GUIDEPOINT® SECURITY

Speed Threat Detection and Response to Stop Breaches Faster

Traditional SIEM solutions are complex, costly, and challenging to arrive at actionable insights. Meaningful threats are often overlooked.

Enhance threat detection, respond faster, and improve your security posture with the next-gen SIEM solution from CrowdStrike, deployed and optimized by GuidePoint Security. Together, we offer cutting-edge solutions and cybersecurity expertise to help mitigate risk, empower innovation, and help customers stay ahead of rapidly evolving cyber threats.

## Unlock the Full Potential of Your CrowdStrike Investments

Digitization, cloud computing, big data, and remote work models require visibility beyond traditional perimeters and need automation to speed threat detection, correlation, and response across various environments, including cloud, on-premises, and hybrid infrastructures.

CrowdStrike and GuidePoint Security have a powerful partnership dedicated to giving organizations what they need most: deeper visibility across all systems to more effectively address a broader spectrum of threats.

GuidePoint engineers are highly certified on the CrowdStrike Falcon® platform and product modules to help our customers realize superior protection, better performance, reduced complexity, and immediate time-to-value. Importantly, our experienced team will help you bridge the gap between security technologies and security operations.

GuidePoint can help with implementation, custom integrations, and tuning your CrowdStrike Falcon® Next-Gen SIEM solutions so you can make better, more informed cybersecurity decisions and minimize risk. We help by:

- ✓ Maturing your CrowdStrike deployment architecture
- ✓ Operationalizing Falcon Next-Gen SIEM and maximizing value
- ✓ Ensuring all CrowdStrike modules are properly implemented and fully utilized
- ✓ Automating contextualization, enrichment, and response to help analysts achieve faster MTTR (mean time to resolution)
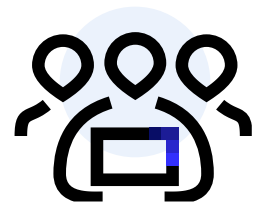
Put a Highly-Trained, ELITE Team on Your Side

Your organization will be backed by our team of cybersecurity engineers, architects and consultants who are veteran practitioners from Fortune 100 companies, the U.S. Department of Defense and U.S. intelligence agencies.

Hundreds of Industry and Product Certifications

Optimize Performance, Maximize Results

GuidePoint's highly skilled and certified technical experts can quickly evaluate, deploy, and optimize the CrowdStrike Falcon platform and product modules to solve real problems for our customers, including:

Falcon Console

Our engineers are well-versed in maximizing the cost-effectiveness and maturity of the CrowdStrike Falcon console. We have the capability to design and implement a data analytics architecture that will marry native Falcon telemetry data with third-party sources for faster detection, better data quality, and improved automated response.

Falcon Next-Gen SIEM

GuidePoint will help you operationalize the Falcon console and Falcon Next-Gen SIEM by delivering upon an extensive set of use cases tailored to quickly and effectively ramp up utilization of the CrowdStrike platform in its entirety, from the CrowdStrike Falcon® Identity Protection module to CrowdStrike Falcon® Fusion SOAR automated workflows. We can help operationalize CrowdStrike by maximizing the effectiveness of first- and third-party data by:

- ⊘ Onboarding data from third-party sources, whether it is a scripted collection, or a monitored input
- ⊘ Designing, deploying, and managing fleets of Falcon Log Collectors
- ⊘ Developing detections, dashboards, queries, and reports in Falcon Next-Gen SIEM
- ⊘ Designing workflows in Falcon Fusion SOAR
- ⊘ Implementing Falcon sensor policies

CrowdStrike Modules

Our professionals will conduct a thorough health check of your CrowdStrike implementation to perform a baseline and identify areas for improvements. GuidePoint's objective will be ensuring the maximum value is extracted from the modules purchased.

Falcon Fusion SOAR Automated Workflows

Designing, defining, and developing automations to assist in investigation may seem daunting. GuidePoint engineers with years of analytics and automation experience can help you embrace automation, at whatever speed suits your organization. Our team can help with your automation efforts by:

- ⊘ Conducting use case sessions to gather and define requirements
- ⊘ Iteratively developing automations that will reduce MTTR
- ⊘ Building workflows and custom integrations within Falcon Fusion SOAR

About CrowdStrike

CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

About Us

GuidePoint Security provides trusted cybersecurity expertise, solutions, and services to help organizations make better decisions that minimize risk. GuidePoint's unmatched expertise has enabled a third of Fortune 500 companies and more than half of the U.S. government cabinet-level agencies to improve their security posture and reduce risk.

GUIDEPOINT®
SECURITY