

SOC Transformation Services

Modernize your SOC with expert-led design, build, and optimization services that establish agentic-ready foundations on the Falcon platform

Today's adversaries move at machine speed across identity, cloud, endpoint, and third-party systems, while many SOC's are still constrained by fragmented data, inconsistent workflows, and architectures built for a different era. The result is slower investigations, uneven response, and security programs that struggle to scale as the landscape evolves. CrowdStrike SOC Transformation Services helps enterprises modernize the SOC foundation so security operations become faster, more consistent, and continuously improving, with structural readiness for future agentic adoption when the organization chooses.

CrowdStrike SOC Transformation Services is a large-scale, expert-led program that helps enterprises design, build, and optimize a modern SOC centered on the CrowdStrike Falcon® platform. Through structured engagements, CrowdStrike delivers a proven yet tailored blueprint that unifies SIEM, data pipelines, workflows, staffing models, and governance into a high-performing SOC operating model, helping teams reduce complexity, accelerate time-to-value, and drive measurable operational outcomes.

Modernizing security operations has become an urgent priority, but the lift is heavy. Organizations must migrate off legacy stacks, redesign processes, and orchestrate new data and workflow patterns while day-to-day operations continue. SOC Transformation Services turns that high-stakes effort into a clear, phased journey with defined outcomes, guided by CrowdStrike practitioners. This reduces the risk, cost, and delay of trying to modernize without expert direction, and prepares the SOC for safe, scalable agentic workflows in the future.

Key benefits

- **Modernize and consolidate the SOC on Falcon:** Retire legacy SIEM and fragmented tools by standardizing operations on the Falcon platform, with unified telemetry and workflows that improve day-to-day speed and consistency.
- **Get to a modern, agentic-ready SOC fast:** Move from legacy to modern through an expert-led, phased journey that avoids the trial-and-error of DIY modernization, keeps operations running, and accelerates time-to-value with clear outcomes at each stage.
- **Design for real attackers, not theoretical ones:** Apply CrowdStrike's frontline incident response, red team, and threat intelligence experience to shape detections, workflows, and runbooks for how adversaries actually operate.
- **Establish the structural readiness for safe automation and future agentic workflows:** Modernize data pipelines, workflows, staffing models, and governance together so the SOC has the controls and operating conditions needed to safely adopt advanced automation and agentic workflows on your terms.

Key service components

Design your SOC of the future, build it with confidence, then optimize and continually refine it over time. CrowdStrike SOC Transformation Services follows a design–build–optimize model, turning a major SOC overhaul into a structured program with clear stages and deliverables.

Design: Clarify the Target SOC and Roadmap

In the design phase, CrowdStrike conducts a structured assessment of the existing SOC, including:

- Current SOC operating model, roles, and responsibilities
- Detection architecture, SIEM usage, and data pipelines
- Existing workflows, runbooks, and governance structures

From this, CrowdStrike defines an agentic-ready operating model and produces a phased roadmap that specifies what to modernize, what to retire, and how to sequence migration to CrowdStrike Falcon® Next-Gen SIEM and related workflows.

Build: Implement the Future-state SOC on Falcon

In the build phase, CrowdStrike experts execute the roadmap by:

- Migrating logs, detections, and workflows from legacy SIEMs to Falcon Next-Gen SIEM
- Redesigning and implementing SOC workflows, automations, and runbooks
- Aligning staffing models and operational processes to the new architecture

This work is led by consultants and embedded resident experts who tune and operationalize Falcon in the customer's environment, allowing internal teams to remain focused on day-to-day security operations while the future-state SOC is stood up.

Optimize: Validate, Refine, and Mature

Once the new SOC foundations are in place, CrowdStrike validates that they perform as intended and are ready to evolve. Activities typically include:

- Red team and blue team validation exercises to test detections, workflows, and escalation paths
- Response readiness refinement based on real-world attack simulations
- Advisory sessions to identify efficiency gains, governance improvements, and opportunities for future agentic workflows

The outcome is a clear, phased roadmap for continued SOC maturity and agentic readiness, supported by ongoing guidance from practitioners who design and run SOC at scale.

About CrowdStrike Services

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