

AI for SecOps Readiness

Operationalize AI in the SOC to boost speed, precision, and scale

AI is an essential tool for the SOC to stay ahead of modern adversaries. CrowdStrike shows you how to use it to move faster, act with precision, and fight AI with AI.

AI is transforming both sides of the cyber fight. Adversaries are using AI to scale reconnaissance, generate more convincing phishing campaigns, and automate attacks at speeds that overwhelm traditional defenses. Security teams face mounting pressure to respond faster, manage complexity, and close gaps with limited resources.

At the same time, organizations are eager to bring AI into the SOC to increase efficiency, improve accuracy, and reduce analyst workload. But most teams lack a clear roadmap for where to start, how to use AI responsibly, and how it can support their people, processes, and tooling.

CrowdStrike's AI for SecOps Readiness service solves that problem. This expert-led engagement helps security teams develop frameworks and use cases to leverage AI in their detection, investigation, and response workflows with clarity and control. Through collaborative workshops and SOC-specific guidance, customers gain a practical roadmap to reduce workload, improve response time, and strengthen the SOC with precision and speed.

Key features

What's delivered:

- **Comprehensive SOC readiness assessment** focused on AI adoption, including team structure, existing workflows, technology stack, and response processes
- **Identification and prioritization of AI use cases** mapped to your specific environment and security operations goals
- **Design guidance** to align AI initiatives with existing detection, investigation, and response tooling

Key benefits

- **Boost analyst efficiency with AI:** Understand how to use AI to accelerate detection, investigation, and response without adding noise or complexity
- **Start with the use cases that matter:** Get practical guidance on where AI fits, what to automate, and how to scale
- **Modernize the SOC with confidence:** Adopt AI in ways that are aligned with your team, tooling, and real threats

- **Evaluation of architectural requirements** for integration AI responsibly, including build-vs.-buy considerations and technical dependencies
- **Mapping of desired SOC outcomes to AI capabilities**, such as enrichment, alert triage, or response automation
- **Interactive workshops** with your SOC leaders, architects, and stakeholders to shape AI strategy, develop implementation plans, and establish governance principles
- **Risk considerations and control recommendations** to support secure AI integration into critical security workflows
- **Summary report** that includes readiness findings, prioritized AI use cases, implementation

Topics covered:

- Discovery workshops (AI people, processes, and technology)
- AI strategy development for security operations
- Use case design and implementation planning

Outcome:

Security teams receive a tailored strategy and roadmap to operationalize AI in the SOC, helping to increase speed, precision, and resilience without introducing unnecessary risk.

Learn More →

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

Why choose CrowdStrike?

CrowdStrike has assisted countless organizations in assessing cybersecurity programs to address the specific factors that matter in today's targeted threat landscape.

- **Expertise:** Unrivaled expertise and skills are drawn from deep experience with security operations, incident response (IR), endpoint recovery, and forensic analysis
- **Tailored analysis:** Detailed findings include accurate and meaningful recommendations that address your specific organization and its risks
- **Methodology and approach:** The CrowdStrike approach consists of interactive workshops that promote open dialogue and provide learning opportunities in real time