علیرضا رضایی

تحقیق جلسه هفتم

Resources

https://www.techtarget.com/searchsecurity/definition/Security-Operations-Center-SOC

security operations center (SOC)

A security operations center (SOC) is a command center facility for a team of information technology (IT) professionals with expertise in information security (infosec) who monitors, analyzes and protects an organization from cyber attacks.

In the SOC, internet traffic, networks, desktops, servers, endpoint devices, databases, applications and other systems are continuously examined for signs of a security incident. SOC staff may work with other teams or departments but are typically self-contained with employees that have high-level IT and cybersecurity skills or outsourced to third-party service providers. Most SOCs function around the clock, with employees working in shifts to constantly log activity and mitigate threats.

Prior to establishing a SOC, an organization must define its cybersecurity strategy to align with current business goals and problems. Department executives reference a risk assessment that focuses on what it will take to maintain the company's mission and subsequently provide input on objectives to be met and infrastructure and tooling required to meet those objectives, as well as required staff skills.

SOCs are an integral part of minimizing the costs of a potential data breach as they not only help organizations respond to intrusions quickly, but also constantly improve detection and prevention processes.

Most large organizations have in-house SOCs, while companies without the staff or resources to maintain one themselves may opt to outsource some or all SOC responsibilities to a managed service provider (MSP), the cloud or a hosted virtual SOC.

SOCs are commonly found in healthcare, education, finance, e-commerce, government, military operations and advanced technology industries.

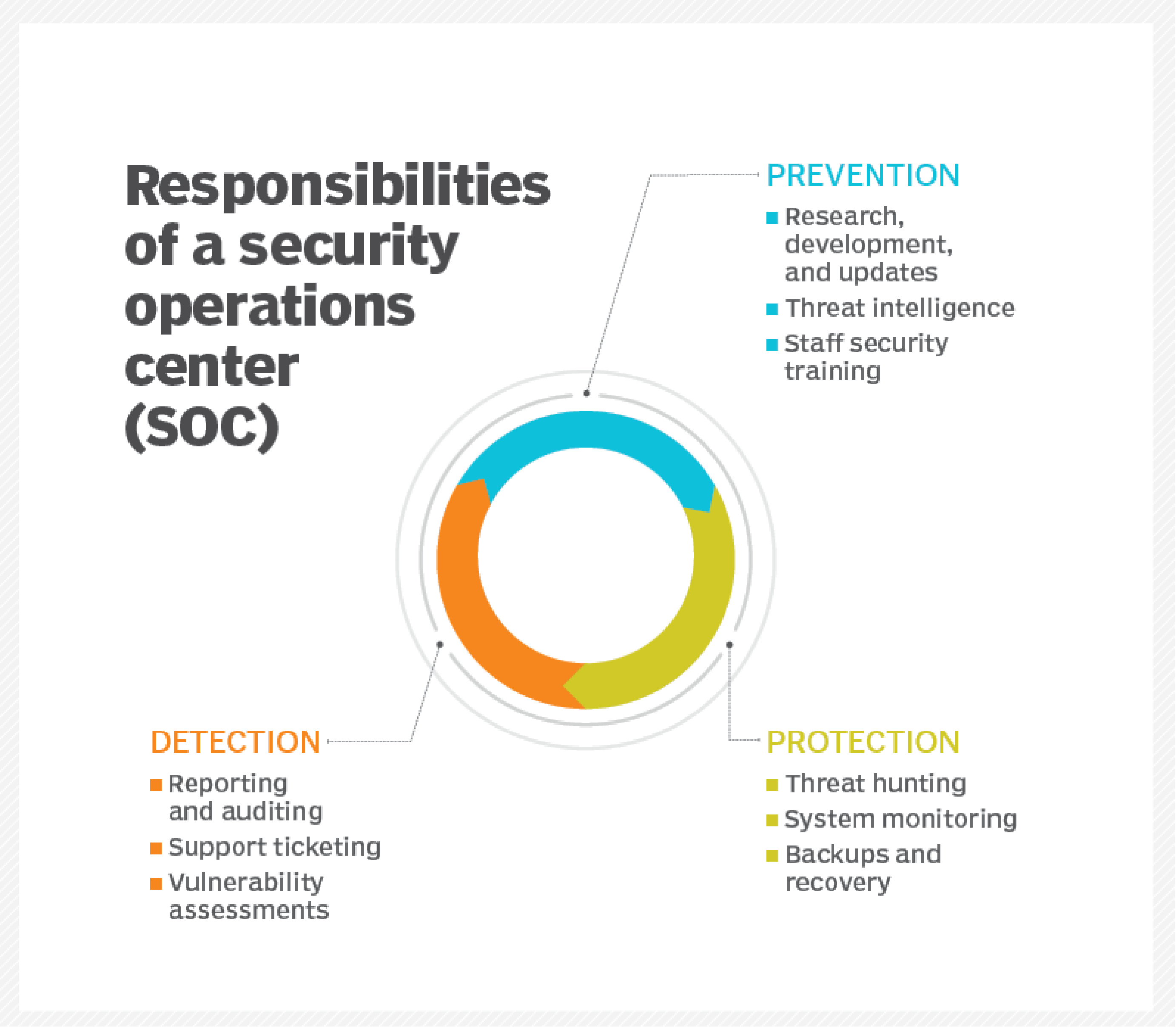
What does a security operations center do?

The overarching strategy of a security operations center revolves around threat management, which includes collecting data and analyzing that data for suspicious activity in order to make the entire organization more secure. Raw data monitored by SOC teams is securityrelevant and is collected from firewalls, threat intel, intrusion prevention and detection systems (IPSes/IDSes), probes, and security information and event management (SIEM) systems. Alerts are created to immediately communicate to team members if any of the data is abnormal or displays indicators of compromise (IOCs).

The basic responsibilities of a SOC team include the following:

- **Asset discovery and management** involves obtaining a high awareness of all tools, software, hardware and technologies used within the organization. These also focus on ensuring all assets are working properly and regularly patched and updated.
- **Continuous behavioral monitoring** incudes examining all systems 24/7 year-round. This enables SOCs to place equal weight on reactive and proactive measures as any irregularity in activity is instantly detected. Behavioral models train data collection systems on what activities are suspicious and can be used to adjust information that might register as false positives.
- **Keeping activity logs** enables SOC team members to backtrack or pinpoint previous actions that may have resulted in a breach. All communications and activity across an organization should be logged by the SOC.
- **Alert severity ranking** helps teams ensure the most severe or pressing alerts are handled first. Teams must regularly rank cybersecurity threats in terms of potential damage.
- **Defense development and evolution** is important to help SOC teams stay up to date. Teams should create an incident response plan (IRP) to defend systems against new and old attacks. Teams must also adjust the plan as necessary when new information is obtained.
- **Incident recovery** enables an organization to recover compromised data. This includes reconfiguring, updating or backing up systems.
- **Compliance maintenance** is key to ensuring SOC team members and the company follow regulatory and organizational standards when carrying out business plans. Typically, one team member oversees educating and enforcing compliance.

Additional SOC capabilities could include reverse engineering, forensic analysis, network telemetry and cryptanalysis based on the specific organization's needs.

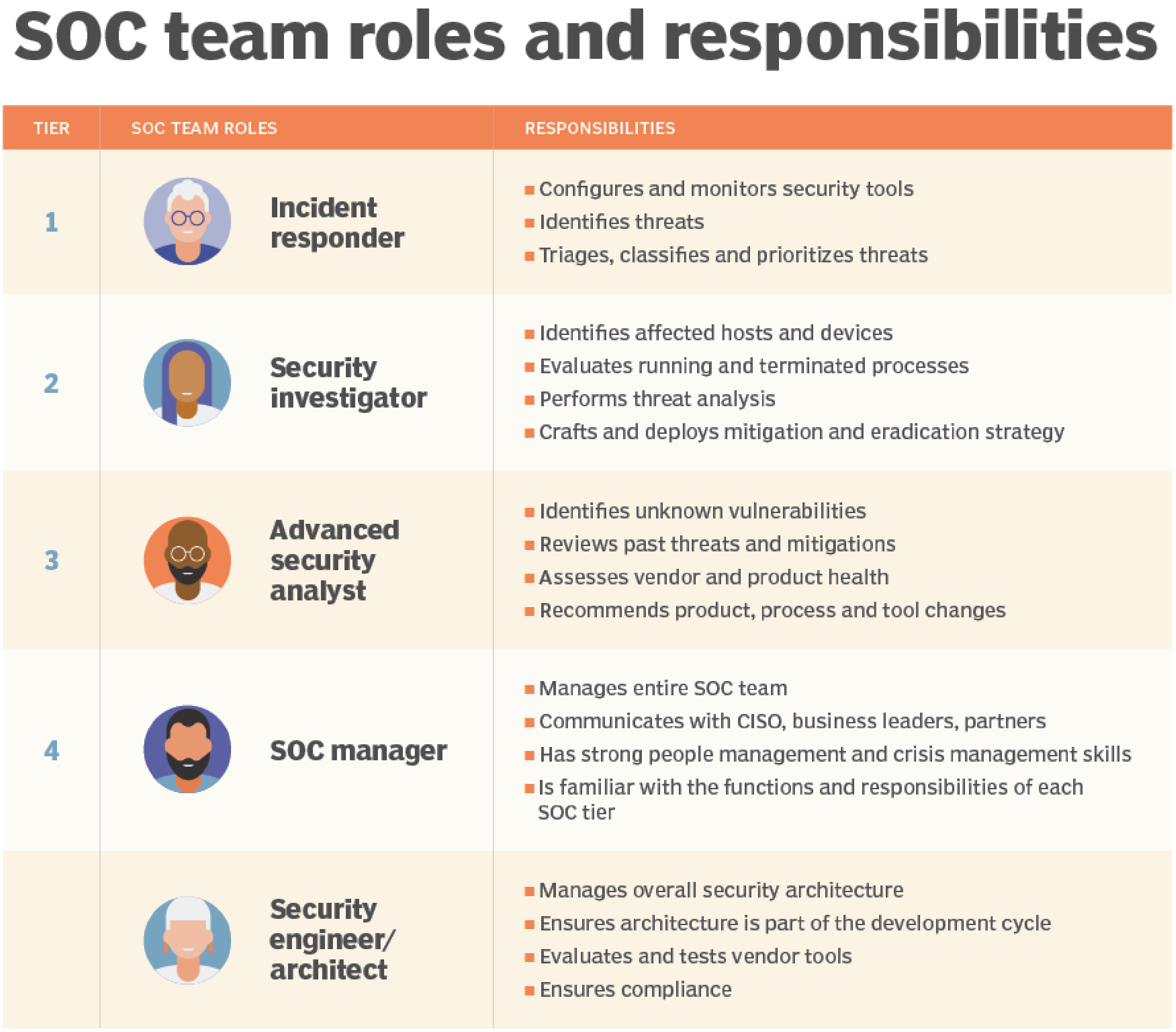


Building a winning SOC team

SOCs are staffed with a variety of individuals that play a role in overarching security operations. Job titles and responsibilities that may be found in a SOC include the following:

- A **SOC manager** is the employee responsible for managing the everyday operations of the SOC and its cybersecurity team. It is also a part of the SOC manager's role to communicate updates with the organization's executive staff.
- An **incident responder** handles successful attacks or breaches, implementing the practices necessary to reduce and remove the threat.
- The **forensic investigator** is in charge of identifying the root cause and locating the source of all attacks, collecting any supporting evidence that is available.
- A **compliance auditor** ensures all SOC processes and employee actions meet compliance requirements.

- A **SOC security analyst** reviews and organizes security alerts by urgency or severity and runs regular vulnerability assessments. A SOC analyst maintains skills such as knowledge of programming languages, systems administrator (sys admin) capabilities and security best practices.
- A **threat hunter** reviews data collected by the SOC to identify hard-to-detect threats. Resilience and penetration testing (pen testing) may also be a part of the threat hunter's routine schedule.
- A **security engineer** develops and designs systems or tools that are necessary to carry out effective intrusion detection and vulnerability management capabilities.



SOC team roles and responsibilities

TIER	SOC TEAM ROLES	RESPONSIBILITIES
1	Incident responder	■ Configures and monitors security tools ■ Identifies threats ■ Triages, classifies and prioritizes threats
2	Security investigator	■ Identifies affected hosts and devices ■ Evaluates running and terminated processes ■ Performs threat analysis ■ Crafts and deploys mitigation and eradication strategy
3	Advanced security analyst	■ Identifies unknown vulnerabilities ■ Reviews past threats and mitigations ■ Assesses vendor and product health ■ Recommends product, process and tool changes
4	SOC manager	■ Manages entire SOC team ■ Communicates with CISO, business leaders, partners ■ Has strong people management and crisis management skills ■ Is familiar with the functions and responsibilities of each SOC tier
	Security engineer/ architect	■ Manages overall security architecture ■ Ensures architecture is part of the development cycle ■ Evaluates and tests vendor tools ■ Ensures compliance

Types of security operations centers

In addition to deciding which job roles are included on the team, there are several SOC models an organization can implement. These include the following:

- **Dedicated or self-managed SOC.** This model has an on-premises facility with in-house staff.
- **Distributed SOC.** Also known as a *co-managed SOC*, this model has semi-dedicated full-time or part-time team members who are hired in-house to work alongside a third-party managed security service provider (MSSP).
- **Managed SOC.** This model has MSSPs providing all SOC services to an enterprise. Managed detection and response (MDR) partners are another form of a managed SOC.
- **Command SOC.** This model provides threat intelligence insights and security expertise to other, typically dedicated, security operations centers. A command SOC is not involved in the actual security operations or processes, just the intelligence side.
- **Fusion center.** This model oversees any security-focused facility or initiative, including other types of SOCs or IT departments. Fusion centers are considered advanced SOCs and work with other enterprise teams, such as IT operations, DevOps and product development.
- **Multifunction SOC.** This model has a dedicated facility and in-house staff, but its roles and responsibilities extend to other critical areas of IT management, such as the network operations centers (NOCs).
- **Virtual SOC.** This model does not have a dedicated on-premises facility. A virtual SOC can be enterprise-run or fully managed. An enterprise-run SOC is generally staffed by in-house employees or a mix of in-house, on-demand and cloud-provided employees. A fully managed virtual SOC, also known as an *outsourced SOC* or *SOC as a service* (SOCaaS), has no in-house staff.
- **SOCaaS.** This subscription-based or software-based model outsources some or all SOC functions to a cloud provider.

Security operations center best practices

There are several agreed-upon best practices for running a SOC. Before a SOC can be successful, it is important to select the SOC model that is most effective for the given organization, staff the team with the best security specialists, and adopt the proper tools and technologies.

Next, implement security orchestration, automation and response (SOAR) processes whenever possible. Combining the productivity of an automation tool with the technical skills of an analyst helps improve efficiency and incident response times. It also enables the SOC function more effectively without interruption.

SOCs rely heavily on the knowledge of individual cybersecurity team members. Managers should provide ongoing training to stay on top of emerging threats, cybersecurity incident reports and vulnerabilities. SOC monitoring tools should be updated to reflect any changes.

A SOC is only as effective as the strategies it has in place. Managers should implement operational protocols that are strong enough to ensure a consistent, fast and effective response.

Other SOC best practices include ensuring full visibility across a business, collecting as much data as possible as often as possible, taking advantage of data analytics and developing processes that are easier to scale for growth.

Benefits of a security operations center

When implemented correctly, a security operations center can provide an organization with numerous benefits, including the following:

- uninterrupted monitoring and analysis for suspicious activity;
- improved incident response times and practices;
- decreased gaps between time of compromise and mean time to detect (MTTD);
- centralized software and hardware assets for a more holistic security approach;
- effective communication and collaboration;
- minimized costs associated with cybersecurity incidents;
- customers and employees who feel more comfortable sharing sensitive information;
- more transparency and control over security operations; and
- established chain of control for data, which is needed if an organization is expected to prosecute those attributed to a cybercrime.

Network operations center vs. security operations center

A NOC is similar to a SOC in that its basic responsibilities are to identify, investigate, rank and fix issues. NOCs function with a NOC manager, or shift team lead, who oversees all employees and processes within the center. Most NOC employees are network or traffic engineers, some of whom may have more specialized or technical backgrounds to cover a diverse range of incidents.

Unlike in a SOC, a NOC team handles only issues that arise in relation to network performance and availability. This includes implementing processes for network monitoring, device malfunctions and network configuration. A NOC is also in charge of ensuring the network meets service-level agreement (SLA) requirements, such as minimum downtime.

A major difference in the type of incidents that SOCs and NOCs respond to is their nature. Network issues are typically naturally occurring system events, such as a malfunction or traffic overload. Security issues are more intelligent and may come from sources outside the organization's control. Due to this, NOCs cover hardware and physical equipment repairs more regularly as most SOC cybersecurity incidents happen virtually.

NOCs are common in organizations that require high network availability, such as universities and government agencies. A NOC could also be useful for organizations that rely on website accessibility and a strong internet connection, such as an e-commerce business. A security operations center may include a NOC if it follows the multifunction SOC model.