CROWDSTRIKE

CrowdStrike Services
Data Sheet

Falcon Next-Gen SIEM Operational Support Services

Optimize your modern SIEM solution to stay ahead of advanced adversaries

Modern next-gen SIEM solutions

A modern next-gen SIEM solution can deliver improved visibility, real-time speed and scale for large data volumes, and advanced capabilities to hunt for the most sophisticated adversaries. By unifying all of your endpoint data along with third-party data, native threat intelligence, AI and workflow automation, you can reduce the time and costs associated with detecting and responding to threats.

The CrowdStrike Services team provides expert guidance when deploying and operationalizing CrowdStrike Falcon® Next-Gen SIEM, a module within the AI-native Falcon cybersecurity platform.

Operationalizing Falcon Next-Gen SIEM

Falcon Next-Gen SIEM Operational Support Services helps you accelerate the deployment of Falcon Next-Gen SIEM aligned to your prioritized use cases and the business outcomes you are looking to achieve with your detection and response solutions.

CrowdStrike consultants can educate, guide and expertly assist your organization. The CrowdStrike team will work side-by-side with you to assess your readiness for Falcon Next-Gen SIEM and assist with planning and installation, data onboarding, content customization and knowledge transfer.

Falcon Next-Gen SIEM allows organizations to make data-driven decisions and take automated actions to stop threats directly within the Falcon platform.

Key benefits

- Get expert assistance in operationalizing the Falcon Next-Gen SIEM module according to best practices
- Accelerate your timeline and achieve maximum value out of enterprise log data
- Define prioritized use cases and key business outcomes to protect your organization
- Provide actionable intelligence to analysts and responders
- Automate response actions within the Falcon platform to improve speed and lower costs

Key service features:

CrowdStrike consultants will provide the following services:

Project Management

- Conduct a project kickoff to understand customer objectives
- Help develop a high-level project plan
- Provide status updates on project activities

Data Onboarding

- Guide discovery and validation of log sources to be ingested to support use cases
- Advise on best practices for log data shipping from the source to Falcon Next-Gen SIEM
- Configure and customize built-in third-party connectors
- Assist with configuration and deployment of Falcon Log Collectors
- Customize existing parsers and build new ones to normalize data to CrowdStrike standards
- Advise on best practices to retain historical log data outside of Falcon Next-Gen SIEM

Content Customization and Use Case Development

- Provide guidance and best practices for migration of use case content from existing SIEM solutions
- Customize, create, translate and/or optimize searches, correlation rules and dashboards
- Assist with CrowdStrike Falcon® Fusion SOAR automation playbook development to build alerts and responses

Knowledge Transfer

- Share relevant knowledge via working sessions throughout the duration of the project
- Provide customized documentation created during the engagement

Why choose CrowdStrike?

Expert assistance:

CrowdStrike Services helps with ingesting third-party data into the Falcon platform

Customized guidance:

CrowdStrike consultants have deep understanding of Falcon Next-Gen SIEM best practices to accelerate your implementation

Use case implementation:

CrowdStrike Services provides expert guidance on detecting and responding to threats with Falcon Next-Gen SIEM

About CrowdStrike

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

We help our customers assess and enhance their cybersecurity posture, implement technologies, test 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: https://www.crowdstrike.com/services/

Email: services@crowdstrike.com