

Falcon Next-Gen SIEM Services

Empower your security operations with CrowdStrike's expert Residency Services and Operational Support Services for seamless deployment, optimized performance and rapid threat response

Overview

Operationalizing, managing and responding to alerts from a cybersecurity platform can be a significant challenge for many organizations. The complexities of deployment, configuration and ongoing tuning can stretch internal resources and delay the realization of true value. CrowdStrike eliminates these obstacles with its industry-leading, cloud-native, AI-powered CrowdStrike Falcon® platform, delivering a seamless, efficient and highly scalable solution that helps your security operations stay ahead of the threat. To help you quickly realize value and ensure maximum return on investment (ROI), CrowdStrike provides the added advantage of having a dedicated Resident embedded within your team, offering hands-on expertise to navigate every phase of deployment and beyond.

CrowdStrike **Operational Support Services** is designed to accelerate the deployment and optimization of the Falcon platform for new customers. CrowdStrike's expert consultants work closely with your team to implement best-practice configurations that provide maximum protection and prevent breaches from disrupting your business. From rapid deployment to fine-tuning, they ensure that Falcon is set up to address your unique security needs, delivering more rapid time-to-value. These consultants bring deep platform expertise, assisting with the optimal configuration for threat prevention and business continuity. With CrowdStrike's Operational Support Services, you can confidently implement and maximize the full potential of your Falcon investment, achieving comprehensive security and a quick ROI.

The **CrowdStrike Residency Program** provides expert Residents who integrate deeply with your organization to manage the Falcon platform and respond to security threats. These Residents specialize in areas across the CrowdStrike portfolio, including CrowdStrike Falcon® Insight XDR endpoint protection, CrowdStrike Falcon® Cloud Security, CrowdStrike Falcon® Identity Protection, CrowdStrike Falcon® Next-Gen SIEM and more. They can work embedded onsite, remotely or in a hybrid model, ensuring alignment with your team. With extensive training and ongoing access to the latest threat intelligence, CrowdStrike Residents help enhance your security posture, safeguard your environment and prevent breaches by leveraging the full power of the Falcon platform. They collaborate with your internal teams to deliver continuous value and help your security operations stay ahead of emerging threats.

Key benefits

- Tailor the configuration and ongoing management of the Falcon platform to your environment
- Receive support to detect and respond to security threats from an embedded CrowdStrike team member with intimate knowledge of your organization
- Access expertise in one or more modules across endpoint, cloud, identity, Falcon Next-Gen SIEM, Falcon LogScale and more
- Gain rapid support with the broader CrowdStrike ecosystem to help solve your most complicated challenges

Falcon Next-Gen SIEM Services Components

Operational Support

Accelerate deployment, optimize security and maximize ROI with CrowdStrike's expert-driven Operational Support Services

Falcon Next-Gen SIEM Operational Support Services

accelerates the deployment process, delivering a best-practice configuration tailored to your specific security needs, ensuring maximum protection against threats and minimizing the risk of breaches.

Available in three tiers:

Essentials

- Up to 5 supported data sources
- Content development of 10 queries — to be used for report view, dashboards or correlation rules
- 2 built-in SOAR workflows
- Estimated project length approximately 150 hours

Advanced

- Up to 10 supported data sources
- Content development of 20 queries — to be used for report view, dashboard or correlation rules
- 4 built-in SOAR workflows
- Estimated project length approximately 225 hours

Premium

- Up to 20 supported data sources
- Content development of 30 queries — to be used for report view, dashboard or correlation rules
- 6 built-in SOAR workflows
- Estimated project length approximately 300 hours

Residency Services

Extend your team with deep functional expertise from a CrowdStrike expert to guide your deployment and daily use of Falcon Next-Gen SIEM

A **CrowdStrike Resident Technologist** provides full-time expertise for seamless integration, configuration and ongoing administration of the platform, while a **CrowdStrike Resident Responder** embeds with your security operations team to enhance threat detection and response.

Falcon Next-Gen SIEM Resident Technologist

Leads and supports the deployment, configuration and integration of the Falcon Next-Gen SIEM module:

- Manages users and access controls, API setup and automation
- Onboards Falcon and third-party data sources, ensuring comprehensive ecosystem coverage and structured data ingestion
- Standardizes log architectures for consistency, implements best practices for log retention, and maintains data integrity
- Creates dashboards and detections, and implements, tunes and reviews reports, views, queries, correlation rules and scheduled searches

Falcon Next-Gen SIEM Resident Responder

Supports SOC, incident response (IR) and threat hunting teams using Falcon Next-Gen SIEM:

- Enables SOC analysts in daily monitoring, threat hunting and incident response
- Assists in setting up and fine-tuning alerting systems for accurate threat notifications
- Guides best practices for triaging alerts, investigations and incident management
- Monitors and triages alerts, advising on potential security events and breaches
- Recommends process improvements based on CrowdStrike's threat intelligence
- Provides tuning recommendations to enhance prevention policies and reduce false positives
- Creates after-action reviews, cyber defense guidance and incident reports

Also available for self-hosted CrowdStrike® Falcon LogScale™ deployments

Additional customization options available on a time and materials basis

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: www.crowdstrike.com/services/

Email: services@crowdstrike.com

