PRESIDIO®

SOLUTIONS BRIEF

Cyber Security

CrowdStrike Falcon NG SIEM Implementation Services

THE CHALLENGE

SOC teams are trapped between legacy SIEMs and half-implemented next-gen platforms. They connect data but drown in noise, shallow use cases, and broken automation. CrowdStrike Falcon NG SIEM is powerful, but without an expert-led deployment to design ingest, tuning, detection rules, and workflows, organizations burn through budget on a modern SIEM that still behaves like a slow, costly log search tool and never delivers the promised ROI.

Accelerate detection, cut SIEM costs, modernize your SOC.

THE SOLUTION

Presidio's CrowdStrike Falcon NG SIEM Implementation Services are engineered to make Falcon NG SIEM fully operational, not just installed. We start by identifying and onboarding the right data sources to support your highest priority use cases, then design and tune detection content for your specific environment and risk profile. From there, we map your SOC processes into Falcon – including triage, investigation, escalation, and response – and implement automation where it delivers the greatest impact, such as enrichment, correlation, and common remediation actions. Throughout the engagement, we focus on measurable outcomes: reduced alert noise, faster investigations, stronger correlation fidelity, and lower data ingestion costs. We work side by side with your SOC team so they can own, extend, and maintain what we build after go-live. The result is not a generic deployment, but a Falcon NG SIEM environment that operates as a modern, threat-driven analytics platform rather than a legacy log search tool, and is explicitly engineered around your threats, your processes, and your SOC metrics.

THE APPROACH

Presidio delivers a prescriptive, outcome-driven implementation of CrowdStrike Falcon NG SIEM focused solely on making your SOC better, not just turning the platform on. We onboard high-value telemetry, design and tune detections, unify data, and embed targeted automation directly into your investigation workflows. Analysts get opinionated playbooks and guided triage in Falcon, while leadership gets measurable improvements in noise reduction, investigation speed, and response quality aligned to clearly defined SOC outcomes.

PRESIDIO

CrowdStrike Falcon NG SIEM Implementation Services

KEY BENEFITS

- Faster detection and response by operationalizing Falcon NG-SIEM analytics and threat intel, improving MTTR within weeks
- Lower SIEM operating costs through optimized data ingestion, routing, and retention
- Significantly reduced alert noise and fatigue via use-case driven detections, targeted tuning, and automation
- Stronger, more consistent investigations using standardized workflows, guided triage, and automated enrichment
- A SOC that runs on threat-driven analytics instead of slow, ad hoc log searches

WHAT MAKES US DIFFERENT

- Proven, Falcon-focused NG SIEM methodology built from large-scale deployments not a generic multi-SIEM model
- Use case & threat-driven approach tied to your business risk, not just raw log source onboarding
- End-to-end engineering of correlation logic, detection content, workflows & automation, plus structured tuning cycles to improve signal-to-noise and analyst efficiency
- Deep expertise in Falcon telemetry, NG SIEM content, native analytics, and cross-platform integrations across endpoint, network, identity, and cloud to reduce time to value
- SOC enablement and maturity roadmap aligned to SOC KPIs (MTTR, coverage, false positives) backed by a deep bench of SecOps, automation, SASE or SSE, and cloud security specialists

WHY PRESIDIO

Presidio is here to guide your digital journey and help you navigate the fast-changing tech landscape. As the bridge between where you've been (foundational IT) and where you're going (ultra-modern AI and cloud services), we measure success in your terms. We strive to build lifetime relationships with those that give us their business, and we do so by being fearless, fast, flexible, and compassionate. It's our mission to earn your trust and deliver innovative, high-quality results at the speed your business needs to succeed.

Turn Falcon NG SIEM into a high-performance SOC engine.

Presidio helps you operationalize Falcon NG SIEM around real threats, real workflows, and real KPIs. We engineer detections, automation, and investigation workflows that reduce noise, speed response, and optimize data costs—so your SOC delivers measurable results, not just more alerts.

Contact Presidio today: www.presidio.com