وتدريب نظام مراقبة الامتثال (Check & Security Compliance Check) . • توفير خدمات احترافية لنظام (FILE INTEGRITY MONITOR&Security Compliance Check) . • تركيب النظام (FILE INTEGRITY MONITOR&Security Compliance Check) . • توريد وتركيب الرخص اللازمة للخوادم (500 خادم). • توريد وتركيب الرخص اللازمة لأجهزة الشبكة (50). • توريد وتركيب الرخص اللازمة للامتثال والالتزام (2). • توريد وتركيب الرخص اللازمة (ESXi 2) . الدعم الفني لا يندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. • توفير ورش عمل لنقل ومشاركة المعرفة لتشغيل وتركيب النظام.(8 موظفين).	لا	1



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	الصفة	البند	وحدة القياس	وصف البند	المواصفات	ملاحظات
				MO NIT OR &Se cur ity Co mp lian ce Che (ck		



رقم الكراسة :

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	الوصف	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية
36	توفير خدمات لمراجعة الاعدادات للتقنيات الرقمية لمدة 200 يوم عمل . توفير خدمات تقييم فجوات امنية لتقييم البنية التقنية والانظمة مع تقييم المخاطر السيبرانية . توفير خدمات امنية لتقييم اختبار الاختراق لعدد 50 نظام او تطبيق و 300 عنوان شبكي و . تطوير خطة معالجة تقنية و وتشغيلية	خدمات احترافية استشارية للامن السيبراني	خدمات احترافية استشارية للامن السيبراني	خدمات احترافية استشارية للامن السيبراني	خدمات احترافية استشارية للامن السيبراني	خدمات احترافية استشارية للامن السيبراني



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	الرقم الفني	الوصف	المواصفات	ملاحظات
33	خ	تطوير إطار مرجعة هيكلية الامن السيبراني متوافق مع متطلبات العمل حسب المتطلبات الفنية الاتية: . Develop the AI Reference Cybersecurity Architecture based on the AI UCF (defined in the previous activity), Threat Catalog, and business needs. The vendor shall:. a.Develop Threat Catalog including threats, actors (adversaries), motives, methods, risks and scenarios for each Use Case defined in Activity. b. Develop AI Reference Cybersecurity Architecture (AI RSA) following SABSA framework up to level three (logical level). The AI RSA shall comprise cybersecurity capabilities (Security Ser+F10vices in SABSA terminology), security drivers, potential threats, the existing related security solutions for each capability, and integration patterns for each domain.. develop cybersecurity rules and standards for each capability (up to 10 security rules for each capability).. d. Map the capabilities to the controls in the AI UCF defined and unified Reference security architecture . . E. The vendor must doing the required assessment with developing the required toolkit with take .approval from the Cybersecurity and relevant dept	تطوير إطار مرجعة هيكلية الامن السيبراني متوافق مع متطلبات العمل حسب المتطلبات الفنية الاتية: . Develop the AI Reference Cybersecurity Architecture based on the AI UCF (defined in the previous activity), Threat Catalog, and business needs. The vendor shall:. a.Develop Threat Catalog including threats, actors (adversaries), motives, methods, risks and scenarios for each Use Case defined in Activity. b. Develop AI Reference Cybersecurity Architecture (AI RSA) following SABSA framework up to level three (logical level). The AI RSA shall comprise cybersecurity capabilities (Security Ser+F10vices in SABSA terminology), security drivers, potential threats, the existing related security solutions for each capability, and integration patterns for each domain.. develop cybersecurity rules and standards for each capability (up to 10 security rules for each capability).. d. Map the capabilities to the controls in the AI UCF defined and unified Reference security architecture . . E. The vendor must doing the required assessment with developing the required toolkit with take .approval from the Cybersecurity and relevant dept	1



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	رقم التمسلي	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
34	خ د م ة	خدمة احترافية واثباتية	شهر	خدمات احترافية لتطوير وتحسين الخدمات الاتية : Identity access Managment Gap Assessment Report . Roadmap and Implementation Plan including all Recommendations . User Data Requirements Analysis Report for IAG . Document detailing Roles and Responsibilities and RACI for IAG . Processes, procedures, and guidelines . Workflows and Forms . IAM Use Cases 30 . PAM use cases 30 .		8



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	الرقم الفني	الوصف	المواصفات	ملاحظات	الرقم التتبعي
35	أجهزة	توريد	يجب توريد وتركيب الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: Solution must be at least 4 ICAP servers distributed in two datacenters. - Solution must be at - least with 20 Engines scanning capability through 6 different dedicated servers distributed in two datacenters. - Solution must support - Solution must support Core technology enablement (CDR, DLP, multi-scanning, etc.). - 24x7x365Maintenance & Support for 3 years. - solution component to be implemented in two different datacenter sites.. The solution should support both Windows Client and Server versions. The solution should support Chrome, Firefox, Safari, Internet Explorer and Microsoft Edge for the management console. Web access to the platform should be via https protocol. The solution should support RBAC . The solution should be able to integrate with SIEM or syslog servers. The solution should provide auditable record of files and emails that has been scanned. The solution should be able to run in air gapped environments. The solution should be able to work in a network connected mode. The solution should expose APIs for integration purposes. The exposed APIs have to be officialy documented. The solution should connect to only one URL to download the new signature definitions. The solution should support signature definition upload previously downloaded from an internet connected machine. The engine and virus definition	لا	1



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				update mechanism should support internet, manual and folder mode. The solution must provide a single pane of glass for central configuration. The solution should integrate with syslog/SIEM systems. The solution must allow the creation of accounts with different roles used to administer the solution, or for auditing purposes. The solution should provide Active Directory and LDAP group-based administrative roles. Solution should have its logs archived locally, and they should be downloadable via the GUI. The solution should support remote administration using RDP and https. The solution should provide built in database. The built in database management should be done from the product user interface. The solution should allow configuration export and backup. The solution should be able to provide 30+ different AV engines . The solution should use signature based detection. The solution should use heuristic based detection. The solution should use machine learning based detection. The multiple AV engines should be able to run in a multithreaded way. The solution should be able to support complex archive processing and extration. The solution should support over 30 different archive types. The solution should allow configuration of the archive handling process. The solution should be able to process password protected archived/files. The detection should run fully on premise with no cloud connection. There should only be 1 licensing component for all the multiple AV engines. The different AV engines have to run in an airgapped environment. The	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				frequency of the signature definition updates has to be configurable. The signature definitions have to all come from one single point. The solution should be able to detect known vulnerabilities in binary data. The solution should be able to integrate inline with 3rd party security controls. The solution should be able to quarantine malicious sample for further analysis. The solution must allow disabling AV engines to exclude them from scanning. The solution should provide a false positive configurable threshold . The solution should be able to provide a known vulnerabilty assessment technology. The solution should detect Vulnerable Installers. The solution should detect IoT Software and Firmware Vulnerabilities. The solution should provide a file type detection technology. The solution should provide a YARA module. The solution has to be able to integrate via REST API. The REST API has to be JSON based. The solution should detect spoofing of over 4,500 file types and block spoofed files. The solution should support extraction for the follwing archive types: Zip, 7z, Jar, rar, rar5, tar, ISO, Gzip, CAB, ARJ, LZH, RPM, DEB, LZMA, WIM, SFX, XZ, VDI, VHD, MBR, CPIO, HFS, .apk .gz .msi .tgz .tbz, bz2. The archive extraction mechanism should be configurable. The solution should process Microsoft Office Documents as archives. The following self extracting archives should be supported: 7zip, WinRAR, PKZIP, IExpress. The solution should be able to blacklist/whitelist by hash, filename, filetype or mime type. The solution should be able to quarantine blocked	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
					files. The quarantine should have the option to integrate with MetaDefender Cloud for Threat Intelligence. The solution should allow different workflow rule configuration to customize the order and process in which files are handled. The solution should provide the option to integrate inline with a 3rd party security control (external scanner). The solution has to be able to integrate with SMB compatible storage (Platinum Support (الصيانة والدعم غير مندرجة تحت الضمان حسب متطلبات وزارة التجارة).



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الغرض	البنية	وحدة القياس	وصف البند	المواصفات	ملاحظات
36	ز	نظ	عد	توف	. يجب توريد وتركيب الحل التقني لأتمتة التقنيات الامنية بالشبكة وغيرها NETWORK POLIY ORCHESTRATION AND ASSURANCE مع كامل مستلزماتها. . توفير الحلول اللازمة لمدة 3 سنوات. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة (8 موظفين). يجب الالتزام بالمواصفات المطلوبة حسب الآتي: Network Policy Orchestration & Assurance Integration with Firewall for 20 and 50 network devices. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: The proposed system should be deployed in two data centers. Also, it should be deployed by the Professional Service team from the mother company.. Bidder should provide HLD , LLD , Operation Guides for End-user and Admins , Minimum Baseline Security Standards , and test uses cases in SDAIA template documents.. The proposed system should be virtual based.. The proposed solution should be able to integrate with SIEM tool and forward all the logs and events to the SIEM solution.. The proposed solution should support multi tiers architecture. . The proposed solution should support Single Sing On.. The proposed solution should support integration with Active Directory (AD), Network Time Protocol (NTP) and Domain Name System (DNS).. Bidder should provide all the required commu ation matrix for the proposed solution.. Bidder should provide the data flow of the proposed solution.. The data should be encrypted in transit.. The data should be encrypted at rest.. The proposed solution should support RBAC model for separation of duties and data.. The	لا



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				proposed solution should be able to integrate with Multi Factor authentication solution (MFA).. The proposed solution should be highly available. The solution should support automatic replication between the solutions in two data centers.. The proposed solution should support integration and not limited to Palo Alto, Cisco, Fortinet, Juniper firewalls (VM, VSYS and Appliances) ,Load Balancers , and WAF . All functionality of the proposed solution's platform should be tightly integrated and operated from a single pane of glass. . The proposed solution should support user customizable query language, which allows the user to perform a variety of tasks . The proposed solution should store unlimited versions of firewall configurations with all changes detected and stored in encrypted database. . The proposed Solution should support continues real-time monitoring and detection of all changes.. The proposed solution should provide a Device Dashboard where information on Rule Usage is displayed and the top used rules should be listed based on percentages in descending order. . Used and Unused Rules:. In addition to the detailed rule usage and object analysis information, the proposed solution should provide information to help optimize the operation of a policy. . The proposed solution should also highlight which rules have seen no activity at all, to help chart a remediation path for the removal of unused rules and reduce policy complexity while increasing security posture. . Redundant / Shadowed Rules:. The proposed solution should	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الرقم الفني	الوصف	المواصفات	ملاحظات
			provide a standard report for identifying redundant and shadowed rules with details that indicate the portion of the rules that causes the redundancy. Users can configure the varying level of redundancy and overlap.. Rule Consolidation:. The proposed solution should provide a standard report that displays security rules on the firewall that may be safely consolidated without changing the behavior of the policy.. The proposed solution should Support Real-Time change analysis and reporting for the monitored Firewalls.. The proposed solution should provide security compliance reports utilizing built-in and customized security controls. . The proposed solution should include extensive policy rule search capabilities and global search functions across multiple policies. Additionally, reporting and compliance checks provide the ability to customize a report to see if a specific object is allowed. This can include IPs, networks, groups, zones, or services. The proposed solution should support real-time compliance custom and assessment dashboard.. The proposed solution operating system should be hardened. . The proposed solution should have ability to Identify any unused rules, unused network objects and unused service objects in existing policies to prevent gaps and reduce unnecessary complexity.. The proposed solution should provide reports for rule consolidation.. The proposed solution should provide Object usage like ports and IPs within the Rule for Clean-up.. The proposed solution should support Creation of custom controls and assessments to identify	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البند	وحد القياس	وصف البند	المواصفات	ملاحظات
				automatically rules for clean-up and recertification.. The proposed solution should provide comprehensive network mapping for managed devices. . The proposed solution should store the data on encrypted disk.. The proposed solution should provide Rule usage in time query capabilities and visualization on histogram.. The proposed solution should have the ability to normalize firewall rulesets for single consistent view across multiple vendors.. The proposed solution should have the ability to generate custom reports and queries.. The proposed solution should provide built-in security policies and baselines based on security best practices. . The proposed solution should support multi-vendor next generation firewalls. . The proposed solution should be able to read and analyze existing policies for managed devices upon deployment. . The proposed solution should support Custom assessments can be run for specific device group or all devices if required.. The proposed solution should provide out of the box compliance reports like ISO 27001, NCA ,CSA etc compliance report generated for individual Firewall and Groups of Firewalls. The proposed solution should provide full audit logs for any system changes. . The proposed solution should support Policy and Rule Documentation for all integrated Firewalls & network devices.. The proposed solution should support Role base access with Granular privileges definition limiting user group access to specific system functions/interface (i.e. dashboard, configuration, change management) as well as functions within	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				particular systems limited to selected device groups or all devices.. The proposed solution should be able to automate and generate reports via email. . The proposed solution should provide user-friendly web interface based on HTML 5. . The proposed solution should support multi-user roles/privileges. . The proposed solution should support authentication of users using RADIUS, AD, LDAP. . The proposed solution should provide web user interface that is compatible with modern web browsers (Internet Explorer, Firefox, and Chrome). . The proposed solution should support single and distributed environment for deployment. . The proposed solution should support Fully customizable Web-based dashboard with customizable metrics, defined using security information query language, including NAT rules. The proposed solution reports and notifications are to be available in a minimum of the following formats HTML, PDF.. The proposed solution should support all functionality through REST-API.. The proposed solution should provide recommendations to fix overly permissive rules. . The proposed solution should allow admins to develop customized controls for security analysis. . The proposed solution should have the ability to graphical mapping and simulating traffic path flow. . The proposed solution should support full-fledged Workflow based Firewall Rule Change Management.. The proposed solution should provide Firewall policies management, Audit and Compliance management as well as automated change management and recertification process	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
					and workflow.. The proposed solution should have the ability to push the configuration directly on the firewalls without needs to firewall management station.. The proposed solution should have the ability to connect read/write with and without centralized firewall managers including Panorama, Cisco FTD, Fortinet Manager. The proposed solution should have the ability to manually and automatically remove deactivated rules. . The proposed solution should provide Firewall policies management, Audit and Compliance management as well as automated change management and recertification process and workflow. . The proposed solution reports and notifications are to be available in a minimum of the following formats HTML, PDF والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) ..



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الرقم الفني	الوصف	المواصفات	ملاحظات	الرقم التمسلي
37	اجهزة	توريد	يجب توريد وتركيب الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي:.. NGFW should cover interconnectivity for the chosen zones.. NGFW should have capability to interconnect through 40Gbps and QSFP interfaces with at least 4 interfaces on each firewall .. NGFW should able at least to handle 50 Gbps throughput as stateful without applying SSL/IPS inspection and 25 Gbps with IPS inspection.. NGFW should able to integrate with environment and be integrated with proposed network security orchestration solution.. NGFW should including the all hardward parts and passive components such as cables,SFP,Stand, etc.. the lincses should be provided for 3 years including the all security function IPS, SSL, Threat feeds, and advanced support. 7. Redundant FANs and Power supply اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة (8 موظفين)	لا	5



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التمسلي	الرقم الفني	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات	الرمز	الكمية
38	رخصة	نظام الكشف والاستجابة	عدد	توريد وتركيب واختبار وتنفيذ وصيانة	Three-years EDR software subscription expansion for 500 endpoints with . - solution component to be implemented in two different datacenter sites.. - 24x7x365Maintenance & Support for 3 years. On premise EDR solution with capability to work as mutitenancy to improve security operations productivity and enhance detection and response capabilities by including more security components into a unified whole that offers multiple streams of telemetry, presenting options for multiple forms of detection and concurrently enabling multiple methods of response. . Centralization of normalized data, Correlation of security data and alerts into incidents. A centralized incident response capability . . Allows deep visibility into all endpoint activity - in real time and retrospectively.. . Simplifies threat hunting and detection.. . Prevents threats through your preferred AV engine and process blocking.. . Automates response with pre-built scripts and playbooks.. . See all endpoint activity across Windows, Mac, and Linux systems and gain unmatched insight through the collection of all executable files and scripts that are analyzed against the latest threat intelligence. . . Detect threats in real time or hunt retrospectively through recorded events. . . Monitor a full software inventory and identify vulnerabilities with links to MITRE CVEs or Microsoft KB Reports.. . View all process data, user activity, registry events, file system activity, and memory data and more.. . Review full software inventory and	لا	500	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التسمية	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				known CVE and KB vulnerabilities. · Collect executable files and scripts for analysis and threat hunting.. · Create and save advanced queries using Boolean logic.. · Monitor endpoints in real-time and retrospectively, on and off the network. · Monitor key events with playback analysis to automatically deliver an incident timeline, along with prioritized alerts.. · The solution must be able to automate response with scripts and playbooks, including the ability to isolate endpoints, terminate processes, remove files, and deploy custom scripts. · The ability to start investigations with memory analysis, vulnerability scans, and system inventory. The ability to capture data and memory and full disk images, as well as the ability to remotely access endpoints to view and take action on files and processes.. · The ability to take action and automate response with a customizable library of scripts and playbooks. · Collect forensically sound data in real time for deeper investigations.. · Remotely access and control endpoint file systems and processes. · Integrate with SIEMs, NGFWs, etc., to execute response actions.. · Maintain full control of endpoints with full remote shell capabilities.. · Endpoint threats must be mapped to MITRE ATT&CK™ to allow SDAIA analysts to see the TTPs in use and to determine the proper response. Untrusted executables are automatically sent to SDAIA sandbox and can be integrated into process blocking (IOC, hash, and YARA rules).. · The solution must support Windows, Linux and MacOS for agents installations. · The solution must automatically collect executables	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				and script file at the first time executed in the environment. · The solution must automatically and dynamically collect installed software on all endpoints and alert against any identified CVE. · The solution must record process activities (process start, image load, process access, service and process exit) in real time. · The solution must record when a process creates a remote thread in another process, or when a thread is created in the current process by another process. · The solution must be able to ingest open source IoCs and YARA rules and use it to run scans on target endpoint(s). · The solution must allow users the ability to query across collected endpoint behaviors and must support saving search queries. · The solution must have Advanced Query Builder to allows for users to craft queries that include Boolean logic, targeting of endpoint groups for inclusion/exclusion, and assists users in creating these advanced queries that are useful for investigation, behavior rule creation, and threat hunting. · The solution must record connected endpoint(s) information including but not limited to: host name, IP Address, processor, memory, OS, OS version and last connected time. · The solution must be able to dynamically update recorded connected endpoint(s) information. · The solution must support endpoint grouping (static groups, dynamic groups and imported groups). · The solution must be able to show endpoint related task results, alerts, USB activities, login history and installed software as part of the endpoint record.. · The solution must support Multitenant	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				architecture. The solution be compliant with CSDC EDR technologies . Share knowleged must be provided الدعم (Support Platinum Plus) الصيانة والدعم غير مندرجة تحت الضمان حسب متطلبات وزارة التجارة	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

الرقم التتبعي	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية	البنية التحتية
---------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البند	وحدة القياس	وصف البند	المواصفات	ملاحظات
				العمل مع الأدوار والمسؤوليات بين المزود والمنظمة، والتفاعل مع أمان المعلومات، واتفاقات مستوى الخدمة والكتب العمل، وإجراءات التصعيد. • يجب على مقدمي خدمات الأمن المُدارة توفير خدمات استخبارات التهديد المُدارة باستخدام مصادر مفتوحة بهدف فهم أحدث التهديدات السيبرانية، في أقرب وقت ممكن بناءً على المخاطر والوضع الأمني. • يجب على مقدمي الخدمات المُدارة توفير الدعم لجميع السجلات بناءً على سياسة الاحتفاظ، وإمكانية تصدير السجلات المحفوظة عند الحاجة. • يجب على مقدمي الخدمات المُدارة محو جميع البيانات/المعلومات التاريخية ذات الصلة بسادايا بما في ذلك جميع الأنشطة والسجلات والحوادث والتكاملات بعد تأكيد تسليم المشروع. • يجب على مقدمي الخدمات المُدارة دعم جميع متطلبات التقارير اللازمة لتلبية جميع متطلبات التنظيم الداخلية والخارجية. • يجب على مقدمي الخدمات المُدارة دعم تبادل المعلومات الاستخبارية مع SOC سادايا بناءً على المعايير المحددة من قبل فريق CTI في سادايا. • يجب على مقدمي الخدمات المُدارة أن يأخذوا في الاعتبار الEDR المقترح للعملية ونطاق متطلبات الكشف والاستجابة. • يجب على خدمات الأمن المُدارة أخذ الموافقة من الإدارة ذات الصلة في الأمن السيبراني لحالات الاستخدام وطلبات التغيير وإنشاء المستخدمين. • يجب الموافقة على أي تصميم أو تغيير من قبل أعضاء فريق الأمن السيبراني وأي قسم ذي صلة من جانب السدايا. • يجب تقديم نقل المعرفة كل 6 أشهر مع أعضاء فريق الأمن السيبراني (SOC) لجميع المستويات مثل: تحليل L1، L2، L3، والهندسة والإدارة. • يجب على المقاولين الامتثال لمتطلبات التكنولوجيا التالية: 1. يجب أن تكون الحلول المقترحة قادرة على توفير وظائف SIEM الجيل القادم. 2. يجب أن تكون حلول SIEM مبنية على تكنولوجيا البيانات الكبيرة مع القدرة على	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم التمسيد	البنود	وحدات القياس	وصف البنود	المواصفات	ملاحظات
				استيعاب تخزين غير محدود. 3. يجب تثبيت تراخيص حلول SIEM دون الاتصال بالإنترنت ويجب أن تبرز الخيارات والقيود الدائمة والاشتراكية للتراخيص. 4. يجب أن تكون حلول SIEM قابلة للتوسيع والانتشار في بيئات متعددة مختلفة. 5. يجب أن تأخذ حلول SIEM قدرات العمل المتعددة في جمع البيانات وإثرائها والبحث فيها والاحتفاظ بها بعين الاعتبار. 6. يجب أن تكون فترة الاحتفاظ على الأقل 6 أشهر من السجلات التي يمكن البحث فيها عبر الإنترنت، و 12 شهرًا من السجلات التي يمكن البحث فيها، وثلاث سنوات من السجلات المؤرشفة التي يمكن البحث فيها. 7. يجب على حلول SIEM أن تتمكن من التعامل مع زيادة مرة واحدة في السعة السائلة (EPS) بمعدل أربع مرات خلال ساعة واحدة دون أي تخزين مؤقت أو تدهور في أداء الحل. 8. يجب أن تكون حلول SIEM قادرة على تحقيق التوافر العالي بين ثلاثة مراكز بيانات مختلفة لطبقات الجمع والترابط والفهرسة والأرشفة. 9. يجب تشفير جميع الاتصالات بين جميع مكونات حلول SIEM. 10. يجب أن لا تفرض حلول SIEM أي قيود على عدد الحقول التي يمكنها فهرستها. 11. يجب أن تسمح التصميمات والبيانات المقترحة لحلول SIEM بالوصول السريع إلى تيرابايتات الأرشفة والبيانات التاريخية. يجب أن تكون قادرة على توفير البحث السريع جدًا والموزع.	



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

القسم الثامن: المواصفات

64- العمالة

أولاً: الشروط الخاصة بالعمالة

- أ. يجب على المتعاقد أن يتخذ الترتيبات الخاصة لاستخدام العمال ومعاملتهم -مواطنين كانوا أو أجانب- وفقاً لأحكام نظام العمل ونظام التأمينات الاجتماعية والأنظمة الأخرى ذات العلاقة. ويلتزم المتعاقد بتوفير المتطلبات الضرورية لعماله بما في ذلك السكن الصحي ووسائل النقل والرعاية الصحية ووسائل السلامة.
- ب. يجب على المتعاقد الالتزام بدفع أتعاب العمالة ومراقبة حالة العمل على ألا تكون أقل من المتعارف عليه في القطاع أو نوع الخدمة الذي ينفذ فيه العمل.
- ج. يحظر على المتعاقد استقطاب أو محاولة استقطاب أي من موظفي الجهة.
- د. باستثناء ما قد ينص عليه العقد فيما بعد، لا يجوز القيام بتنفيذ العمل أثناء الليل أو خلال أيام الجمع، أو أيام الإجازات الرسمية الأخرى بدون إذن مكتوب من الجهة أو ممثل الجهة إلا إذا كان العمل ضرورياً أو لا يمكن الاستغناء عنه مطلقاً من أجل إنقاذ الأرواح أو الممتلكات أو من أجل ضمان سلامة الأعمال. على أن يخطر المتعاقد في مثل هذه الحالة الجهة أو ممثل الجهة فوراً. ويراعى دائماً أن أحكام هذه الفقرة لا تكون واجبة التطبيق في الحالات التي يكون فيها من المعتاد تنفيذ العمل بالتناوب أو على فترتين.
- هـ. يجب على المتعاقد في جميع الأوقات اتخاذ جميع الاحتياطات اللازمة للحفاظ على صحة موظفيه وسلامتهم. وتعيين مسؤول للحفاظ على السلامة والوقاية من الحوادث داخل الموقع. وتكون له سلطة إصدار التعليمات واتخاذ التدابير الوقائية لمنع وقوع الحوادث. ويجب على المتعاقد إرسال تفاصيل أي حادث إلى ممثل الجهة في أقرب وقت ممكن بعد وقوعه. يجب على المتعاقد الاحتفاظ بسجلات وتقديم تقارير بشأن صحة وسلامة العمال والأضرار التي لحقت بالممتلكات. يجب على المتعاقد القيام ببرامج توعوية عن الأمراض واتخاذ التدابير الأخرى اللازمة للحد من مخاطر انتقالها بين موظفيه.
- و. يجب على المتعاقد توفير القوى العاملة ذات الخبرة اللازمة بناءً على المؤهلات المطلوبة لكل وظيفة موضحة في جدول مواصفات العمالة. وللجهة الحق في جميع الأحوال أن تطلب - كتابة - من المتعاقد استبعاد أي شخص غير مرغوب فيه، وأن يستعين بشخص آخر بدلاً منه خلال (15) خمسة عشر يوماً من تاريخ إبلاغه.
- ز. يجب على المتعاقد تزويد الجهة بسجلات مفصلة لموظفيه مصنفة حسب المهارات. حيث يتم تقديم هذه السجلات إلى ممثل الجهة شهرياً، باستعمال النماذج التي يوافق عليها ممثل الجهة. وذلك إلى أن ينجز المتعاقد الأعمال المطلوبة.
- ح. يجب على المتعاقد التأكد من أن جميع المهندسين والفنيين والعاملين بالموقع بما في ذلك الجهاز الفني التنفيذي على كفاله أو كفالة المتعاقد من الباطن المتفق عليهم في هذا العقد. ويجب كذلك وجود عقد عمل رسمي لجميع العاملين معتمد من الجهة. يحق للجهة طلب نقل كفالة عمالة المتعاقد (العمال، الفنيين، والمشرفين) التي تعمل مباشرة لدى الجهة إلى المتعاقد الجديد وذلك لضمان جودة تنفيذ الأعمال.
- ط. يجب على المتعاقد اتخاذ الترتيبات اللازمة لتوفير إمدادات كافية من الطعام على النحو المنصوص عليه في العقد. كما يجب على المتعاقد توفير إمدادات كافية من مياه الشرب والمياه الأخرى لاستخدام موظفيه في الموقع.
- ي. يجب على المتعاقد الاحتفاظ بسجلات تفصيلية يبين فيها أسماء جميع موظفيه وعماله وأعمارهم وجنسهم وجنسياتهم وعدد ساعات العمل، وغير ذلك من المعلومات التي قد يطلبها منه ممثل الجهة. ك. يلتزم المتعاقد باستخراج الإقامات اللازمة للعمالة حسب الإجراءات النظامية وفقاً للأنظمة المعمول بها في المملكة.
- ل. يلتزم المتعاقد بتأمين العمالة اللازمة حسب المسمى الوظيفي والمؤهلات والخبرة المبينة بالجدول التالي (جدول مواصفات العمالة).
- م. يلتزم المتعاقد بتخصيص عمالة نسائية للعمل في الأقسام النسائية أو المواقع التي تتطلب ذلك.
- ن. يجب على المتعاقد أن يقوم بتأمين زي موحد للعمالة الموجودين في مواقع العمل، وما يلزم لهم من وسائل السلامة كالسترات العاكسة وخوذات للرأس.

ثانياً: جدول مواصفات العمالة

لا يوجد



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

65- المواد

أولاً: الشروط الخاصة بالمواد

تخضع المواد المستخدمة في تنفيذ الأعمال للمواصفات والمقاييس المعمول بها في المملكة العربية السعودية.

- 1 يقوم المتعاقد المواد المستخدمة في تنفيذ الأعمال للتأكد من مطابقتها لمواصفات العرض والمقاييس العالمية كما يطلع على نتائج الاختبارات المعمولة للمواد وإعطاء الموافقة (أو عدمها) عليها وتسجيلها والاحتفاظ بنسخة منها، ويجب كذلك أن تكون المواد المستخدمة سواء المحلية أو المستوردة لتنفيذ العقد مطابقة للمواصفات القياسية السعودية وما لم تشتمل منها هذه المواصفات فيجب أن يكون مطابقة لإحدى المواصفات العالمية المعروفة والتي تحددها الجهة أو من يمثلها.
- 2 ويجوز لممثل الجهة أن يأمر المتعاقد بإعداد بيان واضح ومفصل عن ماهية المواد المستخدمة وعن كل مادة على حدة ير ممثل الجهة ضرورة استبيانها، وعلى المتعاقد إعداد ذلك البيان كتابةً خلال فترة (10) عشرة أيام من تاريخ طلبها.
- 3 وإذا أخل المتعاقد بتوضيح ماهية المواد المستخدمة في الموعد المحدد فتعتبر تلك المواد خلاف ما تم الاتفاق عليه بالعقد ولممثل الجهة اتخاذ ما يلزم حسب تقديره من تعليمات أو جزاءات لمعالجة ذلك.

ثانياً: جدول مواصفات المواد



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

تقنية معلومات

اسم الجدول

ال فئ ة	ال بند	و د ة ال ق ي ا س	المواصفات
خ د م ة	خ د م ا ت م د ا ر ة ل ا د ا ر ة و ت ش غ ي ل ال ا ز ظ ة Ma na ge d Se cur ity Ser vic es	ش ه ر	يجب على مقدمي خدمات الأمن المُدارة توفير خدمات الكشف والاستجابة المُدارة وخدمات الاستشارة بشأن التهديدات. يجب على مقدمي خدمات الأمن المُدارة توفير حلول مجمعة تشمل الحوسبة والتخزين والشبكة. يجب على مقدمي خدمات الأمن المُدارة توفير الكشف المستمر للتهديدات باستخدام أدوات الضعف والتكامل مع حلول منصة الكشف والاستجابة المُدارة. يجب على مقدمي خدمات الأمن المُدارة تقديم تقارير أسبوعية أو شهرية للمنظمة بشأن الخدمات المشتركة مع مقدمي خدمات الأمن المُدارة. يجب على مقدمي خدمات الأمن المُدارة توفير ثلاثة مهندسين في الأمن السيبراني لإدارة الضوابط الأمنية المقترحة في الطلب. يجب على مقدمي الخدمات الأمنية المُدارة إجراء تحقيقات عميقة واستجابة للحوادث.



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	و د ة ال ق ي ا س	ال ب ن د	ال ف ئ ة
Bidder should do the configuration and installation	عد د	تركيب وضبط اعداد ادارة ام ن الد اوي ت co nta ine rs sec uri ty	ج ها ز



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحد ة الق ياس	البند	ال فئ ة
General . • Must be a cloud native platform architecture capable of being deployed on different architectures i.e. container, serverless or public cloud. • Must support a non-intrusive deployment i.e. No appliances or Agents. • Supports automated deployments tools and can leverage APIs for onboarding. • "Supports RBAC model for separation of duties and data - Read Only. - Role for adding cloud accounts.. - Limit access to specific accounts or account groups. Support integration of SSO and Federation providers via industry standard protocols i.e. SAML. • "Capability to feed alerts to 3rd party workflow tools in addition to visualising in the Prisma dashboard • Capability to tune alerts generated and customise the type of alerts that are sent to the relevant workflow tools and teams. • Solution provides an industry standard RESTFUL API. . • Containers (K8 - Managed/Unmanaged) Docker + others. • "Deploy out as a cloud native solution without requiring any agents or additional layers being added to container images or underlying cluster.. • Support deployment on multiple container platforms including:. • - Kubernetes (Cloud hosted EKS, AKS and GKE). - Other variants (Openshift, Pivotal etc). - Docker (stand alone and Swarm). - ECS". • Management platform flexibility to allows hosted SaaS or customer hosted container based management console. • "Kubernetes Deployment options:. • - Scripted. - Deployment manifest YAML. - Helm charts". . . . • Provide protection for cloud functions, deploy into the function.. • Discover cloud functions and vulnerabilities via cloud provider APIs. . • Hosts (Linux, Windows). . • "Deploy out as a cloud native solution that supports a deployment on multiple host platforms including:. • - Windows. - Linux". • Management platform flexibility to allows hosted SaaS or customers self hosted management console. . . Vulnerability Assessment Requirement. General . . • Provides high level visualisation on any vulnerabilities that exist . • Filter based on severity of vulnerability. • Capability to export vulnerability assessment information via API, CSV or integration with other platforms . • Allows filtering of vulnerabilities based on specific criteria i.e. CVE number. • Automatic updating of vulnerability feeds without operational overhead. • Where possible, provide mappings against well known vulnerability standards bodies and metrics i.e CVE and leverage common scoring mechanisms i.e. CVSS. . IAC. . • Capability to scan in the CI phase prior to deployment of instances i.e. Terraform , Cloud Formation . . • Containers (K8 - Managed/Unmanaged) Docker + others. . • Ensure that any vulnerability scanning doesn't require changes to be made to the container image via insertion of agents or similar mechanism. • Capability to scan all container images for vulnerabilities irrespective of whether they are deployed in Public Cloud , On-Premise, Hybrid or air gapped environments. • "Perform Vulnerability assessment at the CI (Continuous Integration) phase of the DevOps build pipeline by plugging into well known build platforms i.e.. • - Jenkins. - CircleCi. - Azure DevOps , AWS codepipeline and others. . • Perform integration capability for other lesser known build platforms.. . • Where possible, provide vulnerability metrics directly within the build platform and the option to fail the build if vulnerabilities of a given severity are discovered". • Allow developers to scan a stand alone container image prior to checking into	عدد	أمن البن د ال أويا ت co nta ine rs sec uri ty	خ د م ة



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحد القياس	البند	ال فئة
a registry, build pipeline or running. • "Capability to scan container registries to ensure ongoing health of container image, examples include:. . - Azure Container Registry. - Docker Hub. - Google Container Registry. - AWS EC2 container registry. - Nexus Sonar. - JFrog . . • Many more providing they are Docker Registry 2.0 compliance". • Capability to discover vulnerabilities in running container images within the environment. • Platform provides the capability to concisely visualise vulnerabilities at the Build, Deploy and Run. • Capability to drill down on each container image and visualise the exact layer(s) where vulnerabilities exist, enable fast feedback via integration with DevOps workflows. • "Capability to understand each vulnerability in-depth and threat vectors that may raise the risk profile in the environment.. . - Ease of attack. - Threat Vectors i.e. Network based. - If a fix is available and how long has the vulnerability existed.. - Traits of running containers that elevate risk. - Detailed CVE information and remediation details.. - Understand which containers and hosts the vulnerability exist on.. - Impacted packages/ frameworks.. - Percentage of environment impacted". • The capability to define your own custom vulnerability checks. • "Configure proactive policies to alert on or prevent deployment of vulnerable images into a production environment.. . • Policies should be tunable based on the severity level, labels, images and other factors". • In high security environments that are air-gapped, provide a mechanism to update vulnerability signatures. • Vulnerability managemnt should cover Git Repo including Java , Python & ode repositories on git. . • Serverless - Lambda, Azure, GCP Functions. . • Automatically discover vulnerabilities for Serverless functions including any vulnerabilities in function libraries. • ""Capability to understand each vulnerability in-depth and threat vectors that may raise the risk profile in the environment.. . - Ease of attack. - Threat Vectors i.e. Network based. - If a fix is available and how long has the vulnerability existed.. - Detailed CVE information and remediation details.. - Impacted packages/ frameworks.. • Hosts (Linux, Windows). . • Capability to scan all supported hosts for vulnerabilities irrespective of whether they are deployed in Public Cloud , On-Premise, Hybrid or air gapped environments. • Capability to discover vulnerabilities in running hosts within the environment as well as AWS AMI. • "Capability to understand each vulnerability in-depth and threat vectors that may raise the risk profile in the environment.. . - Ease of attack. - Threat Vectors i.e. Network based. - If a fix is available and how long has the vulnerability existed. - Detailed CVE information and remediation details. - Understand which containers and hosts the vulnerability exist on. - Impacted packages/ frameworks.. - Percentage of environment impacted". • The capability to define your own custom vulnerability checks. • "Configure proactive policies to alert on or prevent deployment of vulnerable hosts into a production environment (Linux hosts only).. . • Policies should be tunable based on the severity level, labels, images and other factors". • In high security environments that are air-gapped, provide a mechanism to update vulnerability signatures. • Have the ability to apply vulnerability rules when when vendor fixes are available. . • Customer specific use cases. . . Compliance Requirement. General . . • Provides high level visualisation on any compliance violations across the environment for the different architectures i.e. Public Cloud, Container			



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
or Serverless. • Filter based on severity of compliance failure. • Capability to export compliance violation events via API, CSV or integration with other platforms i.e Slack, SOAR (Demisto), Jira, Email. • Allows for filtering and searching for specific compliance checks via name, resource impacted or severity plus other metrics i.e. cloud accounts, labels.. • Automatic updating of vulnerability feeds without operational overhead. • Where possible leverage well known compliance standards and regulatory frameworks i.e. NIST, CIS, GDPR PCI, ISO. • Ensure continuous and automatic scanning for compliance without the operators having to manually set and schedule scans. . . • Containers (K8 - Managed/Unmanaged) Docker + others. . • Ensure that any compliance scanning doesn't require changes to be made to the container image via insertion of agents or similar mechanism. • Capability to scan all container images for compliance violations irrespective of whether they are deployed in Public Cloud , On-Premise, Hybrid or air gapped environments. • "Provide out of the box baselining against well know standards and frameworks for container images, runtime and kubernetes configuration. - CIS (Docker & Kubernetes). - NIST 800-190. - PCI. - GDPR". • "Perform compliance audit at the CI (Continuous Integration) phase of the DevOps build pipeline by plugging into well known build platforms i.e.. - Jenkins. - CircleCi. - Azure DevOps and others. . • Perform integration capability for other lessor know build platforms.. . • Where possible, provide vulnerability metrics directly within the build platform with the option to fail the build if compliance violations of a given severity are discovered". • Allow developers to scan a stand alone container image prior to checking into a registry, build pipeline or running. • "Capability to scan container registries to ensure ongoing compliance of images, examples include:. - EC2 container registry. - Nexus Sonar. - JFrog . . • Many more providing they are Docker Registry 2.0 compliance". • Capability to discover compliance violations in existing running containers within the environment. • Platform provides the capability to concisely visualise compliance violations at the Build, Deploy and Run. • The capability to define your own custom compliance checks. • "Configure proactive policies to alert on or prevent deployment of non-compliant images into a production environment.. . • Policies should be tunable based on the severity level, labels, images and other factors". • In high security environments that are air-gapped, provide a mechanism to update compliance signatures. • Capability to only allows the use of "Trusted images". • "Understand what images are running in the enviroment and allow only ""Trusted Images"" to run.. . - Control via registry. - Repo. - Individual Image. - Base layers of image". . • Serverless - Lambda, Azure, GCP Functions. . • "Automatically discover compliance violations for Serverless functions including:. - Embedded Private keys and passwords. - Overly permissive access. - Broad resource access. - Unused services that the function can access. - Suspicious function actions". • ""Capability to understand each compliance failure.. . - Ease of attack. - Threat Vectors i.e. Network based. - If a fix is available and how long has the violation existed.. - Impacted functions. • ". • Hosts (Linux, Windows). . • Capability to scan all container images for compliance violations irrespective of whether they are deployed in Public Cloud , On-Premise, Hybrid or air gapped environments. • "Provide out of the box			



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحد ة الق ياس	البند د	ال فئ ة
baselining against well know standards and frameworks for hosts including Windows, Lunix, Docker host/ daemon/ security ops, Kubernetes master/worker/ federation:. . - CIS (Docker & Kubernetes). - NIST 800-190. - PCI. - GDPR". • Capability to discover compliance violations in existing running hosts within the environment. • The capability to define your own custom compliance checks. • In high security environments that are air-gapped, provide a mechanism to update compliance signatures. • Perform checks look at the Windows host's configuration of the Windows Firewall, Windows Defender / anti-malware, and Windows Update configuration. • Ability to implement security around files and directories in your monitoring profile for changes - File Integrity Monitoring (FIM). . . • Customer specific use cases. . Incident Response and Protection Requirement. General . . • Provide dashboarding detailing any incidents or anomalies along with criticality. • Support different types of threat detection capabilities including static signature, learning and behavioural analysis. • Capability to export compliance violation events via API, CSV or integration with other platforms • Allows for filtering and searching for specific incidents via name, resource impacted or severity plus other metrics i.e. cloud accounts, labels. • Automatic updating of threat intelligence feeds. • Behavioural and learning based models must be automatic without requiring the operator to manually setup thresholds etc. . . • Containers (K8 - Managed/Unmanaged) Docker + others. . • "The platform can baseline container images and their expected behaviours via a combination of static analysis of dockerfiles and deployment manifest combined with dynamic analysis of a running container, this should include:. . - Network activity. - Processes. - File System. . • Container capabilities i.e. Does it have elevate access". • Capability to relearn baseline . • "Capability to report when there is a deviation or abnormal activity compared to the baseline i.e. . . - New process spawned. - Network comms that differs from the baseline. - Exec access to containers". • "Leverages threat intelligence to spot malicious or abnormal behaviour i.e. . . - Crypto Mining. - Malware. - Communication with high risk domains/destinations. - Lateral Movement". • Capability to drill down on incidents and perform forensic investigation and capture/export information related to the incident. • Allows proactive protection against certain incidents including the capability to prevent rogue processes and network activity or in extreme cases to terminate a running container, this should be possible through a flexible policy that can be tailored based on container images, namespace or labels. • The platform automatically maps and learns network activity between the container images in the environment. • Provide a zero trust architecture by implementing microsegmentation to limit lateral movement . • "Provide layer 7 Web application protection for containers hosting web apps, protection should include, protections should include:. . - CSRF Protection. - XSS Protection. - Clickjacking protection. - SQL Injection protection. - Attack Tool protection . - Malformed request protection. . • ". . . • Serverless - Lambda, Azure, GCP Functions. . • "Automatically discover compliance violations for Serverless functions which could lead to incidents including:. . - Embedded Private keys and passwords. - Overly permissive access. - Broad resource access. - Unused services that the function can access. - Suspicious function			



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
actions". • "Capability to protect functions including:. - Network. - Process. • ". • Hosts (Linux, Windows). . • "The platform can baseline hosts and their expected behaviours, this should include:. - Network activity. - Processes". • Capability to relearn baseline learned behaviours. • "Capability to report when there is a deviation or abnormal activity compared to the baseline i.e. . . - New process spawned. - Network comms that differs from the baseline. - Exec access to containers". • "Capability to report when there is a deviation or abnormal activity compared to the baseline i.e. . . - Network comms that differs from the baseline. - App Capabilites. - Application Control / Whitelisting. - Log Inspection. - User, Application and Application Activites. - File Integrity Monitoring". • Capability to drill down on incidents and perform forensic investigation and capture/export information related to the incident. • Allows proactive protection against certain incidents including the capability to alert on rogue applications on hosts, this should be possible through a flexible policy. • The platform automatically maps and learns network activity between hosts in the environment. • Provide a zero trust architecture by implementing microsegmentation to limit lateral movement . • "Provide layer 7 Web application protection for hosts withweb apps, protection should include, protections should include:. - CSRF Protection. - XSS Protection. - Clickjacking protection. - SQL Injection protection. - Attack Tool protection . - Malformed request protection. • Customer specific use cases			
Encryption Key Management - Hardware Security Modules . Certificate-Based Authentication for outside developers	عدد	Encryption Key Management	خ د م ا



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

ال فئة	ال بن د	و د ة ال ق ي ا س	المواصفات
خ د م ة	خ د م ة	ش ه ر	• يتطلب من مقدم العطاء استخدام الأدوات والخبرات التقنية للبيئات السحابية من خلال خبراء ذات خبرة عملية في هذا المجال ويشمل نطاق العمل عمل تقييم ومراجعة الإعدادات للأنظمة السحابية بما يشمل: - مراجعة الإعدادات الأمنية للأنظمة البيئية السحابية المختلفة مع التدقيق على قياس مدى الالتزام بالمعايير والضوابط الأمنية. - يلتزم مقدم الخدمة بالتأكد من تطبيق أفضل ممارسات الامنية المعتمدة من الشركات الأم بالإضافة الى . - الكشف عن الثغرات الأمنية بشكل اوتوماتيكي باستخدام أدوات الاختبارات الأمنية لمكونات البيئة السحابية مثل المنصات السحابية والخوادم وأجهزة الشبكة. - مراجعة التصاميم التقنية للمكونات السحابية والأنظمة المستضافة بالإضافة الى فحص الإعدادات والقواعد المطبقة. - انشاء وتطوير المراجع الأمنية المعتمدة لجميع المكونات السحابية Minimum Security Baseline-Standards وتعزيز المتطلبات الأمنية بتطوير الخدمات السحابية والتطبيقات المقدمة من خلال منصات الاتمته السحابية Cloud Management Platform . - التطوير وتعزيز المعايير الأمنية لنظم إدارة الحاويات السحابية (Kubernetes & Containers) بما يدعم أنشطة التطوير ونشر الحاويات على الخوادم المتعددة
ا ج ه ة	ج ه ا ز م ب د ل ل ل ت ر ز	ع د د	• x RJ45 10/100/10000Mb auto- sensing ports, SFP+ ports, 2 x stacking ports, 1x PSU 48 included. . • 24 x RJ45 10/100/10000Mb auto- sensing ports, SFP+ ports, 1x PSU included. . • 8 x RJ45 10/100/1000Mb auto- sensing ports, 2 x SFP ports, 1 x PSU included. . • Support for minimum of 8 switches per stack for 24 port and 48 port switches . • Must support Comprehensive enterprise-class Layer 2/3 feature set on 24/48 port switches . • The switch (24/48) must support Layer 3 routing and must be offered with its highest available licensing model . • Switch must be compliant . • Switch should be SDN Open Flow ready . • Standards Support . • 802.3 - 10 Base-T . • 802.3u - 100 Base-T . • 802.3ab - 1000 Base-T . • 802.3ac - VLAN Tagging . • 802.3ad - Link Aggregation . • 802.3ae - 10 GigE . • 802.1D - Spanning Tree, GARP and GVRP . • 802.1S - Multiple Spanning Tree . • 802.1W - Rapid Spanning Tree . • 802.1Q - Virtual LANs with Port-based VLANs . • 802.1v - Protocol-based VLANs . • 802.1p - Ethernet Priority with User Provisioning and Mapping . • 802.1X - Port-based Authentication . • 802.2 . • 802.3x - Flow Control . • 802.1AB - LLDP . • 802.1p . • SNMP v1/v2/v3 . • IGMP snooping v1/v2V3 . • IGMP Snooping Querier . • For 24 and 48 port switches, should support routing static capabilities.. • The proposed switch must have 3 years vendor support with 7x24 service. . • The Quantity for the 48 port switches must be 1. • The Quantity for the 24 port switches must be 2. • The Quantity for the 8 port switches must be 1



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البنية	الكمية
x RJ45 10/100/10000Mb auto- sensing ports, SFP+ ports, 2 x stacking ports, 1x PSU 48 . . included. . . 24 x RJ45 10/100/10000Mb auto- sensing ports, SFP+ ports, 1x PSU included. . . 8 x RJ45 10/100/1000Mb auto- sensing ports, 2 x SFP ports, 1 x PSU included. . . Support for minimum of 8 switches per stack for 24 port and 48 port switches . . Must support Comprehensive enterprise-class Layer 2/3 feature set on 24/48 port switches . . The switch (24/48) must support Layer 3 routing and must be offered with its highest available licensing model . . Switch must be FreshAir compliant . . Switch should be SDN Open Flow ready . . Standards Support . . 802.3 - 10 Base-T . . 802.3u - 100 Base-T . . 802.3ab - 1000 Base-T . . 802.3ac - VLAN Tagging . . 802.3ad - Link Aggregation . . 802.3ae - 10 GigE . . 802.1D - Spanning Tree, GARP and GVRP . . 802.1S - Multiple Spanning Tree . . 802.1W - Rapid Spanning Tree . . 802.1Q - Virtual LANs with Port-based VLANs . . 802.1v - Protocol-based VLANs . . 802.1p - Ethernet Priority with User Provisioning and Mapping . . 802.1X - Port-based Authentication . . 802.2 . . 802.3x - Flow Control . . 802.1AB - LLDP . . 802.1p . . SNMP v1/v2/v3 . . IGMP snooping v1/v2V3 . . IGMP Snooping Querier . . For 24 and 48 port switches, should support routing static capabilities.. . The proposed switch must have 3 years vendor support with 7x24 service. . . The Quantity for the 48 port switches must be 1. . The Quantity for the 24 port switches must be 2. . The Quantity for the 8 port switches must be 1	عدد	جهاز المبدل للمنطق المهايطة DMZ Switch	اجهزة
FC Cables LC-LC, LC-MC• Fiber Optic SFP Single mode 1Gig/10Gig• Length 3 mtr• Single mode, 8 core - Fiber Optic Cable. • Fiber Optic Patch Panel: Single Mode Duplex LC Fully Loaded 8/16 port. • Fiber Optic LC Duplex Patch chords 3mtrs• Heat Shrink Sleeves, Pigtails, Alcohol Pads, .Labelling and all other required accessories for splicing	عدد	FC Cables LC LC MC	اجهزة
UTP Cat7 Patch Chords 3mtrs •	عدد	UTP Cables Cat 7	اجهزة



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

ال فئة	ال بن د	و د ة ال ق ي ا س	المواصفات
اج ه زة	ج ه از الم ب د ل للأ ارة MG MT Swi tch	عد د	• 1 x RJ45 10/100/1000Mb auto- sensing ports, SFP+ ports, 2 x stacking ports, 1x PSU 48 included. . • 24 x RJ45 10/100/1000Mb auto- sensing ports, SFP+ ports, 1x PSU included. . • 8 x RJ45 10/100/1000Mb auto- sensing ports, 2 x SFP ports, 1 x PSU included. . • Support for minimum of 8 switches per stack for 24 port and 48 port switches . • Must support Comprehensive enterprise-class Layer 2/3 feature set on 24/48 port switches . • The switch (24/48) must support Layer 3 routing and must be offered with its highest available licensing model . • Switch must be FreshAir compliant . • Switch should be SDN Open Flow ready . • Standards Support . • 802.3 - 10 Base-T . • 802.3u - 100 Base-T . • 802.3ab - 1000 Base-T . • 802.3ac - VLAN Tagging . • 802.3ad - Link Aggregation . • 802.3ae - 10 GigE . • 802.1D - Spanning Tree, GARP and GVRP . • 802.1S - Multiple Spanning Tree . • 802.1W - Rapid Spanning Tree . • 802.1Q - Virtual LANs with Port-based VLANs . • 802.1v - Protocol-based VLANs . • 802.1p - Ethernet Priority with User Provisioning and Mapping . • 802.1X - Port-based Authentication . • 802.2 . • 802.3x - Flow Control . • 802.1AB - LLDP . • 802.1p . • SNMP v1/v2/v3 . • IGMP snooping v1/v2V3 . • IGMP Snooping Querier . • For 24 and 48 port switches, should support routing static capabilities.. • The proposed switch must have 3 years vendor support with 7x24 service. . • The Quantity for the 48 port switches must be 1. • The Quantity for the 24 port switches must be 2. • The Quantity for the 8 port switches must be 1



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	القيمة
System information. License Capacity . • 500-4,000 users. . Hardware Specifications. • 8 GB. Management. • HTTP/S, SSH, CLI, SNMP, Console RJ45. . Network Interfaces . • 4x GE RJ45. Storage. • 4 TB (2 TB x2) Hard Disk. Power Supply . • Single (Optional Dual). Form Factor. • 1U Appliance. Input Voltage . • 100-240V, AC 60-50 Hz. Power Consumption . (Average / Maximum) 120 W / 151 W. Maximum Current. • 100V/5A, 240V/3A. Heat Dissipation. • 550 BTU/h. Operating Temperature . • 32-104°F (0-40°C). Storage Temperature. • -13-158°F (-25-70°C). Humidity. • 5-95% non-condensing. FEATURES SUMMARY. . System. . • Wide range of deployment options:. • Inline, Forward Proxy, Explicit proxy, WCCP/PBR. • Hardware or virtual appliance. • IPv4 and IPv6 address support. • Application Support including HTTP/S. • HA available as active-active and active-backup with. • session synchronization . . Authentication. . • Support for various authentication modes including Radius,. • SAML, LDAP, NTLM, Kerberos. • Password. • In-built authentication requiring no additional device. . . Threat Protection. . • Integration with threat intelligence services for real-time threat updates. • Integration with cloud sandbox to detect advanced threats. • In-built security services requiring no additional appliance. • DNS and Web-Filtering. • Dynamic categorization of websites. • Blocking of malicious and suspicious domains and URLs. • Static blacklists and whitelists. • Application Control. • Granular web application control for social websites. • Support for 3000+ applications. • Antivirus, bonet and DLP. • Content Analysis. • Multiple ICAP servers support. • IPS signature and filters. • Web Rating Override. • SSL/SSH Inspection. • Custom Application Signature. . . Advanced Caching. . • Web and video caching. • Reverse web cache. • Traffic Shaping and QoS policies to prioritize Apps. • Dynamic adaptive streaming over HTTP. • Dynamic adaptive streaming over RTP and RTMPT. . . WAN Optimization. . • Protocol Optimization - support HTTP, MAPI, CIFS, FTP,. • and TCP. • Secure tunneling over across WAN. • Wan Optimization peers. . Management and Reporting. . • Support Syslog server. • Granular role based access. • Reporting and Logging. • Policy tests for ease of deployment	عدد	تقنية الوسيط proxy	نظام



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	و د ة ال ق ي ا س	ال ب ن د	ال ف ئ ة
Up to 6.4 Tbps switching capacity with up to 2 Bpps of forwarding performance.. . • Up to . 36 MB of unified buffer per ASIC.. . • Intel 2.4-GHz x86 CPU with up to 120 GB of USB 3.0 or up to 960 GB of SATA SSD storage for container-based application hosting.. . • Up to 32 nonblocking 100 Gigabit Ethernet QSFP28 ports.. . • Up to 32 nonblocking 40 Gigabit Ethernet QSFP+ ports.. . • Up to 48 nonblocking 25 Gigabit Ethernet SFP28 ports.. . • Up to 48 nonblocking 10 Gigabit Ethernet SFP+ ports.. . • Scalable Layer 3 routing (IPv4, IPv6, and multicast) tables and Layer 2 switching tables.. . • Hardware support for Application Hosting (e.g. with Cisco ThousandEyes Enterprise Agent).. . • 802.1ba AV Bridging (AVB) built in to provide a better AV experience through improved time synchronization and QoS.. . • Precision Time Protocol (PTP; 1588v2) provides accurate clock synchronization with sub- microsecond accuracy, making it suitable for distribution and synchronization of time and frequency over the network.. . • Support for both static and dynamic NAT and Port Address .Translation (PAT)	عد د	ج ه ل ال د ا خ ل C o r e D C S w i t c h	ا ج ه ز ة



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحد ة الق ياس	البند	ال فئة
General Specification . . Should be provided with Next Generation Firewall licenses for IPS, . . Advanced Malware Protection and Application Control Service, URL and DNS filtering. . The device should support both Explicit Proxy and Transparent Proxy along with all NGFW features simultaneously on the same appliance without any compromise.. . The solution should support advanced SDWAN features to aggregate multiple WAN interfaces, measure application performance among the links and selecting best exit interface for traffic using measured SLAs without additional license. . The SDWAN feature shall fully support IPv4 as well as IPv6. . The SDWAN feature should support both passive WAN health measurement through synthetic transactions and active WAN health measurement through monitoring application session information. . Should support both SSL certificate inspection and full SSL inspection. Solution should support TLS 1.1, 1.2 and 1.3 deep inspection. . The solution must support native integration with similar products to form a fabric to share visibility, share threat intelligence and automate response.. . The device must have APIs.. . It should have inbuilt feature of Two-Factor Authentication (2FA) for SSL-VPN and for Admin login, without needing a separate software/hardware to deploy the solution.. . The system must have the ability to integrate with external threat feeds and IP reputation sources from both public and private sources . . The proposed system shall provide robust visibility GUI panels and dashboards. Should support HTML5 based Web UI. The Web UI should not have any Java, Flash or ActiveX components as these components can pose considerable security threats due to frequent-vulnerabilities and end-of-support notices.. . The proposed system shall provide administrators ability to assign arbitrary score given based on the perceived risk of certain events such as visit to malicious websites and malware detection. . . Should be able to send logs simultaneously to existing Centralized logging appliance, multiple Syslog servers and SIEM solutions. . The proposed solution should be leader in last Gartner Network Firewall.. . The proposed solution should be leader in last Gartner WAN Edge Infrastructure.. . The proposed solution should be integrated with any authentication and identification platform and support at minimum; Active Directory, LDAP, RADIUS, TACACS+.. . 8x 100GE/40GE QSFP28 slots and 18x 25GE/10GE SFP28 slots, 2 x GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, 2x 2TB storage and 2 AC power supplies. . 3 Year Advanced Threat Protection (IPS, Advanced Malware Protection Service, Application Control). . 3 Year Secure RMA Service	عدد	جهاز جدار ر الد ماي ة لمر اكز البي انا ت Data ta Ce nte r Fir ew all	اج ه زة



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحد ة الق ياس س	ال بن د	ال فئ ة
x RJ45 10/100/10000Mb auto- sensing ports, SFP+ ports, 2 x stacking ports, 1x PSU 48 . . included. . . 24 x RJ45 10/100/10000Mb auto- sensing ports, SFP+ ports, 1x PSU included. . . 8 x RJ45 10/100/1000Mb auto- sensing ports, 2 x SFP ports, 1 x PSU included. . . Support for minimum of 8 switches per stack for 24 port and 48 port switches . . Must support Comprehensive enterprise-class Layer 2/3 feature set on 24/48 port switches . . The switch (24/48) must support Layer 3 routing and must be offered with its highest available licensing model . . Switch must be FreshAir compliant . . Switch should be SDN Open Flow ready . . Standards Support . . 802.3 - 10 Base-T . . 802.3u - 100 Base-T . . 802.3ab - 1000 Base-T . . 802.3ac - VLAN Tagging . . 802.3ad - Link Aggregation . . 802.3ae - 10 GigE . . 802.1D - Spanning Tree, GARP and GVRP . . 802.1S - Multiple Spanning Tree . . 802.1W - Rapid Spanning Tree . . 802.1Q - Virtual LANs with Port-based VLANs . . 802.1v - Protocol-based VLANs . . 802.1p - Ethernet Priority with User Provisioning and Mapping . . 802.1X - Port-based Authentication . . 802.2 . . 802.3x - Flow Control . . 802.1AB - LLDP . . 802.1p . . SNMP v1/v2/v3 . . IGMP snooping v1/v2V3 . . IGMP Snooping Querier . . For 24 and 48 port switches, should support routing static capabilities.. . The proposed switch must have 3 years vendor support with 7x24 service. . . The Quantity for the 48 port switches must be 1. . The Quantity for the 24 port switches must be 2. . The Quantity for the 8 port switches must be 1	عدد	جهاز المبدل المتعدد الوسائط	إجهزة



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحد القياس	البند	ال فئة
The bidder should propose a solution which contain dedicated secure internal DNS and . . DHCP physical/virtual servers across one datacentre with an overall optimal capacity of 45K DNS QPS and 300 DHCP LPS. . The proposed solution should contain dedicated secure caching DNS with an overall optimal capacity of 23K DNS QPS. . The proposed DNS security solution should contain a dedicated hardware /virtual reporting & analytics server in the main datacentre with total indexing daily capacity of 500MB. . The proposed solution must for 1 and 3 yrs.. . The bidder should propose the below for the SDAIA cloud datacentre. . . The proposed solution should contain dedicated secure internal DNS and DHCP virtual servers across one datacenter with an overall optimal capacity of 75K DNS QPS and 450 DHCP LPS . . The proposed solution should contain dedicated secure caching DNS with an overall optimal capacity of 45K DNS QPS. . The proposed solution should contain dedicated external DNS with an overall optimal capacity of 23K DNS QPS. . The proposed DNS security solution should contain a dedicated virtual reporting & analytics server in the main datacentre with total indexing daily capacity of 5GB. . The proposed solution must for 1 and 3 yrs.. . The proposed solution DNS Firewall solution should leverage on-premises DDI platforms to run the DNS Firewall service.. . The proposed solution should offer internal authoritative DNS, DHCP and hybrid DNS firewalling . . The proposed solution should contain on-premises VM based platforms and should cover 1x datacenters capable of running the DNS Firewall service.. . The proposed DNS Firewall license should be used as a hybrid DNS FW that can support cloud-based DNS Firewalling and on-premises DNS Firewalling at the same time. The on-premises DDI solution and Hybrid DNS FW should both be provided from the same technology vendor. . . The proposed DDI solution should offer flexible licenses that can be moved to/from HW platforms to/from virtual based platforms and vice versa.. . The proposed solution should be capable of integrating thru DNS over TLS with on-premises DDI solution deployed in the network. The DDI solution should be available and produced from the same DNS Firewall vendor.. . The proposed solution should be offered from a technology vendor/manufacturer who is able to offer cloud-based DNS FW for protection against Data Exfiltration over DNS.. . The proposed DNS FW solution should offer support for DNSSEC validation.. . The proposed solution must offer DNS Context-aware Security.. . The proposed solution should be offered from a technology vendor/manufacturer that can support Threat Intelligence from same vendor for DNS based Firewalling.. . The proposed solution should be offered from a technology vendor/manufacturer that should support Threat Intelligence data/IoCs sharing with SIEM and NGFWs thru WAPI calls.. . The proposed solution should be offered from a technology vendor/manufacturer that can offer DNS Firewalling to provide protection against DNS based tunneling, DGA, fast-flux and data exfiltration and infiltration threats.. . The proposed solution should be offered from a technology vendor/manufacturer that can offer DNS Firewalling that should support Behavioral based analytics and detection for DNS based threats.. . The proposed solution should be able to offer DNS Firewalling without any change on the setup leveraging threat	عدد	حم اية نظ ام أسد ماء الذ طا قا ت DN S Se cur ity	ز ظ ام



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	و د ة ال ق ي ا س	ال ب ن د	ال ف ئ ة
intelligence and streamlined behavioral analytics thru machine learning.. • The proposed solution should be capable of integrating with 3rd party security eco-systems from NGFWs and SIEM solutions.. • The proposed solution should be capable of protecting users on-premise behind the network and roaming users or users located in branches that don't have direct connectivity to the datacenter(s).. • The proposed cloud DNS firewall solution should support DNS caching for better application performance.. • All provided components of the solution including internal DNS, DHCP and hybrid DNS FW should be provided from the same technology vendor.. • The proposed solution must offer cloud based and on-premise based protection against Data Exfiltration over DNS.. • The proposed solution should offer DNS FW leveraging threat intelligence and streamlined behavioral analytics thru machine learning.. • The proposed DNS FW solution should offer support for DNSSEC validation.. • The proposed solution must offer DNS Context-aware Security.. • The proposed solution should support Threat Intelligence based DNS Firewalling.. • The proposed solution should offer Threat Intelligence Data Exchange (TIDE) platform support Threat Intelligence data/IoCs sharing with SIEM and NGFWs thru RESFul WAPI.. • The proposed solution should support cloud based and on-premises based Behavioral based analytics and detection for DNS based threats.. • The proposed solution should be capable of integrating with 3rd party security eco-systems including NGFWs (PaloAlto & Fortinet), Vulnerability Management Systems (Tenable/Qualys/FortiGate/PaloAlto/ServiceNow/Rapid7) and SIEM solutions.. • The secure DDI solution should offer the ability to leverage security eco-system and orchestration using outbound restful API calls and notifications to enable triggering actions and automation across 3rd party systems. . • The secure DNS caching solution should offer the ability to leverage outbound restful API calls and notifications upon DNS security events. Solutions that don't support outbound API calls will be discarded.. • The proposed solution should be capable of protecting users on-premise behind the network and roaming users or users located in branches that don't have direct connectivity to the DCs.. • The proposed cloud DNS firewall solution should support DNS caching for better application performance.. • The secure DDI solution should offer DNS firewalling leveraging DNS RPZ threat intelligence that should contain multiple categories of RPZ security feeds. Solutions with single security RPZ feed will be discarded. . • The secure DDI solution should offer be able to offer DNS firewalling with threat intelligence from the same technology vendor that should contain as minimum all below RPZ security feeds: • Base hostnames: The base hostnames RPZ feed is required to enable protection against known hostnames that are dangerous as destinations and are sources of threats, such as APTs, bots, compromised host/domains, exploit kits, malicious name servers and sinkholes.. • Anti-malware: This RPZ feed enables protection against hostnames containing known malicious threats, such as malware command and control (C&C), malware download and active phishing site.. • Ransomware: This RPZ feed enables protection against hostnames containing malware that restricts access to the computer system it infects and demands a ransom for the removal of the restriction. • Bogon: This RPZ feed enables should contain the source addresses of DDoS attacks and is an			



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
informal name for an IP packet on the public Internet that claims to be from an area of the IP address space reserved, but not yet allocated or delegated by an Internet Authority or Registry. Bogons are usually the result of accidental or malicious misconfiguration.. • DHS AIS_IP and DHS AIS_Hostname (2 feeds): AIS is a part of the Department of Homeland Security's (DHS's) effort to create an ecosystem in which, as soon as a company or federal agency observes an attempted compromise, the indicator is shared with AIS program partners.. • DHS AIS NCCIC Watch list Hostnames and Domains and DHS AIS NCCIC Watch list IPs (2 feeds): Indicators contained in these feeds appear on the watch list from the .National Cybersecurity and Communications Integration Center (NCCIC)			
Chassis Chassis with up to 16x2.5" Drives. • Trusted Platform Module Trusted Platform Module 2.0 V3. • Chassis 2.5" Chassis with up to 16 SAS/SATA Drives, 2 CPU. • CPU Gold 6330 2G, 28C/56T, 11.2GT/s, 42M Cache, Turbo, HT (205W) DDR4-2933. • CPU Gold 6330 2G, 28C/56T, 11.2GT/s, 42M Cache, Turbo, HT (205W) DDR4-2933. • Memory Type 3200MT/s RDIMMs. • Memory Type 32GB RDIMM, 3200MT/s, Dual Rank, 16Gb BASE x8. • HDD 2.4TB 10K RPM SAS ISE 12Gbps 512e 2.5in Hot-Plug Hard Drive. • Power Supply Dual, Hot-Plug,Power Supply Fault Tolerant Redundant (1+1), 800W, Mixed Mode. • Rack Power Cord Rack Power Cord 2M (C13/C14 10A). • NIC Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM. • NIC Ethernet X710 Quad Port 10GbE SFP+, OCP NIC 3.0. • BOSS-S2 controller card BOSS-S2 controller card + with 2 M.2 240GB (RAID 1). • SFP SFP+ SR Optic, 10GbE, for all SFP+ ports except high temp validation warning cards. • OS VMware ESXi 7.0 U3 Embedded Image (License Not Included). • OS Licenses VMware vSphere 7 Standard for 1 CPU, up to 32 cores, 1YR VMware SNS. • Warranty Warranty 12Months, 12 Month(s). • Support Support and Next Business Day Onsite Service, 12 Month(s). • Chassis Chassis with up to 16x2.5" Drives. • Trusted Platform Module Trusted Platform Module 2.0 V3. • Chassis 2.5" Chassis with up to 16 SAS/SATA Drives, 2 CPU. • CPU Gold 6330 2G, 28C/56T, 11.2GT/s, 42M Cache, Turbo, HT (205W) DDR4-2933. • CPU Gold 6330 2G, 28C/56T, 11.2GT/s, 42M Cache, Turbo, HT (205W) DDR4-2933. • Memory Type 3200MT/s RDIMMs. • Memory Type 32GB RDIMM, 3200MT/s, Dual Rank, 16Gb BASE x8. • HDD 2.4TB 10K RPM SAS ISE 12Gbps 512e 2.5in Hot-Plug Hard Drive. • Power Supply Dual, Hot-Plug,Power Supply Fault Tolerant Redundant (1+1), 800W, Mixed Mode. • Rack Power Cord Rack Power Cord 2M (C13/C14 10A). • NIC Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM. • NIC Ethernet X710 Quad Port 10GbE SFP+, OCP NIC 3.0. • BOSS-S2 controller card BOSS-S2 controller card + with 2 M.2 240GB (RAID 1). • SFP SFP+ SR Optic, 10GbE, for all SFP+ ports except high temp validation warning cards. • OS VMware ESXi 7.0 U3 Embedded Image (License Not Included). • OS Licenses VMware vSphere 7 Standard for 1 CPU, up to 32 cores, 1YR VMware SNS. • Warranty Warranty 12Months, 12 Month(s). • Support Support and Next Business Day Onsite Service, 12 Month(s).	عدد	خوادم الداخلي	اجهزة



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	و د ة ال ق ي ا س	ال ب ن د	ال ف ئ ة
On-Premise solution that is compliance with all local laws and regulations in Saudi Arabia - - Integrated Active Directory, Exchange and Office 365 management - One-click AD, O365, and Exchange user creation - Bulk management of AD objects via CSV import - 200+ pre-packaged, actionable reports - Automation for routine tasks such as AD cleanup - OU-based help desk delegation - Template-based user provisioning - Protect against data loss disasters with AD backup and recovery - Integration with popular SIEM, HR management, and helpdesk software - iOS and Android mobile apps, and much more - Create users in AD, Exchange, Office 365, Google Apps, and Skype for Business (Lync) in a single step - Create or modify AD objects (users, groups, contacts, OUs, and computers) in bulk via CSV import - Perform AD tasks such as password reset, account unlock, clean up, and more - Streamline the management of AD objects such as users and OUs with customizable templates - Assign, replace, or revoke Office 365 licenses in bulk. Manage shared, remote, room, and equipment mailboxes - Create backups of AD objects and restore all attributes of an object or only specific attributes - Generate and schedule more than 200 preconfigured, granular reports on AD, Exchange, Office 365, and Google Apps - View inactive users, locked out users, disabled computers, and more in just few clicks - Create custom AD reports to obtain the exact data that you require - Export to a number of formats including HTML, PDF, XLS, XLSX, CSV, and CSVDE - Mention specific users or computers in a CSV file for generating their important details - Generate compliance reports to meet regulatory standards such as SOX, HIPAA, and more - Granularly delegate AD, Office 365, and G-Suite tasks to help desk technicians for specific Ous - Delegate tasks such as resetting passwords, creating users, and more - Delegate without elevating technicians' privileges in Active Directory - Automate routine Active Directory tasks such as AD clean up - Configure a review-approval workflow to execute AD tasks with a structured flo - Exercise control over automated tasks by using workflow with automation - Manage users from anywhere- Reset passwords; unlock, enable, disable and delete accounts - View reports on locked out, disabled, password, expired and inactive users - View, manage, and execute AD workflow requests - Audit Windows file servers, failover clusters, NetApp, and EMC storage to document changes to files and folders - Track changes across Windows servers, printers, and USB devices with a summary of events - Leverage advanced statistical analysis and machine learning techniques to detect anomalous behavior and defend against cyber attacks - Monitor, report, and alert on domain controllers in real time - Utilize over 200 detailed, event-specific GUI reports - Track changes to Group Policy and all AD objects - Track logons and logoffs to workstations - View and schedule graphical reports - Report on employee attendance, total active and idle time - Monitor activity on terminal services - Track file creation, modification, and deletion - Get forensics on security and permission changes - Monitor network shares AD45 Utilize file integrity monitoring (FIM) - Also monitor, alert and report on AD FS, AD LDS, LAPS, DNS, NAS devices, scheduled tasks and processes, Windows security log and other system events - Track all changes to Windows AD objects including users, groups, computers, GPOs, and	عد د	نظ ام التد قي ق الام ني للد يل الذ شد ط	ز ظ ام



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحد القياس	البند	ال فئة
OU's. - Achieve AD monitoring with a single, correlated view of all the activities - Monitor every user's logon and logoff activity, including every successful and failed logon attempt across network workstations - Audit Windows file servers, failover clusters, NetApp, and EMC storage to document changes to files and folders - Audit file access - Monitor system configurations, program files, and folder changes to ensure file integrity - Audit removable storage devices. Audit print servers - Monitor RADIUS logons			
M640 Chassis - 2.5". • 2 x Gold 5220 -2.2Ghz - 16 Core. • 8x 16GB DDR4 2666Mhz RDIMM. • 16 • x 900 GB 15K SAS drives. • PERC H330 Mini Blade Controller (RAID 0/1/5/10/50). • 2 x Pass Through Mezz Adapter - VRTX. • Intel X520 10GbE DP KR NDC. • IDSMD with 2 x 16GB SC . .cards. • Dell iDRAC9 License Enterprise	عدد	خادم server	إجهزة



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

ال فئة	البند	و د ة ال ق ي ا س	المواصفات
اج ه زة	نظ ام ادار ة ص للا يا ت دخ ول م سد ؤو ل الاز ظ ة PA M	عد د	"يجب توريد وتركيب نظام ادارة صلاحيات دخول مسؤول النظام PAM الحلول مع كامل مستلزماتها. توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: The product should be deployed in a variety of footprints including a physical appliance, a VMware virtual appliance, , and provide equivalent capabilities in each.. The product provides a bastion-host gateway to broker - as proxy - user access to managed target devices (*NIX, Windows, etc.) with a zero-trust posture.. The solution must be based on a fully featured Appliance, with at least Open Authentication, Zero-Trust model, Password DB, Discovery, Access Control policies, Session Recording, VMware management, Cloud Applications Management, Command Broker hosted on the same Appliance without the need of additional modules or components. The Solution must provide Load Balancing (VIP configuration, algorithms and management) and High Availability (Clustering and Disaster Recovery) capabilities within the Appliance, without the need of any 3rd party software or licenses.. The High Availability Architecture must be able to support One or Multiple Datacenters installation (WAN) without the need of 3rd party software or licenses.. The preferred PAM High Availability is Active-Active, and the Internal Password Database must natively provide a complete Replication Architecture without the need of 3rd party software or licenses. . The High Availability Architecture must be able to support Active-Active and Active-Passive Disaster Recovery installations without the need of 3rd party software or licenses. In case of Multiple Datacenter (WAN) installation, the High Availability Architecture must be able to provide the capability to use any of the PAM Sites to recover (for DR or any other unavailability scenarios) the main Production Site, without the need of 3rd party software or licenses.. The PAM Solution supports an upgrade process in-place, using the provided GUI and based on patch/payload files.. The product's Appliance is highly scalable, supporting (for example) 3000 concurrent SSH sessions, 1500 concurrent RDP sessions, or 2000 concurrent connections of mixed SSH and RDP regardless of which form factor (physical or virtual) is used and with Session Recording active. The product adds scale by simply adding new appliance to a cluster.. The PAM solution must be accessed via a dedicated "PAM Client" to be installed on the Users' Desktops/Laptops. The Session Recording capability must provide a Primary Storage and a Failover Storage, with the possibility to disable completely the Access to the managed devices when the Session Recording storage is not available/mounted. The product supports a variety of authentication methods including LDAP v3 compliant directories including AD, OpenLDAP, RHDS, Novell eDirectory, etc., RADIUS and MFA solutions that integrate with RADIUS, x.509 certificate (browser or Smartcard-based), RSA SecurID, SAML 2.0 as a Relying Party, as well as combined authentication such as LDAP + RADIUS.. The product includes an internal user store for maintaining product administrator's identities, to ensure independence from an external directory for protecting privileged operations.. The product logs all activity including administrative operations and user activity. User Activity attributes actions to the named user.. The PAM Solution must provide proof of compliance with the following



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
Certifications: 23 NYCRR 500, FISMA, HIPAA, NERC, NRC, PCI/DSS, GDPR. The PAM Solution must provide proof of compliance with the Common Criteria certification with a NIAP approved Enterprise Security Management Protection Profile (NIAP- Preferred Protection Profile). The Solution must provide a Target Connector Framework, enabling to easily build custom Connectors for remote targets that are not supported with out-of-the-box Connectors.. The PAM Solution can provide an add-on for reporting any suspicious behavior with privileged access and proactive remediation actions.. This Behavioral Analysis add-on must be based on an Appliance and specifically designed, configured and specialized for collecting and elaborating the PAM data.. 2FA Solution - 2nd Factor Authentication Credentials (i.e. Mobile OTP, Soft Token, etc.) should be generated on a Mobile App and without the need of any connection or network access for the mobile device.. 2FA Solution - 2nd Factor Authentication Credentials (i.e. Mobile OTP, Soft Token, etc.) must support also Push Notification and SMS as alternative methods to receive/consume the second factor credential.. 2FA Solution - 2nd Factor Authentication Credentials technology must be patented by the vendor and must not require any kind of user password being in transit on the network . The PAM Solution controls access to many different endpoint types such as UNIX/Linux via SSH or Telnet, Windows and RDP Published Apps, Databases, Mainframes via TN3270 or TN5250, Network devices via SSH or telnet, web-based apps via http/https/SAML, etc.. The product controls user access to managed systems through the appliance using a "Zero Trust" model that prevents access that is not explicitly granted.. Provides in-line command filtering using white lists/black lists for SSH, network devices and Mainframe command line operations. No endpoint agent needed.. Can detect when violations of the white list/black list rules occur and can automate action as a result including warning the user, logging off the session, or disabling the user's account within the product as well as alerting when the event occurs.. The product provides highly efficient integrated video session recording with low storage requirements. Videos are fingerprinted to ensure they have not been tampered with. Violations of policies are highlighted in the videos. Video Session Recording is supported for RDP, Telnet, SSH (via CA PAM applet and Windows Putty client), HTTP, HTTPS, TN3270 and TN5250 sessions.. The product allows administrators to terminate active sessions from within the product's Web interface.. Provides a socket filtering capability to prevent unauthorized outbound TCP/IP connections on managed systems including *NIX and Windows.. The product supports using RDP to published applications in which the user can be confined, rather than requiring RDP to a full desktop.. The product allows local/desktop applications to be invoked for connecting to the managed devices via the appliance.. The product supports logging in to the managed applications using SAML 2.0, with the product as the IdP.. The product provides fine-grained control over AWS console features so that administration of AWS can be secured, delegated and managed. The product uses AWS APIs to manage all access to AWS. New instances of AWS servers are automatically detected and managed.. The product controls and audits access to privileged accounts in VMware vCenter. New Virtual systems are automatically detected			



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	و د ة ال ق ي ا س	ال ب ن د	ال ف ئ ة
and managed.. The product provides fine-grained control over VMware NSX so that administration of NSX can be secured, delegated and managed.. The product Controls and Audits administrative access to MS Office 365.. The product can be deployed as an MS Azure instance and can Control and Audit administrative access to MS Azure. Kerberos Authentication for RDP sessions when users are logged in with PIV/CAC smart cards (PIV pass-thru).. The product controls access to high-privileged accounts such as *NIX root and Windows Administrator, sa, etc.. The product provides automated login to managed endpoints using privileged credentials, without revealing the credentials to the user.. The product supports password management for privileged accounts, to rotate passwords after it has been used or viewed, and/or at scheduled intervals. Password composition and view policies can be customized.. The product supports SSH Key management for managed endpoints across the hybrid enterprise, including on-prem, private or hybrid cloud, and IaaS-based devices for authentication of privileged accounts and rotation of SSH keys.. The product allows secondary authentication (such as to sudo, databases or other targets that require a second authentication) to be invoked by authorized users and optionally supplies the privileged account credential when it is required.. The product allows "Learn Mode" to build transparent login configurations to acquire credentials when using RDP published applications.. The product uses a simple "Learn Mode" to acquire credentials of web-based apps by allowing users to map the applications credentials to the fields of the product.. The product can require an approval by designated users as a condition of accessing the credentials for managed accounts.. The product can validate that a Ticket exists as a condition of granting access to a privileged credential using the customers help desk including CA Service Desk Manager, BMC Remedy, HP Service Manager, ServiceNow, and Salesforce Service Cloud.. This integration must be provided out-of-the-box. The product provides tools/APIs for enabling applications that require access to privileged accounts to access credentials programmatically, eliminating the need to "hard code" credentials into the script or application. Password can be rotated automatically.. The product should be able to manage passwords stored in plain, hardcoded in system files or user-defined files, JDBC definitions, etc. including within application configuration files, code or scripts.. In addition the solution must provide a JDBC driver wrapper for addressing the J2EE applications use case.. The A2A capability must support at least the following languages: Java, Perl, C, C++, C#, Korn Shell, C Shell, PHP, Python, PowerShell, Visual Basic, Visual C++, VB Script, and JavaScript.. The product should have capabilities to provide credentials for authenticating applications/scripts at run-time and using batch processes.. The A2A capability must operate with a full secured process, as follows:.. · The Account must be classified as A2A. · The Account must have an "alias" so the programmers don't need to know the credential. · PAM must verify the agent/client who's asking the credentials. · PAM must verify the name of the alias. · PAM must verify the script or program invoking the request. · PAM must verify the user ID invoking the request. · PAM must verify the path of the calling program. · PAM must verify the hash of the calling program			



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة .			
• Chassis 8x2.5 Front Storage. • Trusted Platform Module Trusted Platform Module 2.0 V3. • • Chassis 2.5" Chassis with up to 8 Hard Drives (SAS/SATA), 3 PCIe Slots, 2 CPU. • CPU Gold 5317 3G, 12C/24T, 11.2GT/s, 18M Cache, Turbo, HT (150W) DDR4-2933. • CPU Gold 5317 3G, 12C/24T, 11.2GT/s, 18M Cache, Turbo, HT (150W) DDR4-2933. • Memory Type 3200MT/s RDIMMs. • Memory Type 32GB RDIMM, 3200MT/s, Dual Rank, 16Gb BASE x8. • HDD 960GB SSD SAS ISE Read Intensive 12Gbps 512 2.5in Hot-plug AG Drive, 1 DWPD,. • HDD 1.92TB SSD vSAS Read Intensive 12Gbps 512e 2.5in Hot-Plug ,AG Drive SED, 1DWPD,. • Power Supply Dual, Hot-plug, Power Supply Fault Tolerant Redundant (1+1), 800W, Mixed Mode. • Rack Power Cord Rack Power Cord 2M (C13/C14 10A). • NIC Ethernet X710 Quad Port 10GbE SFP+, OCP NIC 3.0. • OS VMware ESXi 7.0 U3 Embedded Image (License Not Included). • OS VMware vSphere 7 Standard for 1 CPU, up to 32 cores, 1YR VMware SNS. • Warranty Parts Only Warranty 12Months, 12 Month(s). • Support ProSupport and Next Business Day Onsite Service, 12 Month(s)	عدد	خوادم المخطط الم حايمة DMZ Server	اجهزة



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحد القياس	البند	ال فئة
"يجب توريد وتركيب نظام الكشف و الاستجابة لأنظمة الشبكة NDR الحلول مع كامل مستلزماتها. توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: . The solution should be available as hardware appliance or virtual appliance or as a software . The solution should provide all the required functionalities in one box only that consumes a maximum of 2U Rack Space without the need to add more boxes Support out-of-band management. Built in GUI for system management. Management interface must be accessible from any standard browser and work on any standard OS. (Windows, MacOSX, Linux, Firefox, Safari, Chrome, Internet Explorer). Solution should not require the installation of any client (thick or thin) . Support up to 200 individual users accounts for management. Support at least 10 unique users logged in simultaneously. Support LDAP based authentication for management access. Support separate management roles for administration and users. Support encrypted session for all management functions (SSL, SSH). Support an integrated database and reporting engine that does not require user-configuration, maintenance, or tuning. . Support an audit log of management activities. Support safe downloading of reconstructed artifacts, either individually or as an archived collection. Support sending system alerts and events to an external syslog and log aggregators. Support SNMP v2 & v3 queries for system health and status. Support sending SNMP traps for system alerts and events. Support sending Email notifications for system alerts and events. Support an API for extended attribute extraction and protocol classification. Ability to revoke a user's access. Support central management for at least 35 remote capture devices. Support encrypted communications between the central manager and all remote capture devices. Support interacting with and configuring all remote capture devices simultaneously from the central manager. Support federated queries to all devices under management from the central manager.. The communication between the central manager and the remote devices should not utilize more than 3% of a 1 Gbps link. Support out-of-band passive deployments. Support a VM based deployment. Support a VM deployment that can regenerate intra-guest VM traffic from a virtual switch to a physical network segment. Support a bare metal install on approved provided hardware. Support cluster mode deployments for enhanced throughput and processing. Support Direct Attached Storage to increase forensic retention beyond internal storage. Support capturing and retaining regenerated traffic from, aggregation TAPs, SPAN ports, and mirror ports. Support efficient capture on multiple interfaces simultaneously. Support both optical and copper connections for capture. Support a minimum of 4x 10 Gbps copper connections for capture. Support capturing inbound and outbound data concurrently. Support full Berkley Packet Filter (BPF) functionality for inclusive/exclusive packet capture per capture interface. Support processing, capturing, and recording packets at a sustained 5 Gbps for 6 hours with 99.999% data capture rate.. Support network links that can burst up to 10 Gbps. Support capture and processing of traffic that is 802.1Q tagged. Support data storage solutions and scale up to 800TB per appliance . Support capture and query of both IPv4 and IPv6 traffic.	عدد	نظام الكشف شبكة و ال س ج ة لأ ظ مة ال ش ة ND R	ز ظ ام



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
Support exporting RAW PCAP data from query results. Support real-time regeneration of traffic flows to secondary capture or analysis solution.. Support playback of historical traffic based on specific time frames to secondary capture or analysis solution. Support the following classes of reputation services: virus scanner, domain reputation, URL reputation, hash reputation, and file analysis integration.. Solution should provide automated workflows and instant reports deliver complete forensic details, contextual awareness and actionable intelligence about breaches—including root-cause exploration and reconstruction of breach activity for fast time-to-resolution.. Support extracting files/artifacts from flows in common network protocols (HTTP, SMRTP, SMB, IM, etc.). Support an integrated solution to preview artifacts/files that have been extracted from flows.. Support interpreting JavaScript to discover obscured content or exploits. Support geo location for identifying the sources of communications by country. Support storing meta-data for 3x longer than capture data. Support efficient DPI inspection regardless of the number of protocol classifiers instantiated. Support alerts for any indexed metadata. Support real-time alerting for reconstructed files . Support a hashing mechanism for extracted file types.. Support near real-time verdict tracking via automated threat intelligence, reputation services AND malware detonation platforms.. Support user configurable dashboards. Support reporting on any and all flows for a predetermined time frame. Support alerting on any single or combination of metadata attribute(s) in near real-time. Support reconstruction of multiple platform file types, including Windows executables and archives (zip, exe, dll, PE, etc.), Mac .pkg and .dmg files, Android .ap files, etc.. Support extraction of large files, i.e. there should be no restriction on the file size of the artifacts being extracted.. Ability to save reports for later use.. Easy configuration of reporting tools.. Support classification and indexing of traffic within nested (tunneled, encapsulated) protocols at least 10 layers deep.. Support Active Directory Integration so it can perform mapping between users and all related attributes such as IP addresses. Support report caching for consecutive queries of the same data. Support integration with other network tools via REST or other API.. Support integration with external firewalls. Support integration with external IPS solutions. Support integration with external SIEM solutions. Support integration with external malware analysis solutions . Support integration with external endpoint forensics solutions. Support session flow . . توفير الدعم الفني والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لا يندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة .			



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحد ة الق ياس س	البند د	ال فئ ة
"يجب توريد وتركيب نظام حفظ وسائط الحزم عبر الشبكة TAP الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي:.. Support tap the links set up with TAPs (and/or SPANs), even if the traffic is not under continuous monitoring.. -Network packet broker with 40 GBE tap feature or more based on the network infra. -Must support captures, aggregates, and distributes network traffic for monitoring nd analysis purposes . port configuration multiple 40GbE ports for connecting to network links, switches, or routes, . -Support packet filtering, load balancing, packet slicing and protocol decapitation . توفير الدعم الفني والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة ."	عدد	نظام حفظ وسائط الحزم عبر الشبكة TAP Network packet broker	نظام
"يجب توريد وتركيب أجهزة فك التشفير عبر الشبكة SSL Broker الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي:.. SSL/TLS visibility. Provides SSL/TLS decryption and encryption, strong cipher support, and flexible deployment.. Dynamic service chaining. Provides service insertion, service resiliency, service monitoring, and load balancing.. Context-based intelligence. Scales with high availability. Granular control . توفير الدعم الفني والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة ."	عدد	نظام فك التشفير عبر الشبكة	نظام



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحد ة الق ياس	البند	ال فئ ة
"يجب توريد وتركيب نظام حماية تسريب البيانات Data loss prevention الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: . Detect sensitive corporate operations documents (Governance, Procedures). . Detect sensitive corporate business documents (Legal, M&A, Marketing). . Detect sensitive design documents (Drawings, Project Plans). . Management console supports two-factor authentication for user authentication.. . All communications from different modules with the management console must be encrypted. . Supporting security logging and auditing of administrative actions.. . The solution must support policy tuning workflow and automation, centralized policy, system events, and incidents from management console . . All DLP modules (email, web, network, servers, storage, Cloud, and endpoints) must be managed by a single management console.. . The solution must have one unified policy applied on all DLP modules (email, web, network, servers, storage, Cloud, and endpoints).. . Supporting multiple concurrent administrators.. . Measure risk reduction and demonstrate compliance by using the reports generated from the management console. . Ability to integrate with classification tool. . Accommodating the following content-aware detection techniques: partial and exact document matching, images, structured data fingerprinting, statistical analysis, extended regular expression matching, and conceptual and lexicon analysis using the following detection technologies: vector machine learning, indexed document matching, remote EDM indexer, and exact data matching. . Includes predefined policies or templates to cover standard regulations and best practices. . Policies can be created using user authentication directory services (LDAP), utilizing user group and username information. . Policies can be created based on IP, email address or domain (both as source and destination). . Policies can be created based on method of data transfer (protocol, USB devices, etc.). . Policies can be created based on port. . Policies can be created using combinations of data elements of structured or unstructured data. . Exceptions can be built into rules to minimize false positives. . New rules can be created by copying an existing rule. . All incidents (gateway, endpoint and discovery) report to a central management console. . All policies (gateway, endpoint and discovery) can be managed from a central management console. . Incident details retain source IP address, destination IP address, protocol, and port. . Incident details retain sender e-mail address, recipient e-mail address, and SMTP headers. . Incident details retain all content in the transaction, not just the content that violated policy. . The solution should be capable of defining DLP Policy based on user risk score and response based on user risk score.. . The solution should be capable of protecting and building policies based on Zero trust users regardless of whether the user is authorized or non-authorized to use the data.. . Incident details retain all attachments in the transaction, not just the attachment that violated policy. . Provides for pre-registration (fingerprinting) of known sensitive data . . Provides pre-registration in the form of fingerprinting both structured and unstructured data . . Structured data fingerprinting method provides for specifying which combination of	عدد	نظام حماية	رخصة



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
data fields constitute a match on a per-policy basis . • Database fingerprinting process allows for direct connection via ODBC (name each supported database) . • Supports detection based on document type, even if file extension has been changed . • Supports sensitive content in file types of any kind . • Supports recursive review of archived files . • Supports inspection and detection of files of any format (note how many file formats). . . . Incidents can be assigned automatically to reviewers . • Incidents can be sorted by severity level . • Incidents can be sorted by sender, recipient, source, destination, protocol, and content type . • Incidents can display and highlight a summary content that violated the policy . • Incident views can be customized based on content pertinent to the reviewer's role and preferences . • Incidents can be grouped by sender, recipient, source, destination, etc., for easy management . • Incident views can be created and saved for easy recall . • Incident reporting can be shared with SYSLOG compatible systems . • Multiple incidents can be assigned to a case for further investigation and remediation . • Cases can be reassigned to different owners after creation . • Case content can be exported with full content and attachments for review by an external reviewer . . . • Interfaces with MTAs to provide for SMTP blocking . • Interfaces with web proxies using ICAP standard for HTTP/FTP blocking . • Supports analyzing SSL traffic using compatible ICAP proxies . • Supports blocking of SSL traffic using compatible ICAP proxies . • Supports notification of policy violation to end user (violation) for email violations . • Supports notification of policy violation to end user (violation) for violations using protocols other than email (HTTP, FTP, etc.) . • Supports notification of policy violation to management . • End user notification is customizable . • End user notification is customizable based on type or severity of violation . • Event reporting includes an explanation of which policy was violated and which portion of the content caused the violation . • Supports "coach mode," notifying user of pending infraction and allowing them to correct or provide justification to proceed. . • Restrict access to specific policy violations based on company role (Compliance, HR, Legal, Finance, etc.) . • Restrict access to policy violations on a per user and per group basis . • Restrict access to actionable functions within policies based on role (Reviewer, Policy Writer, Investigator) . • Limit access to incident details and attachments based on role . • Mask PII or PCI information contained in match summary display based on role . • Restrict access to after-the-fact search capabilities based on role . • Restrict access to case creation, reviewing, modification, or deletion based on role . • Integrate with LDAP for unified user authentication . • Integrate with LDAP groups for unified role definition . • Audit and securely store all user transactions . • Granular access controls to separate system maintenance functions from sensitive information access . • Secure access to the management console using HTTPS . • Secure remote maintenance access to the console using SSH . • Secure storage of local account passwords . • Security hardening measures to remove unnecessary services and network protocols to the DLP systems . • All access to device is logged for an audit trail . • All changes to device configuration or policies are logged . • Audit log is protected from access and manipulation (even via command line or accessing the backend			



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحد ة الق ياس س	البند د	ال فئ ة
of the device). • Supports centralized reporting for multiple network devices in a single reporting console . • Supports reporting on gateway, endpoint and discovery in a single reporting console . • Provides executive dashboard . • Allows for custom report creation . • Custom reports can be saved (memorized) and re-run . • Reports can run automatically on daily, weekly or monthly basis . • Generate reports in PDF or CSV format . • Develop reports built around stakeholder requirements . • Develop reports based on top (X) policy violations, senders, content type, protocol, etc. . • Build reports from GUI based on current view attributes (columns, content filters, view, etc.) . • Build detailed reports based on historical traffic/content analyzed . • Export historical records for archiving or external review/analysis . • Purpose built appliance . • Turn-key installation and deployment . • DLP system, databases, and assets can be managed by a single department in an enterprise environment . • Single data-at-rest inspection device can analyze and index all sensitive content for data stores up to xxx TB . • Supports sustained bandwidth of up to xxx Mbps with bursts to xxx Mbps . • Supports high availability . • Supports fail over . • Supports network attached storage . • Supports offline archiving of data (in what format) . • Supports encryption of sensitive data fields within the database for PCI compliance . • Supports encryption of entire database . • Provides backup and restore capability of event log data, policies and profiles and system configuration . • Supports load balancing of multiple inspection devices without third-party load balancing devices . • Multiple inspection devices can be managed from a central console (single interface) . • Settings, policies and configurations are automatically replicated across multiple inspection devices . • Capable of monitoring both inbound and outbound connections . • Manages event expiration log as storage limits are met . • الدعم الفني والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للطلول والبرامج المقترحة .			



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

ال فئة	ال بن د	و د ة ال ق ي ا س	المواصفات
ز ظ ام	نظ ام حم اية وام ن دخ ول ال مش كة	عد د	"يجب توريد وتركيب نظام حماية وامن دخول الشبكة Network access control الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: 4 . Monitor endpoint status on the network in real-time.. 4 . medium network appliances . • Enforce granular policies for access control and endpoint compliance. • Address security operations with automated network security remediation. • Act as an integration hub to share data with other cybersecurity tools. . Solution Must support Centralized Management with a Centralized License. The proposed solution must support Enterprise management via Virtual Machine or Appliance to manage all the appliances from a single admin console when multiple Appliances/Virtual Machines are used to cover the solution. Solution Must support High Availability for the Enterprise Management. Solution Must Support Interactive Dashboard for the Visibility and the Compliance Status. Solution Must support Asset inventory Dashboard. Solution Must support up to 10 Endpoint Appliances Configuration management. Proposed Solution must have two appliances in the main DC with the following Specs to manage the solution and for centralized license.. Proposed solution should be capable of supporting 10,000 endpoints and managing up to 200 Layer-2/Layer-3 network devices.. Proposed Solution should provide Visibility & Control into (Campus Network, Data Center, Cloud, OT and IoT).. Proposed Solution must be scalable for Future expansion without requiring major Architecture changes.. Proposed Solution must support continuous monitoring and assessment for the endpoints while connected to the Network Infrastructure (Periodic reassessment). Proposed Solution must support Windows, Linux, and Mac OS Operating systems, and must support legacy Windows Operating Systems.. Proposed Solution should be capable to block the access of endpoints which are connected on unmanaged network (I.e Unmanaged Switch).. Proposed solution should be capable of identifying IOT devices such as: IP Cameras, VOIP, Projectors, HVAC devices, etc.. Proposed solution must support IoT credential assessment (Default Credentials, Default SNMP Communities, Default Factory Credentials ..Etc.). Proposed Solution must support passive and active check for well known Vulnerabilities and IOC's. Proposed Solution must support open ports and map it to the devices.. Proposed Solution must support IP to MAC Mapping on wired connected devices based on Switch IP and Switch port.. Proposed Solution must support Data Center Visibility including and not limited to VMware, ACI and all components related to it.. Proposed Solution should have the capabilities to check if VMware Tools are installed on a virtual machine. Such as: . • Tools installed and up to date . • Tools installed but upgrade recommended . • Tools installed but need to be updated . • Tools installed but VM is not managed . • Tools not installed . Proposed Solution should have the capabilities to check if the ESXi host profile is compliant, non-compliant or unknown.. Proposed Solution should have the capabilities to classify different types of VMware virtual machines and servers, such as: . • Virtual Machines . • ESXi Servers . • vCenter Server. Proposed Solution should have the capabilities classifying virtual machines based on VMWare NSX security groups or



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
based on NSX security tags. . Domain, Domain User, Domain Member, OS-Class, IP of the connected switch, Switch Port, Switch Port VLAN, Switch Port Status, Switch Vendor, Access status.. Proposed Solution must support Passive discovery with DPI for IT and IoT protocols.. Proposed Solution must support Passive discovery with SPAN port traffics analysis. .. Proposed Solution should support Access Restriction Based on encryption. Proposed Solution should support Access Restriction Based on patches . Proposed Solution should support Access Restriction Based on AV . Proposed Solution should support Access Restriction Based on Managed Device . Proposed Solution should support Access Restriction Based on AD/LDAP account . Proposed solution should be capable of support/integrating with wide variety of Network switching vendors such as Cisco, Juniper, Arista, Huawei, Brocade / Foundry, etc. without making any change on the existing setup or requiring upgrade to this infrastructure elements.. Solution provided shall provide unrestricted number of Virtual Appliances Licenses to cover our requested total IP Endpoints.. Proposed Solution appliance should support (centralized, distributed and hybrid) architecture.. Proposed Solution should not require any network architecture change . Proposed solution should be deployed without requiring 802.1X for Access Control features. Proposed Solution must integrate with infrastructure devices by using SNMP, CLI. Proposed Solution should support visibility to all the IP enabled devices connected in the network (agentless using Passive and Active Fingerprinting techniques) for both Traditional Endpoints and Industrial IoT Devices. . Proposed solution should not require an agent to perform endpoint profiling, posture Assessment & baselining for full NAC solution features (for managed devices). Agent can be used for managed AD-member Windows endpoints. . Proposed solution should provide information regarding the endpoint connected to the network, such as IP Address, MAC Address, NetBIOS Name, NetBIOS . Proposed solution should support Device tracking (What, Where, Who, When and how). Proposed solution should be capable to provide Post-connect monitoring in an agentless manner. . Proposed Solution Should capable to achieve all feature & functionality with agentless, Agent based & Dissolvable agent mode deployment.. Proposed Solution should provide Visibility & Control into Data Center virtual-machines and its virtualized infrastructure. Proposed solution must support hardware-based and virtual appliance.. Proposed solution should be scalable of supporting 1M+ IP endpoints and managing Layer 2 / Layer 3 devices in non-dot1x mode.. Proposed Solution should support high-availability and clustering.. Proposed solution should allow administrators to review events, do searches, and run reports from a Web UI. . Proposed solution must support the following reporting capability:. 1- Automatically generate reports on scheduled basis.. 2- Administrators should update or define custom reports.. 3- Ability to run certain reports based on security role. 4- Support scheduled reports be delivered via e-mail. Proposed solution should support event logging via severity. For forensic and faster network troubleshooting, the solution should log each & every session/ all important events that pass through and provide simple graphical and statistical reports. & Logs should be exportable to external log server.. The solution should provide real time alerts via eMail..			



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
Proposed solution should support Role Based Access Control for management. Proposed support alert notification. Proposed solution should support report generation in csv, xls or pdf. Proposed Solution should support creation of custom reports. Proposed Solution should support helpdesk notification. Proposed solution must support non-disruptive, out-of-band model (with all feature & functionality) to ensure network keeps functioning even if the solution goes down for whatever reason.. Proposed solution must support built-in configuration wizards and customizable policy templates for rapid time-to-value.. Discuss how can the proposed solution prevent end-stations failing to meet policy from accessing the network and the alternatives for quarantining and/or fixing computers out of compliance.. Proposed solution quarantine method should not rely on specialized hardware or software.. Proposed solution should support VLAN restriction, Switch port block, Dynamic ACL, Endpoint ACL, Port based ACLs and virtual firewalling.. Proposed solution should support performing Pre and Post admission check, policy recheck. Proposed solution should support Compliance and Remediation abilities. Proposed solution should support Guest Management without requiring additional license.. Describe proposed solution policy configuration options: those configured out of the box (best practices) and the flexibility for the state to customize the solution (status checking methods, breadth of status checking options).. Proposed solution should support automatically detecting new endpoint connected to the network. Please describe how this can be done with proposed solution.. Proposed solution should be cable of identifying virtual versus physical hosts. The solution should be able to identify the vendor of the NIC of endpoints. The solution should be able to identify the switch name and the port on the switch to which and endpoint is connected. Proposed solution should be able to identify the user, email address and IP address of managed devices without requiring an agent through integration with existing LDAP server.. Proposed solution should be able to identify on managed the presence/absence of (without requiring an agent):. Windows Services. Windows process. Open ports. External devices. Dual Home. P2P application.. IM application.. Proposed solution should provide IOC scanning to discover and mitigate threats from infected endpoints.. The Solution should be able to identify and classify the Operating System and patch levels installed on managed devices without requiring an agent.. Proposed Solution should support the following User Directory Servers:. • Active Directory. • eDirectory.. • Sun Directory Server.. • Notes.. • Open LDAP Server.. • Radius Protocol Server.. Proposed solution should support the following Widows OS:. • Windows10. • Windows 8. • Windows 7. • Windows vista. • Windows 2000. • Windows XP. • Windows Server 2016 Technical Preview. • Windows Server 2012. • Windows Server 2008. • Windows Server 2003 . Proposed solution should support the following MAC OS:. • OS X 10.6 (Snow Leopard). • OS X 10.7 (Lion). • OS X 10.8 (Mountain Lion). • OS X 10.9 (Mavericks). • OS X 10.10 (Yosemite). • OS X 10.11 (El Capitan). • Mac OS 10.12 (Sierra). • Mac OS 10.13.x (High Sierra). • Mac OS 10.14.x (Mojave). • Mac OS 10.15.x (Catalina). Proposed solution should support the following Linux OS:. • CentOS. • Debian . • Fedora . • Kali. • Mint. • Red Hat Enterprise Linux. • Red Hat Enterprise Desktop. • Red Hat. • Open Suse. • Suse			



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
Enterprise. • Ubuntu. • IGEL. Proposed Solution should support posture assessment of Mac and Linux endpoints while providing an inventory of applications, processes and open ports on an endpoint. In addition, solution should include remediation actions such as kill processes, run scripts, set registry keys or disable dual-homed device adaptors. . Proposed solution should Integrate with LDAP/AD. Proposed Solution should provide built-in method to identify IoT (SNMP / SSH / Telnet) weak and default credentials with ability to add custom credentials to the posture assessment engine. Proposed solution should support Integration with SCCM without requiring creation of any SQL queries (integration should be simple, and out of the box). Proposed solution should support both copper and fiber interfaces (1G/10G).. The solution should support bi-directional information sharing and workflow automation with security technologies such as Advanced Threat Detection (ATD), Vulnerability Assessment (VA), Enterprise Mobility Management (EMM), Next-Gen Firewalls, Endpoint Protection Platforms (EPP) and Security Information and Event Management (SIEM) tools help accelerate system-wide response and achieve operational efficiencies. The OEM should provide a list of all the currently supported integrations.. The Configuration of the solution must be from the vendor by a certified professional service engineer ..the solution must be from the vendor by a certified professional service engineer الدعم الفني والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة .			



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

رقم ال فئة	البند	و د ة ال ق ي ا س	المواصفات
ر د ص ة	ن ظ م م ك ا ف د ة الم ل ف ا ت الخ ب ي ث a	ع د	توريد وتركيب الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. توريد وتركيب الرخص اللازمة للخوادم (350 خادم). توريد وتركيب الرخص اللازمة للأجهزة الطرفية (150 جهاز). . The technology shall support the application whitelisting and advance threat protection . The techonolgy shall support host firewall . Desktop firewall to control network traffic and protect against attacks. Central management console to monitor and manage endpoints. Antivirus and spyware to scan and remove malicious software. Intrusion prevention to prevent unauthorized access and exploits. Suggested solution must support below client operating systems:. . Android, Apple IOS.. . Windows on Arm devices, Windows in S Mode.. . Windows Vista (32-bit, 64-bit) . . Windows 7 (32-bit, 64-bit; RTM and SP1) . . Windows Embedded 7 Standard, POSReady, and Enterprise (32-bit, 64-bit) . . Windows 8 (32-bit, 64-bit) . . Windows Embedded 8 Standard (32-bit and 64-bit) . . Windows 8.1 (32-bit, 64-bit), including Windows To Go . . Windows 8.1 update for April 2014 (32-bit, 64-bit) . . Windows 8.1 update for August 2014 (32-bit, 64-bit) . . Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (32-bit, 64-bit) . . Windows 10 (32-bit, 64-bit) . . Windows 10 Fall Creators Update (version 1709) (32-bit, 64-bit) . . Windows 10 April 2018 Update (version 1803) (32-bit, 64-bit). . Windows 10 Oct 2018 Update (Version 1809) (32-bit, 64-bit). . Windows 10 June 2019 Update (Version 1903) (32-bit, 64-bit). . Windows 10 Des 2019 Update (Version 1909) (32-bit, 64-bit). . Windows 10 May 2020 Update (Version 2004) (32-bit, 64-bit). . Windows Server 2008 R2 (32-bit, 64-bit; R2, SP1, and SP2) . . Windows Small Business Server 2011 (64-bit) . . Windows Server 2012 . . Windows Server 2012 R2 . . Windows Server 2012 R2 update for April 2014 . . Windows Server 2012 R2 update for August 2014 . . Windows Server 2016. . Windows Server 2019. . Mac OS X 10.10, 10.11, 10.12, 10.13, 10.14 (including 10.14.5), 10.15. . Amazon Linux 1, 2.. . CentOS 6.X, 7.x, 8.x ; 32-bit and 64-bit. . Debian 6.0.5 Squeeze, Debian 8 Jessie; 32-bit and 64-bit . . Fedora 16, 17; 32-bit and 64-bit . . Oracle Linux (OEL) 6U2, 6U4, 6U5, 7, 7.1, 7.2, 7.3 . . Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U4 , 8. . SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12, 12 SP1 - 12 SP3, 15 64-bit . . SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12 SP3, 64-bit . . Ubuntu 12.04, 14.04, 16.04, 18.04; 32-bit and 64-bit". "Suggested solution must support below Virtual Environments:. . Microsoft Azure . . Amazon Workspaces . . VMware WS 5.0, GSX 3.2 or later, ESX 2.5 or later . . VMware ESXi 5.5 - 6.7. . Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016 Hyper-V, 2019. . Citrix XenServer 5.6 or later . . Virtual Box by Oracle". Solution should able to Detects and blocks malicious software in real time, including viruses, worms, Trojan horses, spyware, Adware, and RootKit.. Endpoint solution technology should include a behavioral based technology apart from providing the signatures for known threats, vulnerability add heuristic based approach. It should be able to score both good and bad behaviors of unknown applications, enhancing detection and reducing false positives without the need to create rule-based configurations to provide protection from unseen threats i.e. zero-day threats.. Solution firewall engine should have option to allow or block support of network protocols, including



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحد القياس	البند	ال فئة
Ethernet, Token Ring, IPX/SPX, AppleTalk, and NetBEUI. Can block protocol drivers (example: VMware, WinPcap) and should have Adapter specific rules - e.g. Ethernet, Wireless, VPN. Proposed IPS solution should allow customer to edit and create the IPS signature using snort-based format if required.. Solution should able to block devices based on Windows Class ID and should include USB, Infrared, Bluetooth, Serial, Parallel, fire wire, SCSI and PCMCIA.. Solution should also be able to block and give read/write/execute permission for mentioned devices.. Solution should provide application analysis, process control, file and registry access control, and module and DLL control.. "Proposed Solution should be able to deploy flexible and different security policies depending upon the AND/OR relationship of following network triggers:.. • IP address (range or mask). • DNS Server. • DHCP Server. • WINS Server. • Gateway Address. • TMP Token Exists (hardware token). • DNS Name Resolves to IP. • Policy Manager Connected. • Network Connection (wireless, VPN, Ethernet, dialup)". Proposed IPS solution should combines NIPS (network) and HIPS (host) both with Generic Exploit Blocking (GEB) for one signature to proactively protect against all variants, Granular application access control and behavior-based technology mentioned above.. Proposed Anti Spyware solution should be able to bypass Windows File System and should have Direct Access to NTFS Volume to provide raw Disk Scan for superior RootKit protection.. System Lock Down - it should be able to "Locks down" the system by fingerprinting every executable file on the system. It can then monitor all running applications and terminate any application for which the agent does not have a matching fingerprint.. Denial of service detection and protection - Should Protects the system from multiple forms of anomalous network behavior that is designed to disrupt system availability and/or stability.. Anti-spoofing - Should Protects the transmission of data from being sent to a hacker system who has spoofed their IP or Mac Address. Agent has the ability to detect and block process execution chains. It is able to detect when a malicious application tries to execute a trusted application, and then use the trust privileges of that application to access the network.. Anti-application hijacking - Should prevent hackers and web sites from identifying the operating system and browser of individual computers.. Code insertion attack prevention - Prevent malicious applications from inserting code into trusted application to bypass outbound application fire walling.. Protocol adapter attack prevention - Prevent malicious applications from using their own protocol adapter to bypass outbound fire walling.. Anti-Virus Solution proposed should not have failed Virus Bulletin 100 award ever and should have won the same more than 41 times continuously.. Proposed Personal firewall solution should be on the top on Gartner magic quadrant.. Antivirus and Antispyware policy can have options by default to choose High Security and High performance to have a right balance while deployment in the production network.. Antivirus schedules scans should get delayed/rescheduled while laptops are running on batteries.. Antivirus should have behavior-based technology to scan for Trojans, worms and key stroke loggers to protect from zero-day threats. Sensitivity level of this should get adjusted with customized scanning frequency.. Antivirus Solution should have internet browser protection and home page			



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
should be configurable if security risk changes that.. The proposed solution should have email plugin scans attachments, including zip files, removing malware before it reaches the inbox and able to Scan POP 3 email traffic including email clients Microsoft outlook, lotus notes and outlook express.. Desktop Firewall rules should be configurable depending upon the adapters including Ethernet, wireless, Dialup, VPN (Microsoft PPTP, Nortel, Cisco.. Desktop Firewall rules should be configurable depending upon the state of screen saver "ON" & "Off".. Desktop Firewall Policies should be configurable depending upon the time and day.. Product should have readymade policies including -To Make all removable drives read only, to block program from running from removable drives, protect clients files and registry keys, log files written to USB drives, block modifications to host files. Management server should have the capabilities to add multiple domains if required for the different locations to assign the different administrators for other locations. Each domain should share the same management server and database & This separation prevents administrators in one domain from viewing data in other domains. These administrators can view and manage the contents of their own domain, but they cannot view and manage the content of other domains.. To conserve the network bandwidth clients should be configurable to upload the maximum records of logs to the management server.. Product should have a security setting to block all traffic until the firewall starts and after the firewall stops except initial DHCP & NetBIOS Traffic.. The proposed AV solution should have the capability to detect the files through number of users using that file across the globe.. Browser intrusion prevention: AV should be capable enough to block the malicious downloads thorough browsers.. The proposed AV solution should rank the files based on the digital signature, age of the file, prevalence like attributes. The proposed AV client should have a visible indication whenever it connected to the AV console.. AV console should have a threat con which indicates the virus status on the Public network. The Proposed solution should have the deception feature as part of the Endpoint Agent. The Proposed Solution should have Memory exploit mitigation as a part of the same agent. The proposed solution should have EDR feature using same agent. The proposed solution should be a part of Gartner leader quadrant. The proposed solution should have endpoint deception as a part of the single agent. The proposed solution should have Host Integrity identifies and remediates non-compliant or out-of-date endpoints.. The proposed solution should have effective Advance machine learning in file analysis and behavioral analysis.. The proposed solution should have Host IPS can block and detect internal or outbound network attacks and communications and threats at the browser and network level before they make it to the disk and are executed.. Endpoint agent protected from tampering or disabling.. The proposed solution should have a cloud management console as optional. "Endpoint Detection and Response should Detect, hunt, isolate, and eliminate intrusions across all endpoints using AI-driven analytics, investigation playbooks, and unequaled threat intelligence, and it should be integrated with Endpoint Protection as a single agent. EDR Should have the below features:. Detect and Expose - Reduce time to breach discovery and			



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
quickly expose scope . • Apply Machine Learning and Behavioral Analytics to expose suspicious activity, detect and prioritize incidents . • Automatically identify and create incidents for suspicious scripts and memory exploits . • Expose memory-based attacks with analysis of process memory . Investigate and Contain - Increase incident responder productivity and ensure threat containment . • Ensure complete incident playback with continuous recording of endpoint activity, view specific endpoint processes . • Hunt for threats by searching for indicators of compromise across all endpoints in real-time . • Contain potentially compromised endpoints during investigation with endpoint quarantine . Resolve - Rapidly fix endpoints and ensure the threat does not return . • Delete malicious files and associated artifacts on all impacted endpoints . • Blacklist and whitelist files at the endpoint . • Enhanced reporting allows any table to be exported for incident resolution reports . Integrate and Automate - Unify investigator views, orchestrate data and work flows . • Easily integrate incident data and actions into existing SOC infrastructure including Splunk and ServiceNow. • Replicate the best practices and analysis of skilled investigators with automated incident playbook rules. • Gain in-depth visibility into endpoint activity with automated artifact collection ". Respondent should have as part of the platform an End Point solution that allows for detection, validation, and quarantine. All functionality must work on or off of the corporate network and without a requirement for VPN back to the corporate network. The proposed platform must be able to support multiple detection and protection technologies within their solution and should include a signature base engine that leverage on database of known files and their behavior to determine if the file is malicious, without additional payload on file detonation to detect zero day and unknown threats. The solution must have a 2-stage process for quarantine and remediation. The solution must be able to push out new upgrade versions of the endpoint agent. Endpoint agents must be able to be controlled on and off the corporate network for the purposes of detection, triage, and quarantine.. Endpoint Detection and Response solution must be able to learn about zero-day threats from other security devices doing virtual execution. Endpoint Detection and Response solution must be able to take inputs for custom indicators of compromise. Endpoint agent must have capability to protect against threats like Adware, Viruses and software vulnerabilities that exists on the endpoint solution. "Ability to fully forensically analyze identified malware and provide the following information to enterprise staff:. • Comprehensive Host Modification Report. • Copy of malware binary(s). • Full URL trails identifying all of the locations to which the malware attempts to communicate.. • Summary reports of enterprise malware events breaking down malware by type, host, and activity.. • Immediate analysis as to whether the malware maps to a previously KNOWN or UNKNOWN threat. • Severity information, illustrating how effective your other defenses would have worked against this threat.". The proposed solution should dynamically generate the required rules/policies to block/blacklist the malicious file on all endpoint clients without the need to deploy/integration with additional agents. The solution must be able to automatically quanrantine convicted bad files to a different network location.. The solution			



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
must be able to pass Indicators of Compromise (IOCs) such as file hash, to the endpoint solution so that the endpoint solution could block current and future detection of similar files. Solution should be able to detect Kernel level rootkits. Solution should be able to handle reflective DLL injection. The solution should be able to identify across endpoints if the malicious file presents with different names . The solution must provide a single view of suspicious or malicious files across the endpoints . The solution must provide file reputation based on Intelligence information gathered across the globe to aid remediation and investigation processes. The solution must provide the administrator the ability to submit files for Dynamic Malware analysis. . The solution must provide the ability to whitelist or blacklist files across endpoints . The endpoint agent must support file reputation lookup to EDR servers. The endpoint agent must support blocking, deletion and quarantine of threats. The endpoint agent must not impact the performance of the agent.. The endpoint agent must provide host-based intrusion prevention capabilities to protect against network threats targeting endpoints. The endpoint agent shall provide browser-based intrusion prevention capabilities to the endpoints. The endpoint solution must support a deep environment search for IOCs from all endpoints for files and registry keys as well as domains and URLs. The endpoint solution must be able to blacklist and erase malicious files from a single control plane. The solution must be able to quarantine endpoints from a single control plane to prevent further infection . The endpoint solution must correlate threat and malware information with the existing anti-malware solution and prioritize or de-prioritize EDR incidents based on protection status by the anti-malware solution. The proposed APT solution must also have support for current Endpoint protection as part of the platform that allows for detection, validation, containment and remediation of the Endpoint.. The endpoint agent should integrate with the endpoint protection and not require any new agent to be installed on the endpoint. . The endpoint EDR Solution should be able to remediate the endpoint using the existing Endpoint protection or its own tools.. The endpoint EDR solution should be able to detect the unknown malicious malware and should be able to submit the malware for virtual execution from endpoints independent of the Network EDR solution. . The endpoint EDR solution should be able to detect, validate, contain and remediate the endpoints when the user is on or off of the corporate network and without a requirement for VPN back to the corporate network.. The proposed solution should support containment of the endpoints and containment operations should support role-based Administrators.. The endpoint EDR solution should be able to accept IOC's and threat intelligence dynamically from the devices performing Virtual execution analysis on the network (e.g. Integration with Network and Email based EDR solution). The proposed solution should have IoC and Threat Hunt queries on clients directly at scale. The endpoint EDR solution must be able to integrate with SIEM.. The endpoint EDR solution must be able to detect the presence of files that have been written to a system but have not been executed.. The endpoint EDR solution may not interfere with normal user and business operations on the endpoint no matter how busy the system becomes.. The endpoint EDR			



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
solution must provide regular updates of threat intelligence to include indicators involving highly advanced threat groups in state-sponsored targeted attacks.. The endpoint EDR solution upgrades must be supported by standard enterprise software deployment mechanisms as well as the ability to perform upgrades to endpoints within the solution itself.. The Solution provider should allow the submission of suspicious sample for analysis at the click of a button from the solution to avoid Potential False positive . The solution should support the bare-metal and virtual execution sandbox to detect the virtual aware new gen threats.. The implementation of the solution should not add any new agent and should be part of the endpoint protection to the endpoint machine.. The Proposed solution should support flight data recorder . The proposed solution should comprehensive App discovery and inventory to scan and inventories all the apps and files collected from all the endpoints in the environment and provides detailed information about each app and file, including the name, risk score, vulnerability score, publisher, reputation, number of devices it is seen on, and so on.. The proposed solution should comprehensive application control policy and easy Policy Creation with Logical View to add any application from discovered App to white or black list.. Endpoint App Control enables trust in apps, based on a variety of app attributes, allowing or blocking apps based on one or a combination of any number of static (e.g. hash, path, publisher and certificate) and dynamic (e.g. risk and reputation score) attributes.. The App Control policy should enable rule creation on a broad range of parameters that include app name, path, and hash, reputation, publisher, user, user group, and command-line parameters.. The App Control policy should have an option to enforced in "monitor only" mode.. The proposed solution should analyze the difference between what the applications allowed in the environment and what applications run in the environment. . The proposed solution should enable to define trusted updaters which can be from discovered apps or new apps, publisher, directory, files, users, and user groups, that can install or update the software on the endpoints.. The proposed solution should prevent trusted apps from being exploited and prevent untrusted apps from infecting systems..The proposed solution should have application behavior Isolation rules capabilities to protect our devices and these rules allow or block certain application behavior, as the following isolation types. . • Browser isolation (Google Chrome, Firefox, Internet Explorer, Microsoft Edge). • Office isolation. • PDF Renderer isolation. • Platform isolation policy, which includes the following:. o OS settings. o Generic jail settings (high, medium, and low isolation). . The isolation provides rules to protect the following:. • Registry protection. • File protection. • Process interaction protection. • Process execution protection. • Network access protection. • System call protection". The proposed solution should detects any suspicious files in our network based on the intensity levels and enable us to add the detected files to whitelist or blacklist and enable us to isolate a suspicious application with a Platform Isolation policy.. The proposed solution should have ability to discover, inventory and isolate portable applications based on risk rating.. The proposed solution should have deception feature with deploying a wide variety of 'bait' - fake files, credentials, network shares, cache entries,			



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	و د ة ال ق ي ا س	ال ب ن د	ال ف ئ ة
and endpoints - throughout your environment.. The proposed solution should have endpoint deception as a part of the single agent. The proposed solution should have utilize deception techniques to monitor and notify of malicious application behavior.. The proposed solution should be supporting IOS and Android Devices. The proposed solution should prevent attacks on mobile devices running iOS and Android.. The proposed solution should proactively protecting the mobile devices from malware, network threats, and app/OS vulnerability exploits, with or without an Internet connection.. The proposed solution should have capability to enable us to take faster reaction and constant protection, even when devices are disconnected from the Internet.. The proposed solution should Proactively thwart attacks, immediately and automatically when a threat is detected.. The proposed solution should target the exact threat without impacting other resources or processes, and kick in on-demand.. The proposed solution should have protection action against risky apps threats including but not limited to (blocking communication, preventing installation, blocking communication with malicious command-and-control (c&c) servers, and blocking access to sensitive resources). The proposed solution should have protection action against network threats including but not limited to (network automatic launch of VPN tunnel when network threat is detected, blocking access to sensitive corporate resources, and blocking access to fake corporate wi-fi hotspots).. The proposed solution should have protection action against content threats including but not limited to (tunnelling all traffic through a secure web gateway, blocking access to unwanted content, and blocking SMS phishing messages).. The proposed solution should have protection action to automatically disconnect malicious VPNs. The proposed solution should have VPN technology can be implemented in always-on or on-demand mode.. "The VPN technology in the proposed solution should have the capability to operate in two ways: . 1. as an encrypted tunnel through which traffic passes securely between the device and a network.. 2. as a selective traffic blocker. (specific traffic passing through the VPN is dropped and never leaves the device).. Each of these implementations can be always-on or on-demand.". The proposed solution should have Multi-layered mobile defence against known, and zero-day attacks across every mobile threat vector.. The proposed solution should have protection from suspicious networks, apps and behaviors before they can do harm.. The proposed solution should protect privacy and productivity without negatively impacting mobile experience or battery life.. The proposed solution should have automated IT policy enforcement and built-in integrations with all major existing enterprise EMM/ MDM, SIEM, email servers and VPNs.. The proposed solution should have capabilities to integrate with many security solution including but not limited to WSS, CASB, DLP and Endpoint protection. The proposed solution should easy to deploy, adopt, maintain and update.. The proposed solution should zero impact on productivity, experience, privacy and deep analysis of suspicious apps.. The proposed solution should have real-time response and protection against various known, unknown and targeted malware attacks from any suspicious apps and networks.. The proposed solution should have automated corporate asset protection			



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
when under attack.. The proposed solution should have a reputation check capability with machine learning for apps, networks and OS.. The proposed solution should have comprehensive activity logs for integration with any SIEM solution.. The proposed solution should have app analysis capability based on signature, static/dynamic analysis, behavior, structure, permissions, source and more.. The proposed solution should have detection, blocking and remediation of malicious IOS profiles.. The proposed solution should have capability to identify Man-in-the-Middle, SSL downgrading and content manipulation attacks without violating privacy.. The proposed solution should have capability to monitoring devices for unpatched known vulnerabilities and uncovering zero-day vulnerabilities in apps and operating systems.. The proposed solution should provides mobile threat defense for modern operating systems without relying on a 3rd party. The proposed solution should addressing stealthy attacks or APTs with effective Active Directory defense from the endpoint to provide autonomous breach containment, incident response, and domain security assessment.. The proposed solution should autonomously capability to learn the organization's Active Directory structure in its entirety (servers, endpoints, applications, users, branches, naming conventions, configurations, attributes etc.). The proposed solution should able to create an authentic and unlimited obfuscation.. The proposed solution should able runtime evaluation of processes, context and Active Directory activity is evaluated.. The proposed solution should have a high-fidelity alert and the capability to is automatic to blocking the attack.. The proposed solution should provide a real-time forensics reporting that captures actual reconnaissance, credential theft, and lateral movement phases that were performed by the attacker and documenting the attacks chain.. The proposed solution should able to automatic mitigation stops the malicious process on the endpoint to contain the breach in real-time, removing its ability to spawn another process, overwrite another part of memory, run reconnaissance commands, or communicate out to the network.. The proposed solution should have the capability to continuously probes for domain misconfigurations, vulnerabilities, and persistence, and present the domain from the attacker's perspective, and allowing for immediate risk mitigation.. The proposed solution should prevent lateral movement with AD protection and ML based deception technology. The proposed solution should have an automated assessment process uses attack simulations to gather in-depth information about the configuration of the domain, privileged accounts, security settings, GPO, endpoints, domain controller, and Kerberos.. The proposed solution should have autonomously analyzes every component of the domain and Active Directory structure for misconfigurations and backdoors in AD and the entire domain environment.. Solution should be deployed, administered and updated in a single agent package and update mechanism. There should not be any need for multiple deployment of agent & to get the updates to achieve the all product functionality required above. . The proposed solution should have cabapilty to deployment in Cloud, On-Prem, and Hybrid options. Find unmanaged endpoints and deploy single lightweight agent for complete protection.. Security and compliance check both should be managed by a single			



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	و د ة ال ق ي ا س	ال ب ن د	ال ف ئ ة
administration management server and console.. Solution should provide integration with RSA for management console authentication addition to the user credential authentication if required and also should get integrated with LDAP, Syslog, and Active Directory.. The Management servers installed at different locations should have the ability to replicate data, logs and content at defined interval in Multi-Server Architecture with Policy and Log Replication.. The agent should be able to password protect uninstall, password for disabling service and password to open the client GUI so that users will not be able to uninstall the agent.. Agent should have the ability to protect the service from being stopped, even if an administrator logs on.. Update mechanism should include client content updates from management server, internal update servers, external vendor update servers, also from the client that acts as a proxy between a management server and clients in the group and using Third-party tools like Microsoft SMS.. Proposed AV solution should have a single and the same agent for physical and Virtual clients . . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) . . توفير ورش عمل لنقل ومشاركة المعرفة لتشغيل وتركيب النظام..			



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحد القياس	البند	ال فئة
"يجب توريد وتركيب أجهزة حماية تطبيقات الويب WAF الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: 9. Solution must provide analytics capability for device groups in synchronization with improvement in management and visibility with stats notification.. 10. Solution must be able to define and control how traffic is distributed across links, based on real-time traffic flows and throughput.. 11. Solution must be able to automatically build different policies for different applications and rapid deployment based on detected traffic with combined detection and prevention techniques.. 12. Solution must be able to update all signatures and protection mechanisms and licensing in totally isolated environment. 13. Solution must provide automatic self-learning and creation of security policies with versioning capability of the configured policies and rollback.. 14. Solution must provide SSL offloading capability with storing private keys in secure mechanism with capability for tuning SSL parameters.. 15. Solution must provide session tracking mechanisms that enhanced enforcement and reporting capabilities that take into account user sessions and application user names within the application.. 16. Solution must provide request and response logging that support profile by enabling configuration log entries to be reported when requests/responses are received.. 17. Solution must provide protection of AJAX-enabled applications including those that use JSON for data transfer between the client and the server. 18. Solution must provide virus checking on HTTP file uploads and SOAP attachments. Support to Anti-Virus via ICAP communication channel.. 19. Solution must provide XML Web Services access restriction methods defined via Web Services Description Language (WSDL) or XML Schema format (XSD). 20. Solution must provide XML Parser Protection, limit recursions to thwart DoS conditions, limit the numbers of elements, lengths of elements, attack signatures enforcement.. 21. Solution must be able to perform information display masking/scrubbing on requests and responses.. 22. Solution must be able to perform restrictions and filtering based on values and lengths of URL, filetype, parameters, methods, encoding in headers and response, cookies, and body content for all type of HTTP protocols.. 23. Solution must be able to monitor latency of Layer 7 (application layer) traffic to detect the spikes and anomalies in the typical traffic pattern.. 24. Solution must be able to integrate with vulnerability management tools and provide virtual patching capability.. 25. Solution must be able to provide protection based on all OWASP defined vulnerabilities . توفير الدعم الفني والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة	عدد	نظام جدار حماية الشبكة طبقا لتطبيق application firewall	ز ظ ام



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

ال فئة	ال بن د	و د ة ال ق ي ا س	المواصفات
ز ظ ام	نظ ام فد ص الم لفا ت file pro tec tio n san db ox	عد د	"يجب توريد وتركيب نظام كشف الملفات المتقدم عبر الشبكة Host Sandboxing الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: يجب ان يكون للجهاز القدرة على الوصول الى الملفات و فحصها من خلال البرتوكولات التالية: . - Secure WebDAV . - WebDAV . - NFS . - CIFS . يجب ان يكون الجهاز بالمواصفات التالية: . - Network . - Hard Disk 4 x 2 TB HDD, 3.5" RAID 10. - 2RU rack mount. . Interface Ports:2 x Gigabit Ethernet ports. - Up to 50,000 files per day . توفير الاشتراك في Support Platinum Plus) . توفير الدعم الفني والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

ال فئة	ال بن د	و د ة ال ق ي ا س	المواصفات
ز ظ ام	نظ ام ك ش ف الم لفا ت الم تقد م عبر ال شبه كة	عد د	"يجب توريد وتركيب نظام كشف الملفات المتقدم عبر الشبكة Network Sandboxing الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: . يجب ان يكون للجهاز القدرة على العمل . Network . توريد وتركيب عدد 4 نظام حماية الشبكات. Signature-less Detection Capability using Virtual Machine Based Dynamic Analysis. . The. proposed solution should have IPS capabilities. . The proposed solution should have Riskware. detection capabilities. . The solution must detect Zero-Day and APT attacks.. . The solution. should support IPMI. . It should support two management ports. . The proposed solutions should. be certified by the US Department of Homeland Security SAFETY Act Certification. . The. solution must utilize custom Virtual Machine (on-premise) technology to positively identify. malware, including zero-hour vulnerability exploits, polymorphic payloads, and obfuscated javascript.. The virtualization solution must not be detectable by malware in order to avoid evasion.. They Hypervisor must not be an OEM solution such as from VMWare or others. . The solution. has to be capable of automatically downloading threat intel from an intelligence cloud. . all static. analysis will occur in the appliance including: IPS, custom signature, Riskware, CnC rule. matching and others. . The solution should support inline monitoring and blocking (not only TCP. Reset). . The solution OS software must but capable of being automatically updated from the. Web management GUI. . The solution must be able to run multiple Micro Tasks in a single VM. (e.g. run sample across multiple versions of Adobe Acrobat in a Single VM Execution). . The. solution must be administered through a web-based console that doesn't require the installation of. additional software.. . The solution must allow the creation of accounts with different roles used. to administer the solution, or just monitor the alerts.. . The solution must allow the authentication. to the console by using authentication services like RADIUS, TACACS+, LDAP and LDAPS.. . The solution should support remote administration using CLI and GUI (Web Console). . The. solution must be able to detect and report web exploits by using multiple versions of web. browsers and plug-ins.. . The analysis must be performed runtime in order to detect all the. malware actions, even the ones that fail in the virtual environment but might be successful on a. client workstation. Before and after differential Comparison or VM state is not acceptable.. . For. the list of applications supported in the VM's the Vendor must have a method for pushing updates. to the list of applications dynamical to the appliance without requiring a full OS or solution. upgrade.. . The solution must allow the configuration of an ACL to control access to the. management interface. . The solution must be able to utilize NetBIOS and DNS for hostname. resolution when generating alerts.. . IPS Detection of Reconnaissance Activity. . IPS Detection of. Brute Force Attacks. . IPS Uses Dynamic Analysis Engine (VM) for IPS alert validation and. correlation. . The solution should support remote administration using ssh and https. . The. solution must be able to detect and report malware downloaded by users, or downloaded in the. context of a web exploit by using multiple client operating systems with multiple service pack. levels running on both x64 and x86 architectures.. . completely unknown



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج: خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البنية	الفرع
vulnerabilities across. protocols and applications.. · The solution must be able to detect all three stages of the modern. malware's attack lifecycle, while highlighting every stage of the attack: Exploit, Dropper & Data. Exfiltration. · Solution should use customized hypervisor and should include instrumentation. running within itself for run-time detection analysis. · Solution should be able to handle reflective. DLL injection. · Solution should be able to detect Kernel level rootkits. · Solution should be able. to handle packed payloads. · Solution should be able to deal with VM evasion techniques. · . Solution should have the ability to remain fully effective when configured to share no data,. events, nor any information with vendor or the vendors network.. · Solution should have the. ability to detect client-side EXPLOITS prior to any complex malware being downloaded to the. systems; complex malware is defined as malware with complex abilities such as key-logging,. data-stealing, encrypting, migrating, and installing additional complex malware.. · The solution. must be capable of blocking reliably outgoing communications to CnC servers in order to. conserve data integrity on hosts including out of band infections. · The solution must be able to. automatically generate a network communication profile if the malware tries to contact network. resources during the analysis. This profile must be used to determine if systems on the network. are compromised.. · Should provide information such as:. i. Host Modification Report. ii. Copy of. malware binary. iii. PCAP of Malware to Command & Control servers. iv. Meta Format of. Malware to Command & Control servers. v. Full URL trail identifying all of the locations from تاريخ التشغيل. . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة) يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة			
تقييم مستوى نضج الامن السيبراني اعتمادا على مرجعية هيكلية الامن السيبراني للذكاء الاصطناعي متوافق مع متطلبات العمل الاتية: . a.Conduct gap and maturity level assessment (CMMI Maturity Levels) and define the As-Is and To-Be states on the AI Cybersecurity Architecture covering each building block.. b.Provide recommendations on how to fill the gap between current and target state and ensure flexibility and robustness for all new technologies.	عدد	تقييم مستوى نضج الامن السيبراني	الفرع



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

ال فئة	ال بن د	و د ة ال ق ي ا س	المواصفات
ز ظ ام	نظ ام الت حق ق من نزا هة الم لفا ت والا لتزا م	عد د	يجب توريد وتركيب الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. . توريد نظام (FILE INTEGRITY MONITOR&Security Compliance Check&Security Compliance Check) . تركيب نظام (FILE INTEGRITY MONITOR&Security Compliance Check&Security Compliance Check) . توفير خدمات احترافية لنظام (FILE INTEGRITY MONITOR&Security Compliance Check&Security Compliance Check) . توريد وتركيب الرخص اللازمة للخوادم (500 خادم). توريد وتركيب الرخص اللازمة لأجهزة الشبكة (50). توريد وتركيب الرخص اللازمة للتكامل مع الانظمة الامنية (2). توريد وتركيب الرخص اللازمة للامتثال والالتزام (2). توريد و تركيب الرخص اللازمة (2) ESXi . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورش عمل لنقل ومشاركة المعرفة لتشغيل وتركيب النظام.(8 موظفين).
خ د م ة	خد ما ت احت راف ية اسد تش ار ة	ش هر	توفير خدمات لمراجعة الاعدادات للتقنيات الرقمية لمدة 200 يوم عمل . توفير خدمات تقييم فجوات امنية لتقييم البنية التقنية والانظمة مع تقييم المخاطر السيبرانية . توفير خدمات امنية لتقييم اختبار الاختراق لعدد 50 نظام او تطبيق و 300 عنوان شبكي و . تطوير خطة معالجة تقنية و تشغيلية



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :
إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز
الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحد ة الق ياس س	الب ن د	ال فئ ة
تطوير اطار لمرجعة هيكلية الامن السيبراني متوافق مع متطلبات العمل حسب المتطلبات الفنية الآتية: . AI Reference Cybersecurity Architecture based on the AI UCF (defined in the previous activity), Threat Catalog, and business needs. The vendor shall: a. Develop Threat Catalog including threats, actors (adversaries), motives, methods, risks and scenarios for each Use Case defined in Activity. b. Develop AI Reference Cybersecurity Architecture (AI RSA) following SABSA framework up to level three (logical level). The AI RSA shall comprise cybersecurity capabilities (Security Ser+F10vices in SABSA terminology), security drivers, potential threats, the existing related security solutions for each capability, and integration patterns for each domain.. develop cybersecurity rules and standards for each capability (up to 10 security rules for each capability).. d. Map the capabilities to the controls in the AI UCF defined and unified Reference security architecture . . E. The vendor must doing the required assessment with developing the required toolkit with take approval from the .Cybersecurity and relevant dept	عدد	تطوير وثق ص م م م ج ية لم عم ار ة الام ن ال سي براز ي	خدمة
توفير خدمات احترافية استشارية لتطوير وتحسين الخدمات الاتية : Identity access Managment . Gap Assessment Report . Roadmap and Implementation Plan including all Recommendations . User Data Requirements Analysis Report for IAG . Document detailing Roles and Responsibilities and RACI for IAG . Processes, procedures, and guidelines . Workflows and .Forms . IAM Use Cases 30 . PAM use cases 30	شهر	خدمة احترافية راف ية وا ست ش رية	خدمة



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

ال فئ ة	ال بن د	و د ة ال ق ي ا س	المواصفات
اج ه زة	أنظ مة أم ن و د ما ي ة ال شب كة الم تقد مة	عد د	يجب توريد وتركيب الحلول مع كامل مستلزماتها. . توفير الحلول اللازمة مع الرخص التشغيلية لمدة 3 سنوات. :يجب الالتزام بالمواصفات المطلوبة حسب الآتي.: ICAP 4 Solution must be at least 4 servers distributed in two datacenters. - Solution must be at - least with 20 Engines scanning capability through 6 different dedicated servers distributed in two datacenters. - Solution must support - Solution must support Core technology enablement (CDR, DLP, multi-scanning, etc.). - 24x7x365Maintenance & Support for 3 years. - solution component to be implemented in two different datacenter sites.. The solution should support both Windows Client and Server versions. The solution should support Chrome, Firefox, Safari, Internet Explorer and Microsoft Edge for the management console. Web access to the platform should be via https protocol. The solution should support RBAC . The solution should be able to integrate with SIEM or syslog servers. The solution should provide auditable record of files and emails that has been scanned. The solution should be able to run in air gapped environments. The solution should be able to work in a network connected mode. The solution should expose APIs for integration purposes. The exposed APIs have to be officilaly documented. The solution should connect to only one URL to download the new signature definitions. The solution should support signature definition upload previously downloaded from an internet connected machine. The engine and virus definition update mechanism should support internet, manual and folder mode. The solution must provide a single pane of glass for central configuration. The solution should integrate with syslog/SIEM systems. The solution must allow the creation of accounts with different roles used to administer the solution, or for auditing purposes. The solution should provide Active Directory and LDAP group-based administrative roles. Solution should have its logs archived locally, and they should be downloadable via the GUI. The solution should support remote administration using RDP and https. The solution should provide built in database. The built in database management should be done from the product user interface. The solution should allow configuration export and backup. The solution should be able to provide 30+ different AV engines . The solution should use signature based detection. The solution should use heuristic based detection. The solution should use machine learning based detection. The multiple AV engines should be able to run in a multithreaded way. The solution should be able to support complex archive processing and extration. The solution should support over 30 different archive types. The solution should allow configuration of the archive handling process. The solution should be able to process password protected archived/files. The detection should run fully on premise with no cloud connection. There should only be 1 licensing component for all the multiple AV engines. The different AV engines have to run in an airgapped environment. The frequency of the signature definition updates has to be configurable. The signature definitions have to all come from one single point. The solution should be able to detect known vulnerabilities in binary data. The solution should be able to integrate inline with 3rd party security controls. The solution should be able to quarantine malicious sample for further analysis. The solution must allow



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحد القياس	البند د	ال فئة
disabling AV engines to exclude them from scanning. The solution should provide a false positive configurable threshold . The solution should be able to provide a known vulnerability assessment technology. The solution should detect Vulnerable Installers. The solution should detect IoT Software and Firmware Vulnerabilities. The solution should provide a file type detection technology. The solution should provide a YARA module. The solution has to be able to integrate via REST API. The REST API has to be JSON based. The solution should detect spoofing of over 4,500 file types and block spoofed files. The solution should support extraction for the follwing archive types: Zip, 7z, Jar, rar, rar5, tar, ISO, Gzip, CAB, ARJ, LZH, RPM, DEB, LZMA, WIM, SFX, XZ, VDI, VHD, MBR, CPIO, HFS, .apk .gz .msi .tgz .tbz, bz2. The archive extraction mechanism should be configurable. The solution should process Microsoft Office Documents as archives. The following self extracting archives should be supported: 7zip, WinRAR, PKZIP, IExpress. The solution should be able to blacklist/whitelist by hash, filename, filetype or mime type. The solution should be able to quarantine blocked files. The quarantine should have the option to integrate with MetaDefender Cloud for Threat Intelligence. The solution should allow different workflow rule configuration to customize the order and process in which files are handled. The solution should provide the option to integrate inline with a 3rd party security control (external scanner). The solution has to be able to integrate with SMB compatible storage (Plus Platinum) .has to be able to integrate with SMB compatible storage (Plus Platinum) Support (الصيانة والدعم غير مندرجة تحت الضمان حسب متطلبات وزارة التجارة.			



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدتها	البند	الرقم
يجب توفير وتركيب الحل التقني لأتمتة التقنيات الامنية بالشبكة وغيرها NETWORK POLIY ORCHESTRATION AND ASSURANCE مع كامل مستلزماتها. توفير الحلول اللازمة لمدة 3 سنوات. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة (8 موظفين). يجب الالتزام بالمواصفات المطلوبة حسب الآتي: Network Policy Orchestration & Assurance Integration with Firewall for 20 and 50 network devices. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: The proposed system should be deployed in two data centers. Also, it should be deployed by the Professional Service team from the mother company.. Bidder should provide HLD , LLD , Operation Guides for End-user and Admins , Minimum Baseline Security Standards , and test uses cases in SDAIA template documents.. The proposed system should be virtual based.. The proposed solution should be able to integrate with SIEM tool and forward all the logs and events to the SIEM solution.. The proposed solution should support multi tiers architecture. . The proposed solution should support Single Sing On.. The proposed solution should support integration with Active Directory (AD), Network Time Protocol (NTP) and Domain Name System (DNS).. Bidder should provide all the required commu ation matrix for the proposed solution.. Bidder should provide the data flow of the proposed solution.. The data should be encrypted in transit.. The data should be encrypted at rest.. The proposed solution should support RBAC model for separation of duties and data.. The proposed solution should be able to integrate with Multi Factor authentication solution (MFA).. The proposed solution should be highly available. The solution should support automatic replication between the solutions in two data centers.. The proposed solution should support integration and not limited to Palo Alto, Cisco, Fortinet, Juniper firewalls (VM, VSYS and Appliances) ,Load Balancers , and WAF . All functionality of the proposed solution's platform should be tightly integrated and operated from a single pane of glass. . The proposed solution should support user customizable query language, which allows the user to perform a variety of tasks . The proposed solution should store unlimited versions of firewall configurations with all changes detected and stored in encrypted database. . The proposed Solution should support continues real-time monitoring and detection of all changes.. The proposed solution should provide a Device Dashboard where information on Rule Usage is displayed and the top used rules should be listed based on percentages in descending order. . Used and Unused Rules:. In addition to the detailed rule usage and object analysis information, the proposed solution should provide information to help optimize the operation of a policy. . The proposed solution should also highlight which rules have seen no activity at all, to help chart a remediation path for the removal of unused rules and reduce policy complexity while increasing security posture. . Redundant / Shadowed Rules:. The proposed solution should provide a standard report for identifying redundant and shadowed rules with details that indicate the portion of the rules that causes the redundancy. Users can configure the varying level of redundancy and overlap.. Rule Consolidation:. The proposed solution should provide a standard report that displays security rules on the firewall that may be safely consolidated without changing the behavior	عدد	نظام لادارة التقنيات	ز



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
of the policy.. The proposed solution should Support Real-Time change analysis and reporting for the monitored Firewalls.. The proposed solution should provide security compliance reports utilizing built-in and customized security controls. . The proposed solution should include extensive policy rule search capabilities and global search functions across multiple policies. Additionally, reporting and compliance checks provide the ability to customize a report to see if a specific object is allowed. This can include IPs, networks, groups, zones, or services. The proposed solution should support real-time compliance custom and assessment dashboard.. The proposed solution operating system should be hardened. . The proposed solution should have ability to Identify any unused rules, unused network objects and unused service objects in existing policies to prevent gaps and reduce unnecessary complexity.. The proposed solution should provide reports for rule consolidation.. The proposed solution should provide Object usage like ports and IPs within the Rule for Clean-up.. The proposed solution should support Creation of custom controls and assessments to identify automatically rules for clean-up and recertification.. The proposed solution should provide comprehensive network mapping for managed devices. . The proposed solution should store the data on encrypted disk.. The proposed solution should provide Rule usage in time query capabilities and visualization on histogram.. The proposed solution should have the ability to normalize firewall rulesets for single consistent view across multiple vendors.. The proposed solution should have the ability to generate custom reports and queries.. The proposed solution should provide built-in security policies and baselines based on security best practices. . The proposed solution should support multi-vendor next generation firewalls. . The proposed solution should be able to read and analyze existing policies for managed devices upon deployment. . The proposed solution should support Custom assessments can be run for specific device group or all devices if required.. The proposed solution should provide out of the box compliance reports like ISO 27001, NCA ,CSA etc compliance report generated for individual Firewall and Groups of Firewalls. The proposed solution should provide full audit logs for any system changes. . The proposed solution should support Policy and Rule Documentation for all integrated Firewalls & network devices.. The proposed solution should support Role base access with Granular privileges definition limiting user group access to specific system functions/interface (i.e. dashboard, configuration, change management) as well as functions within particular systems limited to selected device groups or all devices.. The proposed solution should be able to automate and generate reports via email. . The proposed solution should provide user-friendly web interface based on HTML 5. . The proposed solution should support multi-user roles/privileges. . The proposed solution should support authentication of users using RADIUS, AD, LDAP. . The proposed solution should provide web user interface that is compatible with modern web browsers (Internet Explorer, Firefox, and Chrome). . The proposed solution should support single and distributed environment for deployment. . The proposed solution should support Fully customizable Web-based dashboard with customizable metrics, defined using security information query language, including NAT			



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
rules. The proposed solution reports and notifications are to be available in a minimum of the following formats HTML, PDF.. The proposed solution should support all functionality through REST-API.. The proposed solution should provide recommendations to fix overly permissive rules. . The proposed solution should allow admins to develop customized controls for security analysis. . The proposed solution should have the ability to graphical mapping and simulating traffic path flow. . The proposed solution should support full-fledged Workflow based Firewall Rule Change Management.. The proposed solution should provide Firewall policies management, Audit and Compliance management as well as automated change management and recertification process and workflow.. The proposed solution should have the ability to push the configuration directly on the firewalls without needs to firewall management station.. The proposed solution should have the ability to connect read/write with and without centralized firewall managers including Panorama, Cisco FTD, Fortinet Manager. The proposed solution should have the ability to manually and automatically remove deactivated rules. . The proposed solution should provide Firewall policies management, Audit and Compliance management as well as automated change management and recertification process and workflow. . The proposed solution reports and notifications are to be available in a minimum of the following formats HTML, PDF . توفير الدعم الفني والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) ..			
يجب توفير الحل مع كامل مستلزماتها. . توفير الحل اللازمة مع الرخص التشغيلية لمدة 3 سنوات. يجب الالتزام بالمواصفات المطلوبة حسب الآتي: NGFW should cover interconnectivity for the chosen zones.. NGFW should have capability to interconnect through 40Gbps and QSFP interfaces with at least 4 interfaces on each firewall .. NGFW should able at least to handle 50 Gbps throughput as stateful without applying SSL/IPS inspection and 25 Gbps with IPS inspection.. NGFW should able to integrate with environment and be integrated with proposed network security orchestration solution.. NGFW should including the all hardward parts and passive components such as cables,SFP,Stand, etc.. the lincseses should be provided for 3 years including the all security function IPS, SSL, Threat feeds, and advanced support. 7. Redundant FANs and Power supply . توفير الدعم الفني والرخص اللازمة لمدة 3 سنوات من تاريخ التشغيل. . الدعم الفني لايندرج تحت ضمان الوكيل المنصوص عليه في نظام وزارة التجارة (يبدأ مع انتهاء مرحلة تركيب النظام) .. توفير ورشة عمل وتدريب للحلول والبرامج المقترحة (8 موظفين)	عدد	أجهزة حوسبة شبكية جدارية	إجهزة حوسبة جدارية
		Next Generation Firewall	



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

ال فئة	البند	و دة ال ق يا س	المواصفات
رذ ص ة	نظ ام الك ش ف والا ست جاء ة للأ جه زة الط رفي ة	عد د	Three-years EDR software subscription expansion for 500 endpoints with . - solution component to be implemented in two different datacenter sites.. - 24x7x365Maintenance & Support for 3 years. On premise EDR solution with capability to work as mutitenancy to improve security operations productivity and enhance detection and response capabilities by including more security components into a unified whole that offers multiple streams of telemetry, presenting options for multiple forms of detection and concurrently enabling multiple methods of response. . Centralization of normalized data, Correlation of security data and alerts into incidents. A centralized incident response capability . · Allows deep visibility into all endpoint activity - in real time and retrospectively.. · Simplifies threat hunting and detection.. · Prevents threats through your preferred AV engine and process blocking.. · Automates response with pre-built scripts and playbooks.. · See all endpoint activity across Windows, Mac, and Linux systems and gain unmatched insight through the collection of all executable files and scripts that are analyzed against the latest threat intelligence. . · Detect threats in real time or hunt retrospectively through recorded events. . · Monitor a full software inventory and identify vulnerabilities with links to MITRE CVEs or Microsoft KB Reports.. · View all process data, user activity, registry events, file system activity, and memory data and more.. · Review full software inventory and known CVE and KB vulnerabilities. · Collect executable files and scripts for analysis and threat hunting.. · Create and save advanced queries using Boolean logic.. · Monitor endpoints in real-time and retrospectively, on and off the network. · Monitor key events with playback analysis to automatically deliver an incident timeline, along with prioritized alerts.. · The solution must be able to automate response with scripts and playbooks, including the ability to isolate endpoints, terminate processes, remove files, and deploy custom scripts. . · The ability to start investigations with memory analysis, vulnerability scans, and system inventory. The ability to capture data and memory and full disk images, as well as the ability to remotely access endpoints to view and take action on files and processes.. · The ability to take action and automate response with a customizable library of scripts and playbooks. · Collect forensically sound data in real time for deeper investigations.. · Remotely access and control endpoint file systems and processes. · Integrate with SIEMs, NGFWs, etc., to execute response actions.. · Maintain full control of endpoints with full remote shell capabilities.. · Endpoint threats must be mapped to MITRE ATT&CK™ to allow SDAIA analysts to see the TTPs in use and to determine the proper response. Untrusted executables are automatically sent to SDAIA sandbox and can be integrated into process blocking (IOC, hash, and YARA rules).. · The solution must support Windows, Linux and MacOS for agents installations. · The solution must automatically collect executables and script file at the first time executed in the environment. · The solution must automatically and dynamically collect installed software on all endpoints and alert against any identified CVE. · The solution must record process activities (process start, image load, process access, service and process exit) in real time. · The solution must record when a process creates a remote thread in another



رقم النسخة : الأولى
تاريخ الإصدار :
رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
process, or when a thread is created in the current process by another process. · The solution must be able to ingest open source IoCs and YARA rules and use it to run scans on target endpoint(s). · The solution must allow users the ability to query across collected endpoint behaviors and must support saving search queries. · The solution must have Advanced Query Builder to allows for users to craft queries that include Boolean logic, targeting of endpoint groups for inclusion/exclusion, and assists users in creating these advanced queries that are useful for investigation, behavior rule creation, and threat hunting. · The solution must record connected endpoint(s) information including but not limited to: host name, IP Address, processor, memory, OS, OS version and last connected time. · The solution must be able to dynamically update recorded connected endpoint(s) information. · The solution must support endpoint grouping (static groups, dynamic groups and imported groups). · The solution must be able to show endpoint related task results, alerts, USB activities, login history and installed software as part of the endpoint record.. · The solution must support Multitenant architecture. The solution be compliant with CSDC Support) .EDR technologies . Share knowleged must be provided (Platinum Plus الصيانة والدعم غير مندرجة تحت الضمان حسب متطلبات وزارة التجارة			



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

ال فئة	ال بن د	و د ة ال ق ي ا س	المواصفات
خ د م ة	الام ن الم دار لمر كز عم ليا ت الام ن ال سي براز ي	ش هر	خدمات SOC الأمنية • يجب على مقدمي خدمات الأمن المُدارة توفير خدمات الكشف والاستجابة المُدارة (مراقبة التهديدات في الوقت الحقيقي) لمدار 24 ساعة يوميًا، طوال السنة، باشتراك سنوي يشمل تراخيص تصل إلى 70 جيجابايت • يجب تحديد وموافقة الوصول إلى خدمات الأمن المُدارة من قبل قسم الأمن السيبراني • يجب استضافة جميع الأصول الأمنية في المنظمة مع وضع خطة محددة لتسليمها إلى الفريق ذي الصلة بناءً على توجيهات مالك المشروع، مع تضمين جميع الوثائق وليس اقتصارًا على: LLD، HLD، حالات الاستخدام، التراخيص، مصفوفة الاتصال، قائمة الوصول للمستخدم، إلخ. • يجب أن تشمل الأصول الأمنية المذكورة، ولكن لا تقتصر عليها: أجهزة الشبكة، Active Directory، مايكروسوفت، أجهزة مكتبة بنظام مايكروسوفت، خوادم بنظام مايكروسوفت، خوادم لينكس، جدران الحماية الحدودية، جدران الحماية لمركز البيانات، EDR، جدار حماية تطبيقات الويب • يجب على مقدمي خدمات الأمن المُدارة توفير جمع السجلات، تحليل السجلات، تقارير السجلات وتحليل البيانات، ويجب أن تتمثل البيانات في مقر المنظمة وفقًا للتوافق. • يجب على مقدمي خدمات الأمن المُدارة توفير رؤية على مدار الساعة في التهديدات والثغرات والهجمات، بالإضافة إلى استجابة الحوادث مع خدمات التصحيح. • يجب على مقدمي خدمات الأمن المُدارة توفير خدمة الكشف والاستجابة وتوفير الرؤية والخبرة التي تسمح لهم بالتعرف عندما تكون هناك حاجة إلى إجراءات استجابة، وتقييم المخاطر. • يجب أن يلتزم مقدمي خدمات الأمن المُدارة بجميع اللوائح ذات الصلة بالأمن السيبراني. • يجب أن توفر خدمات الأمن المُدارة إجراءات التشغيل القياسية (SOPs) بما في ذلك النموذج التشغيلي، وعمليات SOC، وسير العمل مع الأدوار والمسؤوليات بين المزود والمنظمة، والتفاعل مع أمان المعلومات، واتفاقيات مستوى الخدمة والكتب العمل، وإجراءات التصعيد. • يجب على مقدمي خدمات الأمن المُدارة توفير خدمات استخبارات التهديد المُدارة باستخدام مصادر مفتوحة بهدف فهم أحدث التهديدات السيبرانية، في أقرب وقت ممكن بناءً على المخاطر والوضع الأمني. • يجب على مقدمي الخدمات المُدارة توفير الدعم لجميع السجلات بناءً على سياسة الاحتفاظ، وبإمكانية تصدير السجلات المحفوظة عند الحاجة. • يجب على مقدمي الخدمات المُدارة محو جميع البيانات/المعلومات التاريخية ذات الصلة بسادايا بما في ذلك جميع الأنشطة والسجلات والحوادث والتكاملات بعد تأكيد تسليم المشروع. • يجب على مقدمي الخدمات المُدارة دعم جميع متطلبات التقارير اللازمة لتلبية جميع متطلبات التنظيم الداخلية والخارجية. • يجب على مقدمي الخدمات المُدارة دعم تبادل المعلومات الاستخبارية مع SOC سادايا بناءً على المعايير المحددة من قبل فريق CTI في سادايا. • يجب على مقدمي الخدمات المُدارة أن يأخذوا في الاعتبار ال EDR المقترح للعمليات ونطاق متطلبات الكشف والاستجابة. • يجب على خدمات الأمن المُدارة أخذ الموافقة من الإدارة ذات الصلة في الأمن السيبراني لحالات الاستخدام وطلبات التغيير وإنشاء المستخدمين. • يجب الموافقة على أي تصميم أو تغيير من قبل أعضاء فريق الأمن السيبراني وأي قسم ذي صلة من جانب السادايا. • يجب تقديم نقل المعرفة كل 6 أشهر مع أعضاء فريق الأمن السيبراني (SOC) لجميع المستويات مثل: تحليل L1، L2، L3، والهندسة والإدارة. • يجب على المقاولين الامتثال لمتطلبات التكنولوجيا التالية: 1. يجب أن تكون الحلول المقترحة قادرة على توفير وظائف SIEM الجيل القادم. 2. يجب أن تكون طول SIEM مبنية على تكنولوجيا البيانات الكبيرة مع القدرة على استيعاب تخزين غير محدود. 3. يجب تثبيت تراخيص طول SIEM دون الاتصال بالإنترنت ويجب أن تبرز الخيارات والقيود الدائمة والاشترائية للتراخيص. 4. يجب أن تكون حلول SIEM قابلة للتوسيع والانتشار في بيئات متعددة مختلفة. 5. يجب أن تأخذ طول SIEM قدرات العمل المتعددة في جمع البيانات وإثرائها والبحث فيها والاحتفاظ بها بعين الاعتبار. 6. يجب أن تكون فترة الاحتفاظ على الأقل 6 أشهر من السجلات



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

المواصفات	وحدة القياس	البند	الرقم
التي يمكن البحث فيها عبر الإنترنت، و 12 شهرًا من السجلات التي يمكن البحث فيها، وثلاث سنوات من السجلات المؤرشفة التي يمكن البحث فيها. 7. يجب على حلول SIEM أن تتمكن من التعامل مع زيادة مرة واحدة في السعة السائلة (EPS) بمعدل أربع مرات خلال ساعة واحدة دون أي تخزين مؤقت أو تدهور في أداء الحل. 8. يجب أن تكون حلول SIEM قادرة على تحقيق التوافر العالي بين ثلاثة مراكز بيانات مختلفة لطبقات الجمع والترابط والفهرسة والأرشفة. 9. يجب تشفير جميع الاتصالات بين جميع مكونات حلول SIEM. 10. يجب أن لا تفرض حلول SIEM أي قيود على عدد الحقول التي يمكنها فهرستها. 11. يجب أن تسمح التصميمات والبيانات المقترحة لحلول SIEM بالوصول السريع إلى تيرابايتات الأرشفة والبيانات التاريخية. يجب أن تكون قادرة على توفير البحث السريع جدًا والموزع.			

66- المعدات

أولاً: الشروط الخاصة بالمعدات

تخضع المعدات المستخدمة في تنفيذ الأعمال للمواصفات والمقاييس المعمول بها في المملكة العربية السعودية.

ويفحص المتعاقد جميع المعدات ويوصي باعتمادها في حال كانت مطابقة من جميع النواحي للمواصفات والمقاييس العالمية. كما يجب عليه فحص جميع شهادات اختبار هذه المعدات التي أجريت في المصنع ومراقبة وتصديق اختباراتها في الموقع أو مكان الصنع وفي جميع الحالات التي تنص فيها شروط توريد المعدات أو المقاييس العالمية على إجراء هذه الاختبارات كما يجب عليه أن يحتفظ بشهادات الاختبارات التي تجري بهذا الخصوص.

ثانياً: جدول مواصفات المعدات

لا يوجد

67 - كيفية تنفيذ الأعمال والخدمات

تم ذكرها في نطاق العمل

68- مواصفات الجودة

يلتزم المتعاقد بمواصفات الجودة المطلوبة في تنفيذ نطاق الأعمال والخدمات المذكورة في العقد. ويجب على المتعاقد إخطار الجهة بما يتسبب أو قد يتسبب في عدم الامتثال لمتطلبات الجودة في السلع الموردة والخدمات المقدمة وبأي تغييرات أو تعديلات قد تؤثر على هذه الجودة كتغيير موقع تصنيع المواد، أو تغيير المواد الخام ونسبها المستعملة في تصنيع السلع الموردة.

يلتزم المتعاقد بأداء جميع الخدمات اللازمة للمشروع وتنفيذها من خلال موظفيه وفقاً لأعلى مستويات الجودة وبالكيفية والأسلوب المتعارف عليهما مهنيًا. يجب على المتعاقد تقديم خطة ضمان الجودة والتي يعتزم تنفيذها في المشروع لمراجعتها واعتمادها من الجهة الحكومية. يجب أن تتضمن الخطة إجراءات وأدوات ضبط الجودة



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

69- مواصفات السلامة

يلتزم المتعاقد وخلال جميع مراحل التنفيذ بجميع الأنظمة والقواعد المطبقة في المملكة فيما يخص السلامة والصحة والبيئة وأي أنظمة وقواعد تحددها الجهة في نطاق عمل المشروع، ويضمن اتخاذ جميع الإجراءات والاحتياطات اللازمة للامتثال لهذه الأنظمة والقواعد.

يلتزم المتعاقد وخلال جميع مراحل التنفيذ بجميع الأنظمة والقواعد المطبقة في المملكة فيما يخص السلامة والصحة والبيئة وأي أنظمة وقواعد تحددها الجهة الحكومية في نطاق عمل المشروع، ويضمن اتخاذ جميع الإجراءات والاحتياطات اللازمة للامتثال لهذه الأنظمة والقواعد.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

القسم التاسع: متطلبات المحتوى المحلي

1- القائمة الإلزامية

أ. يجب على المتنافس الالتزام بالقائمة الإلزامية الواردة في وثائق المنافسة وذلك عند تنفيذ الأعمال أو المشتريات.

ب. ستقوم الجهة الحكومية بمراقبة أداء المتعاقد في تنفيذ التزامه بشأن القائمة الإلزامية أثناء تنفيذ العقد، ولن تقوم باستثناء أي منتجات مدرجة في القائمة في حال كان بلد المنشأ غير وطني، ولا يدخل في ذلك المنتجات التي حصل المتعاقد على استثناء لها وفقاً للضوابط التي وضعتها هيئة المحتوى المحلي والمشتريات الحكومية.

ج. على المتعاقد الالتزام بالتعليمات الخاصة بتسليم المنتجات الوطنية المدرجة في القائمة الإلزامية، التي تصدرها هيئة المحتوى المحلي والمشتريات الحكومية.

د. على المتعاقد الالتزام بالضوابط الخاصة بالاستثناء من القائمة الإلزامية التي تصدرها هيئة المحتوى المحلي والمشتريات الحكومية.

2- اشتراطات المحتوى المحلي

اشتراطات آلية وزن المحتوى المحلي في التقييم المالي

أ. يجوز للمتنافس تقديم خط الأساس للمحتوى المحلي في هذه المنافسة والذي سيكون جزء من معايير التقييم المالي للعروض وفقاً للشروط والأحكام الملحقه بهذه الكراسة

ب. يلتزم المتنافس بتقديم نسبة المحتوى المحلي المستهدفة وفق الشروط والأحكام الملحقه بهذه الكراسة.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

القسم العاشر: الشروط الخاصة

مرفق

في حال انطباق اشتراط شهادة المحتوى المحلي (خط الأساس) على المنتجات المدرجة في القائمة الإلزامية؛ فيلتزم المتعاقد - أو متعاقديه من الباطن - بتوريد منتجات القائمة الإلزامية من مزودي الخدمات والمصانع المستوفية لهذا الاشتراط.



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB

القسم الحادي عشر: الملحقات

- ملحق رقم(1) الشروط والاحكام لالية وزن المحتوى المحلي في التقييم المالي على مستوى المنشأة .
- ملحق رقم (2) معايير تقييم العروض
- ملحق رقم (3) نموذج التأهيل المستوى الاول
- ملحق رقم (4) المتطلبات العامة
- ملحق رقم (5) قائمة التدقيق
- ملحق رقم (6) نموذج العقد
- ملحق رقم (7) نموذج تقييم أداء المتعاقد
- ملحق رقم (8) خطاب تقديم العطاء
- ملحق رقم (9) مكان تسليم العروض في حال تعذر تسليم العروض من خلال منصة اعتماد
- ملحق رقم (10) الشروط الخاصة
- ملحق رقم (11) القائمة الإلزامية للجهات الحكومية (يونيو 2024)



رقم النسخة : الأولى

تاريخ الإصدار :

رقم الكراسة :

المملكة العربية السعودية

إسم الإدارة :

إسم النموذج : خدمات الأمن السيبراني لدعم الاستراتيجيات التقنية لمركز

الذكاء الاصطناعي NCAI-HPCCYB