☐ Working Draft ☒ Approved ☐ Adopted

Document Owner: Taqnyat

Last Review Date: Dec

Logging and Alerting

There are many ways to setup logging to capture the required data for use in incident detection and response. The key components of a strong logging and alerting design include all devices synchronizing time to a common source and the log server being segmented from the devices logging to it. When looking at the volume of data that is generated on a network, a time difference of only a few seconds can have a major impact in the ability to correlate events on different systems. Additionally, lack of time synchronization can cause legal issues making log files inadmissible as evidence.

Store log files separate from the trusted network, in the event of a compromise, the attacker will likely first try to cover their tracks within the logs. By segmenting the log data, we protect this information for later forensic analysis.

Logging and Alerting Recommendations

Performance and event data should be logged on all critical systems. Log files should undergo manual or automated analysis on a regular basis and if possible, generate alarms for predefined thresholds and events. At a minimum, organizations should enable auditing and logging on Domain Controllers, Firewalls and Switches. Log files should be sent to and stored on an isolated and secured network segment.

An isolated network segment can be achieved by setting up a non-domain member virtual machine on a firewall segment. Infrastructure cost would be minimal; however, some log aggregation and analysis software would be recommended.

Below are examples of the type of data that should be gathered:

The following events should be consistently and/or uniformly logged:

- Changes to programs and system settings
- Changes to critical hardware elements
- All server system startups and shutdowns
- Abnormal system events (e.g. performance deterioration, files filling up, programs ending abnormally)
- Changes to security parameter settings
- Changes to network configuration settings
- All successful and unsuccessful login attempts
- All logoffs
- All access to restricted information
- All additions, deletions and modifications to user accounts, user privileges, access rules and permissions
- Attempts to perform unauthorized functions
- All password changes
- All activities performed by privileged accounts
- All access to sensitive transactions

شركة تقنيات الجوال
Taqnyat
JEDDAH 4030394715 - RIYADH 1010296

The following information (regarding system events) should be consistently/uniformly logged:

- Host name
- User account
- Date and time stamp
- Description of the activity performed
- Event ID or event type
- Reason for logging event
- Source and destination network addresses
- Referring page (in case of HTTP access)
- Type of browser used (in case of HTTP access)

Waivers

Waivers from certain policy provisions may be sought following the FRSecure Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

شركة تقنيات الجوال
Taqnyat
JEDDAH 4030394715 - RIYADH 1010296254

Version History

Version	Modified Date	Approved Date	Author	Reason/Comments
1.0.0	January-2023	Jan-2023	Taqnyat CIOS	Document Origination

شركة تقنيات الجوال
Taqnyat
JEDDAH 4030394715 - RIYADH 1010296254