SOC Definition & Fundamentals

What Is A SOC?

A Security Operations Center (SOC) is an essential facility that houses a team of information security experts responsible for continuously monitoring and evaluating an organization's security status. The main objective of a SOC team is to identify, examine, and address cybersecurity incidents by employing a mix of technology solutions and a comprehensive set of procedures.

The SOC team usually consists of proficient security analysts, engineers, and managers overseeing security operations. They collaborate closely with organizational incident response teams to guarantee security concerns are promptly detected and resolved.

Various technology solutions, such as Security Information and Event Management (SIEM) systems, Intrusion Detection and Prevention Systems (IDS/IPS), and Endpoint Detection and Response (EDR) tools, are utilized by the SOC team to monitor and identify security threats. They also make use of threat intelligence and engage in threat hunting initiatives to proactively detect potential threats and vulnerabilities.

Besides employing technology solutions, the SOC team follows a series of well-defined processes for addressing security incidents. These processes encompass incident triage, containment, elimination, and recovery. The SOC team cooperates closely with the incident response team to ensure proper handling of security incidents, safeguarding the organization's security stance.

In summary, a SOC is a vital element of an organization's cybersecurity approach. It offers continuous monitoring and response capabilities, enabling organizations to promptly detect and address security incidents, minimizing the consequences of a security breach and decreasing the likelihood of future attacks.

How Does A SOC Work?

The primary function of the SOC team is to manage the ongoing operational aspect of enterprise information security rather than concentrating on the development of security strategies, designing security architecture, or implementing protective measures.

The SOC team mainly consists of security analysts who work collectively to detect, assess, respond to, report on, and prevent cybersecurity incidents.

Besides the primary responsibilities of a SOC team, some SOCs may possess advanced capabilities like forensic analysis and malware analysis. These abilities enable the SOC team to conduct in-depth investigations of security incidents and examine the root cause of the incident to avert future attacks.

As previously mentioned, the SOC team also collaborates closely with the incident response team to guarantee proper handling of security incidents and the preservation of the organization's security posture.

Roles Within A SOC

A SOC team consists of diverse roles responsible for handling the continuous, operational aspect of enterprise information security. These roles may encompass:

- `SOC Director`: Responsible for overall management and strategic planning of the SOC, including budgeting, staffing, and alignment with organizational security objectives.
- `SOC Manager`: Oversees day-to-day operations, manages the team, coordinates incident response efforts, and ensures smooth collaboration with other departments.
- `Tier 1 Analyst`: Monitors security alerts and events, triages potential incidents, and escalates them to higher tiers for further investigation.
- `Tier 2 Analyst`: Performs in-depth analysis of escalated incidents, identifies patterns and trends, and develops mitigation strategies to address security threats.
- `Tier 3 Analyst`: Provides advanced expertise in handling complex security incidents, conducts threat hunting activities, and collaborates with other teams to improve the organization's security posture.
- `Detection Engineer`: A Detection Engineer is responsible for developing, implementing, and maintaining

? Go to Questions

Table of Contents

SIEM & SOC Fundamentals

SIEM Definition & Fundamentals

Introduction To The Elastic Stack

SOC Definition & Fundamentals

MITRE ATT&CK & Security Operations

SIEM Use Case Development

SIEM Visualization Development

SIEM Visualization Example 1: Failed Logon Attempts (All Users)

SIEM Visualization Example 2: Failed Logon Attempts (Disabled Users)

SIEM Visualization Example 3: Successful RDP Logon Related To Service Accounts

SIEM Visualization Example 4: Users Added Or Removed From A Local Group (Within A Specific Timeframe)

Alert Triaging

The Triaging Process

Skills Assessment

Skills Assessment

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

- `Detection Engineer`: A Detection Engineer is responsible for developing, implementing, and maintaining detection rules and signatures for security monitoring tools, such as SIEM, IDS/IPS, and EDR solutions. They work closely with security analysts to identify gaps in detection coverage and continuously improve the organization's ability to detect and respond to threats.
- `Incident Responder`: Takes charge of active security incidents, carries out in-depth digital forensics and containment and remediation efforts, and collaborates with other teams to restore affected systems and prevent future occurrences.
- `Threat Intelligence Analyst`: Gathers, analyzes, and disseminates threat intelligence data to help SOC team members better understand the threat landscape and proactively defend against emerging risks.
- `Security Engineer`: Develops, deploys, and maintains security tools, technologies, and infrastructure, and provides technical expertise to the SOC team.
- `Compliance and Governance Specialist`: Ensures that the organization's security practices and processes adhere to relevant industry standards, regulations, and best practices, and assists with audit and reporting requirements.
- `Security Awareness and Training Coordinator`: Develops and implements security training and awareness programs to educate employees about cybersecurity best practices and promote a culture of security within the organization.

It is important to note that the specific roles and responsibilities within each tier can vary depending on the organization's size, industry, and specific security requirements.

In general, the tiered structure can be described as follows:

- `Tier 1 Analysts`: Also known as "first responders," these analysts monitor security events and alerts, perform initial triage, and escalate potential incidents to higher tiers for further investigation. Their main goal is to quickly identify and prioritize security incidents.
- `Tier 2 Analysts`: These analysts are more experienced and perform deeper analysis of escalated incidents. They identify patterns and trends, develop mitigation strategies, and sometimes assist in incident response efforts. They may also be responsible for tuning security monitoring tools to reduce false positives and improve detection capabilities.
- `Tier 3 Analysts`: Often considered the most experienced and knowledgeable analysts on the team, Tier 3 analysts handle the most complex and high-profile security incidents. They may also engage in proactive threat hunting, develop advanced detection and prevention strategies, and collaborate with other teams to improve the organization's overall security posture.

SOC Stages

Security Operations Centers (SOCs) have evolved significantly from their early days as Network Operation Centers focused primarily on network security. In the first generation, known as SOC 1.0, organizations invested in certain security layers such as security intelligence platforms or identity management systems. However, the lack of proper integration led to uncorrelated alerts and a buildup of tasks across multiple platforms. This stage was characterized by an emphasis on network and perimeter security, even as threats began exploiting other vectors. Surprisingly, some organizations continue to rely on this outdated approach, seemingly waiting for a major breach to occur.

The emergence of sophisticated threats, including multi-vector, persistent, and asynchronous attacks with concealed indicators of compromise, has spurred the transition to SOC 2.0. Malware, including mobile variants, and botnets serve as the primary delivery methods for these attacks. The longevity, evolving behavior, and growth of botnets over time have become focal points for threat intelligence. SOC 2.0 is built on intelligence, integrating security telemetry, threat intelligence, network flow analysis, and other anomaly detection techniques. Additionally, layer-7 analysis is employed at this stage to identify low and slow attacks and other hidden threats. A forward-looking approach to threat research and collaboration between SOCs, either within sectors or at the national level, is crucial for SOC 2.0's success. Emphasis is placed on complete situational awareness, pre-event preparedness through vulnerability management, configuration management, and dynamic risk management, as well as post-event analysis and learning through incident response and in-depth forensics. Refining security intelligence rules and deploying countermeasures are also vital in this stage.

The cognitive SOC, or next-generation SOC, seeks to address the remaining shortcomings of SOC 2.0. While SOC 2.0 has all the essential subsystems, it often lacks operational experience and effective collaboration between business and security teams to create rules that detect threats specific to business processes and systems. Moreover, many organizations still lack standardized incident response and recovery procedures.

Cognitive SOCs aim to resolve these issues by incorporating learning systems that compensate for experience

gaps in security decision-making. While the success rate of this approach may not be perfect in every instance, it is expected to improve over time.

Reference: https://www.linkedin.com/pulse/evolution-security-operations-center-20-beyond-krishnan-jagannathan/

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

+ 0 True or false? SOC 2.0 follows a proactive defense approach.

True

Submit

Previous Next

Mark Complete & Next