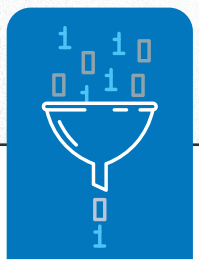
How Managed SOC Defends Against Cyberattacks

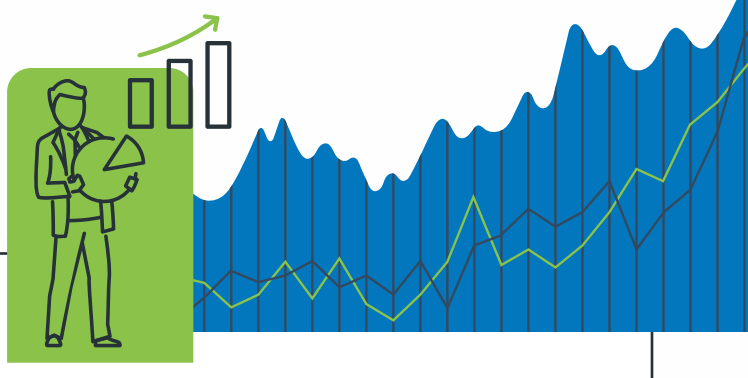
A managed security operations center (SOC) is essential for organizations of all sizes to defend against a myriad of advanced cyberthreats, such as ransomware, credential harvesting and account takeover. Also known as a managed detection and response (MDR) solution, a managed SOC detects, analyzes and responds to threats in real-time, helping organizations stop intruders in their tracks and protect critical assets. However, do you know how a managed SOC defends against advanced cyberattacks?

This infographic provides a detailed walkthrough of how a managed SOC solution effectively defends your users, applications and data against cyberthreats.



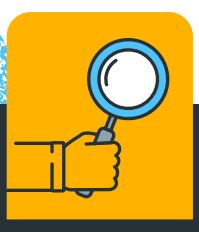
DATA COLLECTION

First, SOC analysts collect data telemetry from multiple sources, such as network devices (i.e., firewalls, intrusion prevention and detection systems, secure web gateways), cloud resources, SIEMs, AV, and endpoint logs. The more information a SOC can gather, the better it is at catching stealthy threats.



DATA ANALYSIS

As data collection occurs, SOC analysts analyze the data in real-time using a variety of advanced tools and technologies, such as artificial intelligence (AI), and experienced eyes to identify patterns and anomalies that indicate potential threats. This analysis supports various processes and tasks in the SOC, including threat and vulnerability management, advanced threat detection, incident prioritization and elimination.



THREAT ANALYSIS

Once a potential threat is detected, SOC analysts further investigate it using threat intelligence feeds and malware analysis tools to determine the severity and potential impact. They weed out any false positives by collecting additional data and analyzing it to confirm the presence of a real threat or indicator of compromise.

ALERT GENERATION

If a threat successfully penetrates an organization's defense, the SOC rapidly alerts the victim organization's incident response team and helps them triage and prioritize their response, making it faster and easier for them to take appropriate action to mitigate the threat.

RESPONSE AND REMEDIATION

The SOC experts then work hand-in-hand with the organization's cybersecurity team to develop and implement a response plan that efficiently mitigates the impact of the attack and prevents further damage. This includes disconnecting infected systems from the environment, blocking malicious content and traffic, and restoring normal operations as soon as possible.

Kaseya Managed SOC powered by RocketCyber adds an unbeatable defensive asset to your cyberdefense

Managed SOC is the ideal solution for MSPs as well as small and midsize enterprises looking to add advanced threat protection to their security stack. It uncovers suspicious and malicious activities by monitoring three critical attack vectors: endpoint, network and cloud. Managed SOC empowers MSPs and IT professionals to reduce risks while adding much-needed defense-in-depth security for today's digitally transformed businesses.

Learn more about Managed SOC