Sharing allow:
TLP - GREEN

Approved

System Logging and Security Monitoring Standard

Document ID: **SEC-06**
For: Alliance Federation
Approval Date: 2023-03-22
Approved By: NSC

1. Introduction

The purpose of this standard is to define a consistent approach for the implementation of logging and monitoring practices across the Alliance Federation. This will ensure effective and early detection and identification of security or operational events and will enable forensics.

2. Definitions

Information security definitions are available in *SEC-00 Information Security Glossary*.

3. Applicability

This standard applies to all Alliance Federation Systems and Services, including all services, systems, components, hosts (both physical and virtual), networking equipment, and applications or any systems and services both internally or externally, that directly or indirectly support the mandated services.

Service Owners must ensure that the services, systems or components they are accountable for, are designed, configured and operated in accordance with this standard.

4. Logging and Monitoring Requirements

4.1 Required Logging Activities

All components in scope must generate logs or records as applicable for the following types of events:

4.1.1 **Resource utilization:** For each resource allocated via an allocation process, a log of the actual resource allocated and a log of resource consumption must be recorded.
4.1.2 **Metrics:** Metrics required to assess current system or service state (i.e. availability, performance, utilization, etc) must be recorded.
4.1.3 **Access and authorization**: All access and authorization events must be recorded when a user or machine initiated session is created or re-established.
4.1.4 **Authentication**: All authentication events must be recorded.
4.1.5 **Network activity**: All network communications activity about data entering or leaving a facility secured perimeter must be recorded. It is also recommended to log in the same way all communication between internal security domains.
4.1.6 **Asset information**: Assets information must be recorded in compliance with requirements defined in the Asset Management standard.
4.1.7 **Vulnerabilities**: Vulnerability information must be recorded in compliance with requirements defined in the *SEC-04 Vulnerability Management Standard*.
4.1.8 **Use of privileges**: For each service, system or component, a log of all attempted and successful privilege escalation must be recorded.
4.1.9 **Identity Auditing**: For every account or identity, events pertaining to the creation, modification, or deletion must be recorded.

Every system or component must be configured to ensure that its clock is synchronized to a reliable and trustworthy time source. Every system or component should also be configured to maintain time accuracy and to prevent clock drifting or tampering. Every log or record must contain a timestamp that is compliant with the ISO 8601 format where possible and be mapped to Coordinated Universal Time (UTC) where possible, or use local time with an offset from UTC. Timestamps must provide time resolution up to the milliseconds and systems clock should aim at maintaining clock accuracy consistent with this resolution.

In the situation where records contain unique identifiers or keys that can be changing over time, a record of these changes must also be made available to ensure uniqueness of log records.

4.2 Centralized Logging

Every system or component must be configured to record its logs to a trusted and authorized remote logging system. Where possible, a single logging system within a security domain should be used. Required log events identified in section 4.1 must be made available to the Alliance Federation through the authorized Alliance Federation monitoring platform(s) and in compliance with any applicable Alliance Federation data standards.

Logging and monitoring systems must be configured to detect and generate timely alerts upon system error, loss of integrity, or storage failure or exhaustion that could prevent logs from being captured or from being accurate.

4.3 Required Monitoring Activities

Logs should be used to detect or identify anomalies or suspicious activity. It is recommended to develop security baselines and use automation to generate timely alerts. Through monitoring activities, logs will be used by authorized personnel to detect, alert, investigate or track suspicious activities as well as to report on system or service status and usage. Monitoring use cases and baselines must be documented, including proper identification of required logs and datasets, along with intended or authorized use.

4.4 Access Control

Logging systems must be configured to limit access to authorized individuals or systems only. Such access must be limited to the minimal access needed to perform job duties and must protect logs from unauthorized modification. Access to logging systems and logs therein must be recorded. Access to logs or content therein must be provided through an interface or system that prevents tampering or altering of logs or records.

4.5 Log Classification and Sharing

The Cybersecurity Data classification of logs is according to the *SEC-02 Data Classification Policy*. The default data classification for logs is High Risk Information (Level 3), with the exception of Resource Utilization and Metrics for which the default classification is Medium Risk Information (Level 2). The Data Owner or Data Steward is responsible for ensuring that the Data Classification is appropriate and to reclassify if necessary. Any such reclassification must be documented and communicated while ensuring that appropriate logging systems are being used.

By default, the logs Sharing Designation is TLP:AMBER. This designation means that the logs can be shared with the Alliance Federation on the principle of least privilege and that any further sharing requires prior approval by the Data Owner or Data Custodian. The sharing of logs must be done using approved platforms and in compliance with *SEC-03 Data Handling Standard*.

4.6 Log Retention

Logging systems must be designed to account for the expected log volume, including potential reasonable bursts. Electronic logs that are collected must be maintained and readily available for a minimum duration of 90 days. Various situations might result in the need for early destruction. Any such situation must be documented and approved by the Data Owner or Data Custodian.

4.7 Log Disposal

Upon reaching end of life, logs and logging systems must be disposed of securely and in compliance with the *SEC-03 Data Handling Standard*.

5. Related Information

SEC-00 Information Security Glossary
SEC-02 Data Classification Policy
SEC-03 Data Handling Standard
SEC-04 Vulnerability Management Standard
Asset Management Standard