Press release

May 27, 2025
National Center of Incident Readiness and
Strategy for Cybersecurity

Co-sealing the Australian-Led International Document “Implementing SIEM and SOAR Platforms”

1. Overview

On May 27, 2025, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) co-sealed and published an international document providing guidance on SIEM and SOAR platforms (hereinafter referred to as the "Document"). The Document was authored by the Australian Signals Directorate’s Australian Cyber Security Centre (ASD’s ACSC). Tentative translations will be released as soon as possible.

The following countries co-sealed the Document and are listed in the Document: Australia, Japan, the United States of America (US), United Kingdom (UK), Canada, New Zealand, Singapore, South Korea, and the Czech Republic.

The Document is intended for organizations that are considering procuring or are already operating SIEM and/or SOAR platforms.* It provides definitions, possible advantages, challenges, and best practices for procuring, installing, and maintaining these platforms. The Document is divided into three parts: (1) Executive Guidance, (2) Practitioner Guidance, and (3) Priority Logs for SIEM Ingestion — Practitioner Guidance.

The NISC co-sealed the Document because if Japanese companies, including critical infrastructure providers, refer to the advice in the Document on SIEM and SOAR platforms, it will greatly contribute to enhancing Japan's cybersecurity.

The NISC will continue to make efforts to foster international collaboration in the field of cybersecurity.

2. Overview of the Document

(1) Introduction

Practitioner Guidance provides guidance on the following four points for organizations that are considering procuring or are already operating SIEM and/or SOAR platforms:

(2) Overview of the four points

A) Definition of SIEM and SOAR:

SIEM refers to a software platform or device that collects, centralizes, and analyzes log data from multiple sources within a network. SOAR refers to a set of software platforms that automate responses to anomalous activities detected on a network.

B) Possible advantages of SIEM and/or SOAR:

Enhanced visibility within the network by collecting and centralizing logs and creating dashboards and reports; enhanced incident detection, including early warning of unusual activities; and enhanced responses through SIEM’s log

collection, centralization, early warning, and SOAR's automated response capabilities

C) Challenges in implementing SIEM and/or SOAR:
In order to achieve effective log analysis, SIEM must be configured to match an organization's unique IT environment; setting up SOAR requires a number of staff with specialized skills; and implementation requires significant ongoing costs.

D) Best practice principles for implementing SIEM and/or SOAR:
Provide referenceable best practices for a wide range of technical and human resources issues regarding procurement, installation, and maintenance.

* "Priority Logs for SIEM Ingestion — Practitioner Guidance" classifies the specific data sources of the logs that practitioners should collect according to priorities, thereby providing useful information for Japanese companies and other organizations.

3. Related links

[Link to the original]

For enquiries regarding this press release, please contact:

National Center of Incident Readiness and Strategy for Cybersecurity
International Strategy Group, International Cooperation Unit
Phone: 03-6277-7071

(End)