CROWDSTRIKE

SECURITY OPERATIONS CENTER (SOC) ASSESSMENT

Enhance the performance of your SOC

SECURITY OPERATIONS ARE OVERWHELMED WITH ALERTS

The sheer volume of security events, incidents and false positives means security teams are already over-extended, wading through a sea of alerts — and unable to afford the time to review their security postures and implement positive changes.

This lack of available security resources makes it a challenge to assess the current posture of SOC capabilities. When you become embedded in a daily routine of alert fatigue, it's difficult to realize the gaps that may exist. In addition, simply keeping up with the latest trends, technologies, processes and threat intelligence becomes a luxury that few have the time for.

ENHANCE SECURITY MONITORING AND INCIDENT RESPONSE

The CrowdStrike® Security Operations Center (SOC) Assessment helps organizations quickly understand how to mature their security monitoring and incident response capabilities and takes them to the next level.

The SOC Assessment methodology has been developed based on many years of combined SOC consultant experience, in conjunction with CrowdStrike's front-line incident response experience and threat intelligence expertise. The SOC Assessment is uniquely positioned to provide organizations with an industry-leading approach that helps define their SOC program.

KEY BENEFITS

Delivers an in-depth assessment and identifies gaps in your cybersecurity operations and incident response program

Determines how mature your organization currently is and provides guidance on achieving your desired future state of security operations

Provides a detailed, prioritized plan to reduce your organizational security risk with impactful improvements to operations

SECURITY OPERATIONS CENTER (SOC) ASSESSMENT

KEY CAPABILITIES

The SOC Assessment involves review of documentation, discussions with staff and manual review of your SOC. The output is a detailed, tailored report of the issues discovered and their impact, along with recommended steps for operational improvements.

- **Engaging workshops:** In interactive workshops, CrowdStrike experts gather information on your existing SOC operations and share best practices.
- **In-depth reporting:** You receive a detailed, tailored report based on the workshops, documentation analysis and follow-up discussions.
- **Prioritized areas for improvement:** The assessment includes a roadmap of prioritized recommendations that will strengthen and improve your SOC's ability to effectively detect and respond to cybersecurity incidents.

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services delivers Incident Response, Technical Assessments, Training, and Advisory Services that help you prepare to defend against advanced threats, respond to widespread attacks, and enhance your cybersecurity practices and controls.

We help our customers assess and enhance their cybersecurity posture, test their defenses against real-world attacks, respond to incidents, accelerate forensic investigations, and recover from a breach with speed and precision. Harnessing the power of our Security Cloud and the CrowdStrike Falcon® platform, we help you protect critical areas of enterprise risk and hunt for threats using adversary focused cyber threat intelligence to identify, track and prevent attacks from impacting your business and brand.

CrowdStrike: **We stop breaches.**

Learn more at **www.crowdstrike.com/services/**
Email: **services@crowdstrike.com**

WHY CHOOSE CROWDSTRIKE?

Expertise: CrowdStrike leverages deep expertise in security operations, incident response and forensic analysis to review your SOC capabilities.

Depth of analysis: Attention to detail with deep discovery and analysis identifies gaps and compares those gaps to known best practices for security monitoring and incident response.

Methodology and approach: The Services team's approach consists of interactive workshops that promote open dialogue, allowing CrowdStrike's experienced consultants to understand the depths of an organization's strengths and opportunities for improvement.