

### Definitions

**End points:** Any user device connected to a network. End points can include personal computers, personal digital assistants, scanners, etc.

**Flow:** The traffic that corresponds to a logical connection between two processes in the network.

**IP:** Internet Protocol is the method or protocol by which data is sent from one computer to another on the Internet.

**Packet:** The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.

### Overview

Most components of the IT infrastructure at {COMPANY-NAME} are capable of producing logs chronicling their activity over time. These logs often contain very detailed information about the activities of applications and the layers of software and hardware that support those applications.

Logging from critical systems, applications, and services can provide key information and potential indicators of compromise and is critical to have for forensics analysis.

### Purpose

Log management can be of great benefit in a variety of scenarios, with proper management, to enhance security, system performance, resource management, and regulatory compliance. {COMPANY-NAME} will perform a periodic risk assessment to determine what information may be captured from the following:

- Access – who is using services
- Change Monitoring – how and when services were modified
- Malfunction – when services fail
- Resource Utilization – how much capacity is used by services
- Security Events – what activity occurred during an incident, and when
- User Activity – what people are doing with services

### Policy Detail

#### Log generation

Depending on the volume of activity and the amount of information in each log entry, logs have the potential of being very large.

Information in logs often cannot be controlled by application, system, or network administrators, so while the listed items are highly desirable, they should not be viewed as absolute requirements.

#### Application logs

Application logs identify what transactions have been performed, at what time, and for whom. Those logs may also describe the hardware and operating system resources that were used to execute that transaction.

#### System logs

System logs for operating systems and services, such as web, database, authentication, print, etc., provide detailed information about their activity and are an integral part of system administration.

When related to application logs, they provide an additional layer of detail that is not observable from the application itself. Service logs can also aid in intrusion analysis, when an intrusion bypasses the application itself.

Change management logs, that document changes in the IT or business environment, provide context for the automatically generated logs.

Other sources, such as physical access or surveillance logs, can provide context when investigating security incidents.

Client workstations also generate system logs that are of interest, particularly for local authentication, malware detection, and host-based firewalls.

### Network logs

Network devices, such as firewalls, intrusion detection/prevention systems, routers, and switches are generally capable of logging information. These logs have value of their own to network administrators, but they also may be used to enhance the information in application and other logs.

Many components of the IT infrastructure, such as routers and network-based firewalls, generate logs. All of the logs have potential value and should be maintained. These logs typically describe flows of information through the network, but not the individual packets contained in that flow.

Other components for the network infrastructure, such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) servers, provide valuable information about network configuration elements, such as IP addresses, that change over time.

### Time synchronization

One of the important functions of a log management infrastructure is to relate records from various sources by time. Therefore, it is important that all components of the IT infrastructure have synchronized clocks.

{COMPANY-NAME} uses Network Time Protocol (NTP) for time synchronization.

### Use of log information

Logs often contain information that, if misused, could represent an invasion of the privacy of members of {COMPANY-NAME}. While it is necessary for {COMPANY-NAME} to perform regular collection and monitoring of these logs, this activity should be done in the least invasive manner.

### **Baseline behavior**

It is essential that a baseline of activity, within the IT infrastructure, be established and tracked as it changes over time. Understanding baseline behavior allows for the detection of anomalous behavior, which could indicate a security incident or a change in normal usage patterns. Procedures will be in place to ensure that this information is reviewed on a regular and timely basis.

### **Investigation**

When an incident occurs, various ad hoc questions will need to be answered. These incidents may be security related, or they may be due to a malfunction, a change in the IT infrastructure, or a change in usage patterns. Whatever the cause of the incident, it will be necessary to retrieve and report log records.

Thresholds shall be established that dictate what level of staff or management response is required for any given log entry or group of entries and detailed in a procedure.

### **Log record life-cycle management**

When logs document or contain valuable information related to activities of {COMPANY-NAME}'s information resources or the people who manage those resources, they are {COMPANY-NAME} Administrative Records, subject to the requirements of {COMPANY-NAME} to ensure that they are appropriately managed and preserved and can be retrieved as needed.

### Retention

To facilitate investigations, as well as to protect privacy, the retention of log records should be well defined to provide an appropriate balance among the following:

- Confidentiality of specific individuals' activities
- The need to support investigations
- The cost of retaining the records

Care should be taken not to retain log records that are not needed. The cost of long-term retention can be significant and could expose {COMPANY-NAME} to high costs of retrieving and reviewing the otherwise unneeded records in the event of litigation.

### Log management infrastructure

A log management infrastructure will be established to provide common management of log records. To facilitate the creation of log management infrastructures, system-wide groups will be established to address the following issues:

- Technology solutions that can be used to build log management infrastructures
- Typical retention periods for common examples of logged information