

SOC

A Security Operations Center (SOC) is a team responsible for protecting an organization from cyber threats and improving its cybersecurity posture.

The team can be **in-house or outsourced** and continuously monitors things like user accounts, computers, servers, networks, and websites to catch threats in real time.

Their main goal is to **detect, respond, and recover** from cyberattacks.

Detect

SOC teams must spot hidden threats before they cause harm. This can mean responding to alerts about suspicious activity or actively searching for unusual behavior in system logs.

Respond

When a threat is detected, the team quickly investigates to confirm if it's a real attack or a false alarm. If it's real, they determine the attack's scope and goal.

Recover

The priority for a SOC team is to keep operational services secure and running smoothly. After an attack, the team works to restore systems and prevent future incidents.

SOC teams also stay ahead of hackers by studying **new cyber threats and fixing weaknesses before they can be exploited**. Most SOC's operate 24/7, and large companies with locations around the world may have a Global SOC (GSOC)

Asset and tool inventory







To effectively defend the organization, the SOC needs a clear view of the assets it's protecting and the tools it's using. This includes tracking everything from databases and cloud services to endpoints and applications, ensuring no gaps in coverage. The team also monitors security solutions like firewalls and anti-malware tools.

Log management

The SOC collects and examines log data from every system and device within the organization to track normal behavior and spot any abnormalities that could signal a threat, like malware or ransomware.

Threat detection

SOC teams rely on SIEM and XDR data to find real threats. They sort through the noise to identify actual issues, then prioritize the threats based on how serious they are and how much damage they could cause.

<p>Phishing: Cybercriminals trick individuals into revealing sensitive information by posing as legitimate entities through emails, messages, or fake websites.</p> 	<p>Malware: Malicious software, including viruses, ransomware, and spyware, is designed to damage or gain unauthorized access to systems.</p> 	<p>Ransomware: A type of malware that locks or encrypts data until a ransom is paid, often disrupting entire organizations.</p> 
<p>Insider threats: Employees, contractors, or business partners with access to an organization's systems can pose risks—either intentionally or unintentionally.</p> 	<p>DDoS (Distributed Denial-of-Service) attacks: Attackers overwhelm a network, server, or website with excessive traffic, causing slowdowns or crashes.</p> 	<p>Data exfiltration: Cybercriminals steal sensitive data from an organization to sell it, exploit it, or use it for identity theft or corporate espionage.</p> 

}	Firewall	This tool monitors traffic to and from the network, allowing or blocking traffic based on security rules defined by the SOC.
}	Log management	This solution collects and organizes alerts from all security tools and network devices, offering a clear view of all activity within the system.
}	Vulnerability management	This tool scans the organization's systems and network for weaknesses that could be exploited by attackers.
}	User and entity behavior analytics	This technology uses AI to analyze data collected from various devices to establish a baseline of normal activity for every user and entity. When an event deviates from the baseline, it's flagged for further analysis.

Security Information and Event Management (SIEM)	This solution aggregates data from multiple security systems and log files, helping teams detect evolving threats and respond quickly. Using AI and threat intelligence, it allows SOC's to streamline incident response and stay ahead of potential attacks.
Security Orchestration, Automation, and Response (SOAR)	This platform automates recurring and predictable enrichment, response, and remediation tasks, freeing up time and resources for more in-depth investigation and hunting.
Extended Detection and Response (XDR)	This solution integrates data from multiple security products, providing a comprehensive approach to threat detection and response. It offers visibility across endpoints, servers, cloud environments, and emails, while automating responses to security

The importance of a SIEM

Without a SIEM, it would be extremely difficult for a SOC to achieve its mission. A modern SIEM offers:

-

Log aggregation: A SIEM collects the log data and correlates alerts, which analysts use for threat detection and hunting.

-

Context: Because an SIEM collects data across all the technology in an organization, it helps connect the dots between individual incidents to identify sophisticated attacks.

-

Fewer alerts: Using analytics and AI to correlate alerts and identify the most serious events, a SIEM cuts down on the number of incidents people need to review and analyze.

-

Automated response: Built-in rules allow SIEMs to identify probable threats and block them without the interaction of people.

