

CrowdStrike Falcon Next-Gen SIEM Resident Program

A resident expert works alongside your team to streamline your journey with CrowdStrike's Falcon Next-Gen SIEM

Overview

Onboard and maintain CrowdStrike Falcon® Next Gen-SIEM to replace a legacy SIEM solution without diverting personnel and resources from other important projects. CrowdStrike provides for this via a Resident Consultant embedded within your team that will help you tackle SIEM migration and management challenges and maximize your return on investment with CrowdStrike.

CrowdStrike Services offers two types of Falcon Next-Gen SIEM Residents: Engineers and Responders. A Resident Engineer is a full-time resource for implementation advice, best practice configurations and ongoing administration of the CrowdStrike Falcon® platform and its associated modules. A Resident Responder works in lockstep with your SOC and incident response (IR) teams, aiding in threat hunting activities to help you more effectively and efficiently detect and respond to cyberattacks.

The CrowdStrike Residency Program

CrowdStrike Residents bring deep functional expertise and gain detailed knowledge of your security environment to help manage the deployment and day-to-day operations of Falcon Next-Gen SIEM. With cyber threats becoming increasingly sophisticated, a dedicated expert ensures that your SIEM deployment is not only robust but also adaptive to emerging threats.

A CrowdStrike Resident can operate onsite, remotely or in a hybrid model to ensure close alignment with your team. By leveraging the power of the Falcon platform and in-depth knowledge of the latest threat intelligence, a CrowdStrike Resident can help improve your security posture to safeguard your environment and stop breaches.

CrowdStrike Residents allow your team to maintain focus on their core responsibilities while your CrowdStrike resource handles the intricacies of SIEM, SOAR and XDR operations. Residents help you quickly realize the return on your investment through expert guidance and rapid deployment.

Key benefits

Seamless legacy SIEM

migration: Hands-on expertise and guidance for a smooth transition from legacy systems, with minimal disruption for continuity in security operations

Platform adoption: Expert guidance and hands-on support, enabling the full potential of CrowdStrike Falcon Next-Gen SIEM without diverting resources from other initiatives

Comprehensive data

management: Delivery of best practices and strategies around data ingestion, standardization and pipeline health, enabling consistent and reliable data flow

Analyst enablement:

Comprehensive training and best practices implementation for SOC analysts, empowering them with advanced skills in threat hunting, incident response and security monitoring for more effective defense against cyber threats

Service features

CrowdStrike Residents can provide long-term support for your Falcon platform modules and assist your organization with detection and response efforts. The CrowdStrike Residency Program provides onsite, remote or hybrid dedicated Resident Engineers and Resident Responders that can deliver the following:

Resident Engineer

- Leads and supports the deployment, configuration and integration of the CrowdStrike Falcon Next-Gen SIEM platform in your environment
 - » Users and access controls
 - » API setup and automation
- Data onboarding and integration
 - » Onboards Falcon and third-party data sources, ensuring comprehensive mapping and coverage of your security ecosystem
 - » Inventories and categorizes all data sources for a structured approach to data ingestion
- Log management and standardization
 - » Parses and standardizes log architectures to ensure consistency and reliability in data processing
 - » Implements best practices for log retention and management, maintaining data integrity and accessibility
- Content creation
 - » Creates dashboards and detections
 - » Implements, tunes and reviews reports, dashboards, views, queries, correlation rules and scheduled searches

Resident Responder

- Assists and enables the SOC, IR and/or threat hunting teams using Falcon Next-Gen SIEM
 - » Guides SOC analysts on the effective use of the Falcon platform for daily monitoring, threat hunting and incident response
 - » Assists in setting up and fine-tuning alerting mechanisms to ensure SOC analysts are promptly and accurately notified of potential threats
 - » Provides guidance on best practices for triaging alerts, conducting investigations and managing incidents within the SIEM
- Monitors and triages alerts generated by CrowdStrike technology to advise on potential security events, incidents and breaches
- Provides advice on improving processes and procedures based on CrowdStrike's threat intelligence and knowledge of advanced threats
- Provides tuning recommendations to help improve prevention policies and decrease false positives
- Creates and provides after-action reviews, cyber defense techniques, guidance and reports on incident findings to appropriate constituencies

Outcomes

Accelerated the Time-to-Value and ROI

Streamline complex SIEM migration projects and maximize value through fully operationalized technology.

Dedicated Project Team Member

A dedicated full-time employee is assigned to your projects for the full service term, providing personalized support and guidance. We seamlessly integrate with your team, and CrowdStrike Residents have unrestricted access to CrowdStrike's support resources and expertise, along with the ability to escalate.

Flexibility

Scale up or down, and allocate Resident Consultant hours flexibly around your projects.

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 the CrowdStrike 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