SANS

Information Logging Standard

Last Update Status: *Updated October 2022*

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

1. Overview

Logging from critical systems, applications and services can provide key information and potential indicators of compromise. Although logging information may not be viewed on a daily basis, it is critical to have from a forensics standpoint.

2. Purpose

The purpose of this document attempts to address this issue by identifying specific requirements that information systems must meet in order to generate appropriate audit logs and integrate with an enterprise's log management function.

The intention is that this language can easily be adapted for use in enterprise IT security policies and standards, and also in enterprise procurement standards and RFP templates. In this way, organizations can ensure that new IT systems, whether developed in-house or procured, support necessary audit logging and log management functions.

3. Scope

This policy applies to all production systems on <Company Name> Network.

4. Policy

4.1 General Requirements

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

4.1.1 What activity was performed?
4.1.2 Who or what performed the activity, including where or on what system the
4.1.3 activity was performed from (subject)?
4.1.4 What the activity was performed on (object)?
4.1.5 When was the activity performed?
4.1.6 What tool(s) was the activity was performed with?
4.1.7 What was the status (such as success vs. failure), outcome, or result of the activity?

4.2 Activities to be Logged

© 2022 SANS™ Institute

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

4.2.1 Create, read, update, or delete confidential information, including confidential authentication information such as passwords;
4.2.2 Create, update, or delete information not covered in #1;
4.2.3 Initiate a network connection;
4.2.4 Accept a network connection;
4.2.5 User authentication and authorization for activities covered in #1 or #2 such as user login and logout;
4.2.6 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;
4.2.7 System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;
4.2.8 Application process startup, shutdown, or restart;
4.2.9 Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for 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
4.2.10 Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

4.3 Elements of the Log

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term “indirectly” means unambiguously inferred.

4.3.1 Type of action – examples include authorize, create, read, update, delete, and accept network connection.
4.3.2 Subsystem performing the action – examples include process or transaction name, process or transaction identifier.
4.3.4 Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
4.3.5 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. Note that such identifiers should be standardized in order to facilitate log correlation.
4.3.6 Before and after values when action involves updating a data element, if feasible.
4.3.7 Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.
4.3.8 Whether the action was allowed or denied by access-control mechanisms.

© 2022 SANS™ Institute

Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

4.4 Formatting and Storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Note that the construction of an actual enterprise-level log management mechanism is outside the scope of this document. Mechanisms known to support these goals include but are not limited to the following:

4.4.1 Microsoft Windows Event Logs collected by a centralized log management system;

4.4.2 Logs in a well-documented format sent via *syslog*, *syslog-ng*, or *syslog-reliable* network protocols to a centralized log management system;

4.4.3 Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document; and

4.4.4 Other open logging mechanisms supporting the above requirements including those based on CheckPoint OpSec, ArcSight CEF, and IDMEF.

5. Policy Compliance

5.1 Compliance Measurement
The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

None.

7. Definitions and Terms

None.

8. Revision History

© 2022 SANS™ Institute

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.
October 2022	SANS Policy Team	Converted to new format.

© 2022 SANS™ Institute