LOG MONITORING STANDARD

Effective: September 1, 2020

Logs from critical systems, applications and services can provide key information and potential indicators of compromise of security. The retention and review of logs are critical from a forensics standpoint.

Purpose of Standard

The purpose of this Standard is to identify specific requirements that information systems must meet in order to generate appropriate audit logs and integrate with Catalyst's log management function.

Application of Standard

This Standard applies to core networking infrastructure such as firewalls and routers in addition to critical servers on the Catalyst network that support logging. Critical servers are publicly exposed, store restricted data or information that must be protected for regulatory compliance purposes.

General Requirements

All systems that handle personal information, accept external network connections, or makes access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to answer the following questions:

1. What activity was performed?
2. When was the activity performed?
3. Who (or what) performed the activity?
4. On what object was the activity was performed?
5. What was the status (i.e. success vs. failure), outcome, or result of the activity?

Activities to be Logged

Logs shall be created whenever any of the following activities are requested to be performed by the system:

1. Create, read, update, or delete restricted information, including confidential authentication information such as passwords;
2. Create, update, or delete information not covered in Paragraph 1 above;

3. Accept an external network connection;
4. User authentication and authorization for activities covered in Paragraphs 1 or 2, such as user login and logout;
5. Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;
6. System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;
7. Application process startup, shutdown, or restart;
8. Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as CPU memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and
9. Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

Elements of the Log

All logs shall identify or contain at least the following elements:

1. Type of action – examples include authorize, create, read, update, delete, and accept network connection
2. Subsystem performing the action – examples include process or transaction name, process or transaction identifier
3. Identifiers (as many as available) for the subject requesting the action – examples include username, computer name, IP address, and MAC address
4. Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address
5. Before and after values when action involves updating a data element, if feasible
6. Date and time the action was performed
7. Whether the action was allowed or denied by access-control mechanisms
8. Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable

Log Analysis

1. Log aggregation tools will be used for correlation and analysis.

2. Logs shall be reviewed to identify anomalies or abnormal events. When automation is not possible, reviews will occur on a weekly basis.

3. On an ongoing basis, log aggregation and correlation tools shall be tuned to better identify actionable events and decrease event noise.

Violations of Standard

- **Non-Compliance.** An employee who violates this Standard may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

- Data Classification Standard

Definitions and Terms

- None

Administration of this Standard

- **Questions.** You are encouraged to ask any questions you may have about this Standard. To learn more, please contact secure@catalyst.org.

- **Reporting.** It is important that you immediately report any suspected violation of this Standard by a Catalyst employee or third party to your manager or to HR. All good faith allegations of violations of this Standard will be fully and confidentially investigated.

- **Exception to Standard.** Limited exceptions to the Standard may apply due to variations in devices and platforms. Management does not have the authority to approve exceptions to this Standard. Any request for an exception to the requirements of this Standard must be submitted to the Information Security Officer, who will review the risk of non-adherence and issue exceptions where deemed prudent.

- **Applicability.** This Standard applies globally unless contrary to local laws and regulations. Operations in different countries may have more stringent policies or implementing procedures where required by local law. In the event of a conflict, these more stringent policies or implementing procedures will take precedence.

Revision History

Date	Name	Description	Responsibility
09/01/2020	James Mbassa	Initial release.	Owner