Log Management Policy

ACME Evil Anvil Corporation

March 2019

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC7.2

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. This log management and review policy defines specific requirements for information systems to generate, store, process, and aggregate appropriate audit logs across the organization's entire environment in order to provide key information and detect indicators of potential compromise.

b. This policy applies to all information systems within the organization's production network.

c. This policy applies to all employees, contractors, and partners of the organization that administer or provide maintenance on the organization's production systems. Throughout this policy, these individuals are referred to as system administrators.

2 Background

a. In order to measure an information system's level of security through confidentiality, integrity, and availability, the system must collect audit data that provides key insights into system performance and activities. This audit data is collected in the form of system logs. Logging from critical systems, applications, and services provides information that can serve as a starting point for metrics and incident investigations. This policy provides specific requirements and instructions for how to manage such logs.

3 Policy

a. All production systems within the organization shall record and retain audit-logging information that includes the following information:

    i. Activities performed on the system.

    ii. The user or entity (i.e. system account) that performed the activity, including the system that the activity was performed from.

    iii. The file, application, or other object that the activity was performed on.

    iv. The time that the activity occurred.

    v. The tool that the activity was performed with.

    vi. The outcome (e.g., success or failure) of the activity.

b. Specific activities to be logged must include, at a minimum:

i. Information (including authentication information such as usernames or passwords) is created, read, updated, or deleted.

ii. Accepted or initiated network connections.

iii. User authentication and authorization to systems and networks.

iv. Granting, modification, or revocation of access rights, including adding a new user or group; changing user privileges, file permissions, database object permissions, firewall rules, and passwords.

v. System, network, or services configuration changes, including software installation, patches, updates, or other installed software changes.

vi. Startup, shutdown, or restart of an application.

vii. 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.

viii. Detection of suspicious and/or malicious activity from a security system such as an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

c. Unless technically impractical or infeasible, all logs must be aggregated in a central system so that activities across different systems can be correlated, analyzed, and tracked for similarities, trends, and cascading effects. Log aggregation systems must have automatic and timely log ingest, event and anomaly tagging and alerting, and ability for manual review.

d. Logs must be manually reviewed on a regular basis:

i. The activities of users, administrators and system operators must be reviewed on at least a monthly basis.

ii. Logs related to PII must be reviewed on at least a monthly basis in order to identify unusual behavior.

e. When using an outsourced cloud environment, logs must be kept on cloud environment access and use, resource allocation and utilization, and changes to PII. Logs must be kept for all administrators and operators performing activities in cloud environments.

f. All information systems within the organization must synchronize their clocks by implementing Network Time Protocol (NTP) or a similar capability. All information systems must synchronize with the same primary time source.