

4.6.1 Logging and Monitoring

Contents

1. Definitions	2
2. Purpose	2
3. Scope	2
4. Policy	2
5. Non-compliance	4
6. References	4

Version	Adjustment Date	Approved By	Approval Date
2.0	4/7/2024	Saud Alsulami	7/7/2024

1. Definitions

For purposes of this “Logging and Monitoring” the following definitions apply:

- **Event Logs:** structured records generated by information systems and network devices that capture significant events, activities, and changes occurring within an organization's IT infrastructure. These logs typically include details such as timestamps, event descriptions, source IP addresses, user accounts, and other relevant information.
- **Real-time Monitoring:** the continuous and immediate observation of event logs and system activities to identify and respond to security incidents or anomalies as they occur.
- **Event Analysis:** the process of examining event logs to assess their significance, understand the context, and determine potential security implications. This analysis aids in identifying security threats, vulnerabilities, and areas requiring further investigation or action.
- **Incident Response:** the set of predefined procedures and actions taken to address and mitigate security incidents and breaches discovered through event log analysis.
- **Retention Period:** specifies the duration for which event logs must be stored and maintained. It may be defined by legal and regulatory requirements, industry standards, or the organization's internal data retention policy.
- **Encryption:** the process of converting event log data into a secure and unreadable format to protect it from unauthorized access during transmission or storage. This ensures the confidentiality and integrity of sensitive log information.

2. Purpose

This Logging and Monitoring Policy outlines the requirements and procedures for logging, monitoring, and analyzing events related to the information assets belonging to the organization. The policy ensures that event logs are generated, retained, and protected to enhance the security of Taqnyat systems.

3. Scope

This policy applies to all IT infrastructure, including the servers, network devices, and applications, within the Taqnyat network.

4. Policy

- 4.1. All events relevant to the security and operation of Taqnyat services must be logged and sent to SIEM.



- 4.2. These events must be included, but are not limited to, login attempts, configuration changes, firewall logs, and other critical security-related activities.
- 4.3. Event logs must contain sufficient information to facilitate analysis and investigation, including timestamps, source IP addresses, user accounts, and descriptions of the events.
- 4.4. Real-time monitoring of event logs must be conducted by NOC and cybersecurity teams to detect and respond to security incidents promptly.
- 4.5. Detected events must be analyzed to determine their significance, potential security implications, and appropriate response actions.
- 4.6. Incidents identified through event log analysis must trigger the organization's incident response procedures for swift and effective resolution.
- 4.7. Event logs must be retained for a minimum period of one year, as required by legal and regulatory requirements.
- 4.8. The retention period for records does not mean keeping them on the SIEM application, but rather storing them through backups in encrypted and secure storage locations.
- 4.9. Event logs must be protected against unauthorized access, tampering, and deletion.
- 4.10. Access to event logs must be restricted to authorized personnel only.
- 4.11. Event logs must be stored in a secure location, separate from the systems generating the logs, to prevent loss in case of system compromise.
- 4.12. Event logs containing sensitive information must be encrypted during transmission and storage.
- 4.13. It is necessary to review the alerts issued by the SIEM daily in case there are any serious alerts that need to be addressed



5. Non-compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

6. References

- ISO 27002
- National Cybersecurity Authority's (NCA) ECC standards
- NIST CSWP

