# Network security logging and monitoring

CANADIAN CENTRE FOR CYBER SECURITY

December 2022 | ITSAP.00.085

Networks are the backbone infrastructure supporting information technology (IT) systems, operational technology (OT), and industrial control systems (ICS). A secure network infrastructure is vital for organizations and governments as it offers critical protection from breaches, intrusions, and other cyber threats. Logging and monitoring are measures that will help your organization identify indicators of compromise (IoCs), take corrective actions in a timely manner, and minimize the impact when a security incident occurs. This document provides high-level guidance for conducting network logging and monitoring.

## What is network security logging and monitoring?

**Logging** is the process of collecting data that represents specific activities, events, error conditions, or the general status of an information system or network. The goal is to capture security-relevant data for system administrators to gain insight on how systems are behaving, and to support investigations of potential or actual breaches.

**Monitoring** is the process of observing the data collected from multiple sources, including network devices, servers, applications, databases, and other IT infrastructure components, in order to identify changes and anomalies. The goal of monitoring is to look for indications of known attacks, unusual changes in system behaviour or unauthorized security-related activities. Monitoring should be conducted by security analysts or a security team, and not by the system administrators that set up and configure the systems.

### Security information and event management (SIEM)

One type of commonly used tool for logging and monitoring is a security information and event management platform. A SIEM centralizes data from users, network devices, applications, and endpoints. Some of its basic capabilities include:

- Monitoring and analyzing real-time and historical events.
- Normalizing or reformatting log data into a standard format to facilitate analysis.
- Facilitating audit record correlation and analysis (e.g. correlating events with vulnerability scan results).
- Detecting security incidents as well as issuing notifications and alerts to users when threats (real or potential) are identified.
- Ingesting dynamic information about IoCs and reporting if they are detected on the network.
- Archiving logs, which is beneficial during incident detection, response, and post-incident recovery.

## What are the benefits of network logging and monitoring?

Logging and monitoring activities can help your organization detect internal or external threats, and mitigate network vulnerabilities before they can be exploited by threat actors. Other benefits of logging and monitoring includes:

- Monitoring device use compliance against organizational policies.
- Facilitating risk-based decision making with near real-time monitoring.
- Discovering potential security weaknesses, vulnerabilities, and configuration errors within a network.
- Detecting rogue or unauthorized devices on the network.
- Detecting security incidents from analysis of log data, which can assist with identifying the source and the extent of compromise during investigations of security incidents.
- Facilitating the evaluation of the overall health of your network infrastructure.

### Cloud-service providers (CSP) and network monitoring

If your organization subscribes to a cloud service, be informed and understand how your CSP is protecting you and your valuable assets. Some examples of questions to ask are:

- What kind of monitoring is being performed?
- What is the level of monitoring (e.g. how often is log data reviewed and assessed)?
- What certifications does the CSP meet (e.g. AICPA SOC 2 Type 2)?
- Where is the client subscriber's log data stored?
- What log data is available to client subscribers?
- What is the log data retention and destruction policy?

Communications Security Establishment | Centre de la sécurité des télécommunications



Canada

# Network security logging and monitoring

CANADIAN CENTRE FOR CYBER SECURITY

December 2022 | ITSAP.00.085

The information gathered from logging and monitoring activities provides valuable input for your organization to make informed and effective risk-based decisions. By implementing the following best practices, you can strengthen your organization's cyber security posture, minimize the risks to your operations, and avoid unnecessary disruptions to your clients.

## Network security logging and monitoring best practices

- ☐ Develop a monitoring plan that defines the risks to which your organization is exposed; identifies important assets and events that need to be logged and monitored; and specifies your organization's log retention policies, and monitoring processes, procedures, and tools.
- ☐ Implement a logging strategy for collecting data from all necessary sources. Aim to centralize and consolidate log data using a SIEM tool. This will facilitate security and network operations to perform data analysis and take immediate corrective actions.
- ☐ Ensure log data at rest is cryptographically protected to prevent from being maliciously tampered with.
- ☐ Establish a baseline behaviour of your network traffic patterns and performance metrics. This will give you a point of reference to detect anomalous behaviour.
- ☐ Monitor outbound connection attempts from internal networks and evaluate whether there are indications of a compromised host.
- ☐ Monitor for unauthorized data transfers from the system to detect exfiltration of data signaling a potential breach or compromise.
- ☐ Implement malware prevention measures such as anti-virus software and application allow lists. For more information, see Preventative Security Tools (ITSAP.00.058) and Top 10 IT security action items: No. 10 Implement application allow lists (ITSM.10.095).
- ☐ Deploy monitoring agents at the network edge, like external boundaries, to detect connections from unknown sources.
- ☐ Where possible, automate the collection of logs and data analysis. Use tools that can analyze logs and automatically trigger alerts on relevant events.
- ☐ Use tools and technologies for efficient data collection and analysis. The National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-137, Appendix D provides information on various tools and technologies for data gathering, aggregations, and analysis, such as SIEM tools, Intrusion Detection Systems (IDSs), and Intrusion Prevention Systems (IPSs).
- ☐ Develop an incident response plan and related policies. For more information, see Developing your incident response plan (ITSAP.40.003).
- ☐ Establish a security operations center (SOC) or subscribe to a SOC service. A SOC uses people, processes, and technology to continuously monitor, identify, mitigate, and investigate cyber security threats to your network infrastructure.
- ☐ Back up device configurations in a safe, and centralized location.
- ☐ Monitor configurations on all devices connected to the network. Check for any changes to the system configuration against a known baseline.
- ☐ Limit the number of system administrators that can make changes to your infrastructure. Ensure each has their own account with passphrases or strong passwords and multi-factor authentication (MFA), where possible. As an example, you can choose to follow the Information Technology Infrastructure Library (ITIL) change management process.
- ☐ Continuously monitor network infrastructure components such as devices, servers, applications, databases, routers, and firewalls. Collect information on the state of the devices, their compliance with established policy, and device events related to user, authentication, and connection activity in particular.
- ☐ Monitor activity related to user accounts and user access (e.g. creation, deletion, disabling, password changes, lockouts, failed logons, and privilege escalation).
- ☐ Verify legal requirements and related policies regarding personal information that can be present on a network, and adjust monitoring activities accordingly. For example, do not perform deep inspection or other intrusive monitoring on banking or health-related websites.
- ☐ Perform regular network security audits. Valuable information from the audit will enable you to adjust your logging and monitoring practices accordingly. For more information, see Network security auditing (ITSAP.00.086).

### ICS/OT systems and network monitoring

For operators of ICS/OT systems, take caution when using automated inventory and vulnerability detection tools which can scan these systems aggressively. These tools may cause devices to behave erratically, stop working/crash, restart or need manual intervention to revert to an operational state. Consider the following when selecting technologies for monitoring your ICS and OT systems:

- Ensure technology is ICS-focused and understands ICS communications, such as deep packet inspection capabilities.
- Ensure the technology is ICS capable, for example, it maintains profiles for data communications protocols such as modbus or fieldbus.

Communications Security Establishment | Centre de la sécurité des télécommunications



Canada