What Is ***SOC*** ( ***Security Operations Center*** ) ?

Although the staff size of SOC teams vary depending on the size of the organization and the industry, most have roughly the same roles and responsibilities. A SOC is a centralized function within an organization that employs people, processes, and technology to continuously monitor and improve an organization’s security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

* **Prevention and detection:**When it comes to cybersecurity, prevention is always going to be more effective than reaction. Rather than responding to threats as they happen, a SOC works to monitor the network around-the-clock. By doing so, the SOC team can detect malicious activities and prevent them before they can cause any damage.  
  When the SOC analyst see something suspicious, they gather as much information as they can for a deeper investigation.
* **Investigation:**During the investigation stage, the SOC analyst analyzes the suspicious activity to determine the nature of a threat and the extent to which it has penetrated the infrastructure. The security analyst views the organization’s network and operations from the perspective of an attacker, looking for key indicators and areas of exposure before they are exploited.  
  The analyst identifies and performs a triage on the various types of security incidents by understanding how attacks unfold, and how to effectively respond before they get out of hand. The SOC analyst combines information about the organization’s network with the latest global threat intelligence that include specifics on attacker tools, techniques, and trends to perform an effective triage.
* **Response:**After the investigation, the SOC team then coordinates a response to remediate the issue. As soon as an incident is confirmed, the SOC acts as first responder, performing actions that such as isolating endpoints, terminating harmful processes, preventing them from executing, deleting files, and more.  
  In the aftermath of an incident, the SOC works to restore systems and recover any lost or compromised data. This may include wiping and restarting endpoints, reconfiguring systems or, in the case of [ransomware attacks](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-ransomware/), deploying viable backups in order to circumvent the ransomware. When successful, this step will return the network to the state it was in prior to the incident.

SOC Challenges

SOC teams must constantly stay one-step ahead of attackers. In recent years, this has become more and more difficult. The following are the top three challenges that every SOC team faces:

* **Shortage of cybersecurity skills:**Based on a survey by Dimensional Research, 53% of SOCs are having difficulties hiring skilled personnel. This means that many SOC teams are understaffed and lack the advanced skills necessary to identify and respond to threats in a timely and effective manner. The (ISC)² Workforce Study estimated that the cybersecurity workforce needs to grow by 145% to close skills gap and better defend organizations worldwide.
* **Too many alerts:**As organizations add new tools for threat detection, the volume of security alerts grows continually. With security teams today already inundated with work, the overwhelming number of threat alerts can cause threat fatigue. In addition, many of these alerts do not provide sufficient intelligence, context to investigate, or are false positives. False positives not only drain time and resources, but can also distract teams from real incidents.
* **Operational Overhead:**Many organizations use an assortment of disconnected security tools. This means that security personnel must translate security alerts and policies between environments, leading to costly, complex, and inefficient security operations.

Addressing SOC Challenges

For many Security Operations Center (SOC) teams, finding malicious activity inside the network is like finding a needle in a haystack. They are often forced to piece together information from multiple monitoring solutions and navigate through tens of thousands of daily alerts. The results: critical attacks are missed until it’s too late.

Designed to address SOC challenges, Check Point [Horizon](https://www.checkpoint.com/horizon/) enables security teams to expose, investigate, and shut down attacks faster, and with 99.9% precision. Easily deployed as a unified cloud-based platform, it increases security operations efficiency and ROI.

Horizon SOC goes beyond [XDR](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-xdr-extended-detection-and-response/) with AI-based incident analysis augmented by the world’s most powerful threat intelligence and extended threat visibility, both inside and outside your enterprise. By providing easy access to exclusive threat intelligence and hunting tools it enables faster and more in-depth investigations.

**Check Point**[**Horizon**](https://www.checkpoint.com/horizon/)**helps enterprises protect their networks by delivering:**

* Unrivaled accuracy to quickly detect and shut down real attacks
* Rapid incident Investigations
* Zero-friction deployment