Best practices for setting up a security operations centre (SOC)

CANADIAN CENTRE FOR CYBER SECURITY

May 2023 | ITSAP.00.500

A security operations centre (SOC) combines people, processes, and technology to work together to improve your organization's resilience against cyber threats. A SOC is run from a central location by a team of information security professionals, including security engineers who may work closely with your development team, security analysts, and threat hunters. As cyber threats become more complex and threat actors become more sophisticated, many SOCs are being set up regionally as a first line of defence against cyber attacks, especially in healthcare and academia. Other reasons why SOCs are becoming more popular include an increase in the number of industrial control systems (ICS) and operational technologies (OT), as well as the adoption of mobile and cloud technologies. This document provides guidance for organizations of all sizes on best practices for setting up and operating your SOC. It also provides guidance to organizations interested in subscribing to a SOC as a service (SOCaaS) from a third-party provider.

What does a SOC do?

A SOC is primarily responsible for detecting and responding to cyber incidents and threats. SOCs can also conduct, vulnerability assessments, penetration testing, threat hunting, and auditing for regulatory compliance. SOCs performs the following activities:

Monitor

Continuously collect security and event data in real-time from across your organization’s IT infrastructure. This includes data from on-premises (on-prem) devices, the cloud, ICS and OT systems, remote systems, and mobile devices.

Detect

Identify abnormal trends, discrepancies, or other indicators of compromise (IoCs) from the volumes of data collected. Potential threats are categorized by severity and evaluated to determine whether they are actual threats your organization should be concerned about. Automated detection tools can also be used to isolate real threats.

Respond

Take immediate action to respond to incidents and deploy appropriate mitigation measures to address the threat. Following an incident, SOCs will restore your network and systems back to their baseline state and recover any lost or compromised data.

Analyze

Conduct root cause investigation using log data and other information to determine the source of the incident. This can help prevent similar incidents from happening in the future.

SOC as a service (SOCaaS)

If your organization has limited resources, it may be challenging to set up and operate a SOC. As an alternative, your organization could consider a SOCaaS subscription model. One option to explore is a hybrid approach to security. With this approach, SOC functions like monitoring and incident response would be done in-house but specialized functions like penetration testing or malware analysis would be outsourced. When selecting a SOCaaS provider, you should consider the following:

- What SOC services are offered?
- Can teams and services be easily scaled up or down to adapt to organizational needs or in response to specific events?
- Can services be tailored to your organization’s environment and industry?
- What tools and technologies are used to collect the data?
- What data will be captured?
- How will the data be used?
- Where is the data stored?
- How is sensitive data protected?
- What is included in the service level agreement (SLA)?
- How is the SLA measured or assessed?
- What security standards and practices are followed to assure supply chain vulnerabilities are mitigated?

What are the benefits of a SOC?

One of the main advantages of a SOC is that it combines efforts to support incident response, including threat identification, containment, eradication, recovery, and reporting. These combined efforts will assist your organization, whether it’s a large enterprise or within critical infrastructure, in improving your cyber security posture. Other benefits that a SOC can provide include:

- **Proactive threat hunting.** By combining historical data and threat intelligence, SOCs can help to find early evidence of attacks that might otherwise have gone unnoticed. SOCs can use artificial intelligence (AI) technology to look for patterns in the data collected and flag suspicious traffic for follow-up. Using various tools, SOCs can establish a baseline of your organization's expected traffic to facilitate finding malicious activities.
- **Improved incident detection and response times.** Depending on the size and level of expertise, SOCs can quickly detect signs of an attack, conduct an initial investigation, and start remediation to stop the threat. This heightened response can limit the extent of damage to your organization and help to prevent threat actors from accessing your valuable assets and sensitive information.
- **Cost savings.** SOCs can maximize your IT environment and reduce the number of tools and devices required to adequately protect your environment, reducing your IT budget.
- **Increased security visibility and centralized management of incidents.** Using tools and dashboards to provide real-time situational awareness of your organization’s security posture, SOCs will help you better coordinate resources needed to fix and contain threats.
- **Regular auditing of systems.** By ensuring industry and government regulations are followed, SOCs can help to protect your organization from reputational damage, administrative or material privacy violations, and legal liability in case of a breach.

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada

Best practices for setting up a security operations centre (SOC)

May 2023 | ITSAP.00.500

Considerations when establishing your SOC

With cyber attacks becoming more frequent and complex, the question is not if an attack will happen, but when. This is something your organization should keep in mind. A SOC can help to increase your organization's resilience against cyber threats and minimize the impact in the event of a compromise. The following are some best practices to consider when setting up and operating a SOC:

1. Develop a SOC strategy with the appropriate scope.

□ Identify which organizational assets, like systems and data, are highly valuable or sensitive and need to be monitored and protected.

□ Perform a cyber security risk assessment to understand the threats your organization faces. It can also be useful to understand the level of sophistication of threat actors targeting your organization. For Government of Canada (GC) departments, refer to ITSG-33, Annex A, Table 5 for description of threat agents. For non-GC organizations, consult the structured threat information expression (STIX) v2.1 framework for description of threat actor skill levels.

□ Understand the legal, regulatory, and compliance requirements that your organization operates under to know what the SOC is required to do or protect.

2. Design a SOC solution that meets organizational needs.

□ Select a SOC model that is comparable to your organization's threat profile and is achievable given your resources. Your requirements and the threats you face will change over time, so your model should be easily adapted to keep pace.

□ Incorporate threat-oriented defence into the routine security operations including those from threat frameworks such as MITRE ATT&CK and OWASP top ten.

□ For large organizations with broad geographical coverage, like hospitals and schools, consider integrating or consolidating multiple SOCs into a regional SOC. This enables SOCs to share information, jointly invest in tools and expert staff, and increase the situational awareness for the participating organizations.

3. Implement and operate the solution efficiently.

□ Collect meaningful data from sensors and logs generated from applications, operating systems, the network, the cloud, and ICS/OT systems.

□ Use automated technologies as part of your incident response strategy.

□ Select an event management solution that includes log collection and processing, storage, querying, alerting, and incident management. A number of commercial and open-source security information and event management (SIEM) platforms are available to help your organization derive value from the volumes of event data collected daily. Consider the ongoing configuration, support and licensing requirements when choosing the appropriate SIEM platform.

□ Establish a clear incident response plan, and test it regularly, to ensure critical functions can be restored and recovered in a timely manner. Simulate the issue response within an isolated, testing zone so that the production environment is not affected.

□ Ensure SOC services operate within their legal and regulatory requirements. Appropriate security controls should be in place and enforced, like data validation to identify sensitive information.

□ Develop clear documentation of processes and procedures to enable SOC team members to work efficiently.

□ Build the right SOC team by hiring people with a wide range of technical skills and experience. Create a retention strategy to minimize staff turnover.

□ Provide ongoing training to new and existing employees. This can improve their job satisfaction and improve skill levels to keep pace with evolving and emerging technology.

□ Invest in appropriate resources to care for your employees mental well-being. This can avoid burn out as a SOC is an area of high operational tempo.

4. Maintain and update the solution as necessary over time.

□ Encourage regular communication and collaboration amongst SOC team members and various stakeholders, like users, management, and system owners, across the organization. This can create a valuable feedback mechanism for the SOC to provide better services to your clients.

□ Collect metrics to measure SOC performance and effectiveness which will allow you to adjust the SOC operations accordingly.

□ Enhance SOC activities to include attack simulation and assessments, cyber deception, and insider threat hunting in order to stay ahead of sophisticated threat actors.

Learn more

- Network security logging and monitoring (ITSAP.80.085)
- Developing your incident response plan (ITSAP.40.003)
- Developing your IT recovery plan (ITSAP.40.004)
- National Cyber Security Centre's (NCSC) publication on building a security operations centre (SOC)
- MITRE Corporation's 11 strategies of a world-class cybersecurity operations center

Communications Security Establishment
Centre de la sécurité des télécommunications