Press release

August 22 2024
National Center of Incident Readiness and Strategy for Cybersecurity

Co-sealing the Australian-Led International Guidance on the Best Practices for Event Logging and Threat Detection

1. Overview

On August 22, 2024, the National Center of Incident Readiness and Strategy for Cybersecurity co-sealed and published an international guidance entitled "Best practices for event logging and threat detection" (hereinafter referred to as the "Guidance"). The Guidance was prepared by the Australian Cyber Security Centre (ACSC) under the Australian Signals Directorate (ASD). Tentative translations will be released as soon as possible.

The following nine countries co-sealed the Guidance and are listed as co-authors: Australia, Japan, United States (US), United Kingdom (UK), Canada, New Zealand, Singapore, South Korea and Netherland.

The Guidance is primarily for senior information technology (IT) decision makers and network operators and is the international best practice for event logging and threat detection. We decided to co-seal it because providing technical measures to combat “living off the land” techniques, which are considered difficult to detect, will contribute to the enhancement of cybersecurity in Japan.

We will continue our efforts to strengthen international cooperation in the field of cybersecurity.

2. Overview of the Guidance

(1) The increased prevalence of malicious actors employing living off the land techniques highlights the importance of event logging. The Guidance describes best practices for event logging and threat detection for the cloud, enterprise networks, enterprise mobility, and OT (Operational Technology) networks.

(2) The Guidance is intended for medium to large organizations and is especially for senior information technology (IT) and OT decision makers, IT and OT operators and network administrators and critical infrastructure operators.

(3) Best practices for event logging include:

A) Event Logging policy
Regarding creating a log policy, list the details to be included in the event log (event log details to retain), and ensure content and format consistency, timestamp consistency, and event log retention (retention period, etc.).

B) Centralized log collection and correlation
Describe the prioritization of logs to retain (a detailed list of log sources) for enterprise networks, OT, enterprise mobility and cloud.

C) Secure storage and event log integrity
Describe event logs protection and access restrictions to ensure integrity.

D) Detection strategy for relevant threats

Examples of abnormal behavior are listed below. It is recommended that abnormal behavior is automatically detected.

- a user logging in during unusual hours (e.g. non-working hours, holidays or on leave)
- an account accessing services that it does not usually access, for example, administrator or HR services
- a user logging in using an unusual device
- a high volume of access attempts
- instances of impossible travel or concurrent sign ins from multiple geographic locations
- downloading or exporting a large volume of data
- network logins without defined computer access or physical access log validation
- a single IP address attempting to authenticate as multiple different users
- creation of user accounts, or disabled accounts being re-enabled, especially accounts with administrative privileges
- netflow data indicating one device talking to other internal devices it normally does not connect to
- unusual script execution, software installation, or use of administrative tools
- unexpected clearing of logs
- an execution of the process from an unusual or suspicious path
- configuration changes to security software, such as Windows Defender, and logging management software

(End)