Implementing SIEM and SOAR platforms: Executive guidance

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

National Cyber Security Centre
a part of GCHQ

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

JPCERT CC®

CSA SINGAPORE

National Cyber and Information Security Agency NÚKIB

The authors would like to acknowledge the industry partners that contributed to this publication

Introduction

This publication:

- explains the value of Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms.
- explains how these platforms work.
- outlines their challenges.
- provides high-level recommendations for implementing them.

It is primarily intended for decision-makers at an organisation's executive level but can be used by any organisation that is considering whether and how to implement a SIEM and/or a SOAR.

This publication is one of three in a suite of guidance on SIEM and SOAR platforms:

Implementing SIEM and SOAR platforms: Executive guidance

This document is intented for executives. It defines SIEM/SOAR platforms, outlines their benefits and challenges, and provides broad recommendations for implementation that are relavant to executives.

Implementing SIEM and SOAR platforms: Practitioner guidance

This document is intended for cyber security practitioners. In greater technical details, it defines SIEM/SOAR platforms, outlines the benefits and challenges, and provides best practice principles for implementation.

Priority logs for SIEM ingestion: Practitioner guidance

This document is intended for cyber security practitioners and provides detailed, technical guidance on the logs that should be prioritised for SIEM ingestion. It covers log sources including Endpoint Detection and Response tools, Windows/Linux operating systems, and Cloud and Network Devices.

This guidance should also be read alongside Best Practices for Event Logging and Threat Detection, which provides high-level recommendations on developing a logging strategy.

1. What is the value of SIEM and SOAR platforms?

SIEM and SOAR platforms may be components of your organisation's logging and visibility strategy. Visibility is foundational for the detection of malicious cyber activity and is critical for an effective and holistic cyber security strategy.

These platforms can:

- enhance the **general visibility** of what is happening on your organisation's network by collecting, centralising, and analysing important, qualified event data that would otherwise be extremely complex and scattered
- enhance your organisation's **detection** of cyber security events and incidents by generating swift alerts about suspicious activity
- enhance event and incident detection by preventing malicious actors from modifying/deleting certain data to maintain their access to the network, as was observed in the Volt Typhoon campaign[1]
- enhance your organisation's **response** to cyber security events and incidents by prompting timely intervention through alerting and ensuring incident responders have access to data that records what happened
- in the case of a SOAR, enhance event and incident response by automating certain response actions, shortening the mean time to respond, and allowing the security team to focus on more complex problems
- assist with implementing the Australian Signal Directorate's Essential Eight Maturity Model and and the Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Performance Goals (CPGs), which both require log data to be collected and centralised.[2]

Consequently, these platforms can help to keep your organisation's systems and services functioning and protect your data from unauthorised access or modification and theft.

However, these benefits are only delivered where the SIEM or SOAR is properly implemented (see Section 3).

2. How do these platforms work?

The network of a single organisation can be extremely complex, containing multiple devices, applications, operating systems and cloud services. Each of these sources within the network may also generate log data, or particular information about what is happening within the source (such as user activity on a device).

A SIEM is a type of software platform that **collects, centralises**, and **analyses** log data.

A SIEM gathers complex and dispersed log data from across the network and consolidates it into streamlined reports and dashboards. A SIEM also analyses this data through the application of rules and filters in order to detect anomalous network activity that could represent a cyber security event or incident. Many SIEM products enhance this analysis by incorporating up-to-date cyber threat intelligence from external sources. If it detects a potential event or incident, the SIEM will generate alerts, prompting the organisation's security team to investigate and respond as necessary.

A SOAR is a type of software platform that builds upon the collection, centralisation, and analysis of log data. Some SOAR platforms perform these functions themselves, while others integrate with an existing SIEM and leverage its log collection, centralisation, and analysis.

Either way, a SOAR automates some of the **response** to detected cyber security events and incidents. It does so by applying predefined 'playbooks', which set certain actions to be taken when specific events occur, such as isolating the source of the event in the network. These automated actions do not replace human incident responders but can complement them.[3]

3. What are the key challenges of implementing these platforms?

Neither a SIEM nor a SOAR is a 'set and forget' tool. Implementing either platform is an intensive, ongoing process that requires highly skilled human personnel. These personnel face two key technical challenges.

The first is ensuring that the SIEM produces alerts when cyber security events and incidents are occurring and, inversely, no alerts when no events/incidents are occurring. To achieve this, personnel need to identify the right types and quantities of log data for the SIEM to ingest, as well as the right rules and filters to apply to that data. This includes developing a threat model that defines events of interest that can trigger alerts related to the model in order to promote accurate alerting. If accurate alerting is not achieved, security teams may be operationally overwhelmed by false alerts from the SIEM or miss real events/incidents because of the absence of alerts.

The second key technical challenge is ensuring that the SOAR only takes appropriate action in response to actual cyber security incidents, and does not take action against regular network activity or impede human incident responders. If accurate actioning is not achieved, the SOAR may significantly disrupt service delivery.

To meet these technical challenges, personnel must carefully configure the SIEM and/or SOAR for the unique network and organisation in which it is used. They must then continually adjust it and test its effectiveness as the network, technology, and cyber threat landscape keep changing. This ongoing work may be done internally, by an external service provider, or through some combination of the two.

Properly implementing a SIEM and/or SOAR therefore involves significant costs. These may include the upfront and sustained:

- licensing and/or data use costs of the platform
- costs of hiring and retaining staff with in-demand, specialist skills in implementing a SIEM and/or SOAR
- costs of upskilling existing staff, as well as the continual training that is necessary to enable them to maintain the platform as the technology, network, and threat landscape change
- service costs, if implementation is outsourced.

However, failing to detect or properly respond to a cyber security incident can be extremely costly. It may also lead to your organisation having systems taken offline, service delivery disrupted, data leaked or destroyed, and public confidence lost. For more on defining scope of implementation for your organisation, please see Implementing SIEM and SOAR platforms: Practitioner guidance.

4. Recommendations for implementation

Below are high-level, strategic recommendations for executives who are considering whether and how to implement a SIEM and/or SOAR. It is important to note that these platforms are just one form of technology that can collect and centralise log data and enhance incident detection – there are other options, such as log management tools.

a. Consider whether you need to, and can, implement the platform in-house

If your organisation manages sensitive information or provides critical services, it may be necessary to implement the platform in-house.

A key benefit of implementing a SIEM and/or SOAR in-house is that staff will generally have strong knowledge of the organisation's unique network and business processes, as well as authority to query users about unusual behaviour and instigate incident response actions. In contrast, outsourcing can produce visibility gaps, work duplication, and communication difficulties.

However, developing and retaining an in-house capability can be challenging because it is resource-intensive and these skills are in high demand. Executives should expect that multiple personnel will need to work on implementing the SIEM and/or SOAR on a full-time basis. Operating these platforms can also involve long periods of highly stressful work.

If your organisation does outsource some or all of the implementation, the authoring agencies recommend considering whether different service providers:

- provide a high-quality, 24/7 monitoring and incident response service
- are known to have good cyber security posture
- are bound by foreign data storage requirements
- are located in a foreign nation or have offices in foreign nations.

You should also pay special attention to contractual provisions regarding:

- how the service's effectiveness will be verified and assured
- how the service provider will verify their compliance with the legislative, regulatory, and internal requirements that apply to your organisation
- the service provider's skill level
- the services to be delivered, including use of standards, training and end user feedback
- the degree of visibility the service provider will provide back to your organisation
- the division of responsibility and liability for detecting and responding to cyber security incidents.

b. Look for potential hidden costs across different products

The authoring agencies recommend carefully examining the costs involved in different SIEM and/or SOAR products. It is common for personnel to feed a SIEM increasing amounts of log data over time to improve the platform's visibility and detection. Most SIEM pricing models are based on the quantity of data the SIEM ingests. Some products cap ingestion according to a pre-purchased amount. For products that do not, your organisation should be mindful of the potential to incur very significant costs if ingestion is not carefully managed.

The Implementing SIEM and SOAR platforms: Practitioner guidance publication provides further guidance on ways to reduce the costs of collecting, centralising, and analysing logs through these platforms, and on defining the scope of implementation for your organisation. Please also see Best practices for event logging and threat detection.

c. Plan for the ongoing costs of implementation, particularly training costs

As outlined above, properly implementing a SIEM and/or SOAR involves significant upfront and sustained costs. Organisations should consult vendor documentation to determine whether alternative logging options can reduce these costs. For organisations that develop an in-house capability, the authoring agencies recommend committing significant effort and funding to continually train staff over time.

d. Properly implement a SIEM before you consider implementing a SOAR

In general, it is necessary to properly implement a SIEM and ensure it is accurately alerting you to cyber security events and incidents before implementing a SOAR.

e. Ensure the performance of the platform(s) is tested

It is essential to establish internal processes and procedures for testing whether the platform is effectively alerting you to cyber security events and incidents, as continual changes in networks, technologies and the cyber threat landscape will affect performance.

Once a mature SIEM and/or SOAR capability has been established, the authoring agencies recommend testing performance by using an external professional service capability, such as penetration testing. The authoring agencies recommend researching different SIEM and/or SOAR vendors that best suit the needs of your organisation.

Endnotes

[1] See Identifying and Mitigating Living Off the Land Techniques | Cyber.gov.au

[2] Please note that SIEMs are not the only tool that can collect and centralise log data, so if this is your organisation's primary concern, other tools might be more cost-effective. In particular, CISA's Logging Made Easy (LME) is a no cost, open source platform that centralises log collection. LME is intended for small- and medium-size organisations that need a log management and threat detection system; do not have an existing security operations centre (SOC), SIEM solution, or log management and monitoring capabilities; and/or work within limited budgets, time or expertise to set up and manage a logging and threat detection system. To get started with LME, download it directly from CISA's LME GitHub page. See Implementing SIEM and SOAR platforms: Practitioner guidance for further details.

[3] Please note that SIEMs and SOARs are just one form of detection technology. Other forms, such as canary technology, are not discussed here.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre