CROWDSTRIKE

CrowdStrike Services

Data Sheet

CrowdStrike AI Red Team Services

Fortify your GenAI rollout through proactive assessments and attack emulations

Increase confidence in your GenAI security posture

As global organizations increasingly adopt generative AI to drive innovation and efficiency, adversaries are evolving their tactics just as quickly to exploit these transformative technologies. AI systems, particularly those integrated with external data sources and plugins, create new attack surfaces that are highly attractive to adversaries. CrowdStrike's AI Red Team Services are specifically designed to confront these emerging threats.

CrowdStrike's industry-leading experts emulate advanced adversarial attacks, rigorously test for vulnerabilities and identify security gaps across your AI infrastructure. They uncover misconfigurations and risks that could lead to data breaches, remote code execution or system manipulation — providing you with clear, actionable insights to fortify your defenses.

As a leader at the forefront of AI-native cybersecurity, CrowdStrike empowers organizations to confidently adopt AI while staying ahead of adversaries, ensuring that your systems are resilient against even the most sophisticated threats.

AI Red Team Services components

AI Application Penetration Testing

- **Extensive testing against the Open Worldwide Application Security Project (OWASP) Top 10 for LLMs:** Ensure AI integrations are secure from vulnerabilities identified in the leading industry standards.
- **Analysis of AI integration points:** Identify weaknesses in AI plugins, data sources and other integration points.
- **Detailed, actionable reporting:** Get clear, concise insights with actionable steps to strengthen AI security defenses.

Key benefits

- **Gain security validation:** Engage in a comprehensive exercise assessing your AI environment to uncover vulnerabilities across systems.
- **Identify vulnerabilities across the GenAI stack:** Protect your AI integrations from threats like data exposure and operational impact.
- **Improve your long-term AI security posture:** Get recommendations for maintaining the resilience of your AI integrations to innovate with peace of mind.
- **Safeguard sensitive data from adversaries:** Test large language models (LLMs) and their integrations for sensitive data exposure.

Adversarial Emulation Exercise

- **Emulated adversarial tactics:** Replicate real-world attacks to expose security gaps before they can be exploited.
- **Tailored red team exercises:** Engage in customized emulations based on your specific AI infrastructure.
- **Recommendations for securing data and applications:** Learn practical steps to prevent sensitive data leakage and unauthorized access.

Red Team / Blue Team Exercise

- **Strengthened defenses:** CrowdStrike's Red Team emulates real-world attacks, while the Blue Team helps your internal team detect and respond.
- **AI-enhanced investigations:** CrowdStrike® Charlotte AI™ surfaces real-time insights and automates analysis to improve Blue Team threat identification and response.
- **Improved processes and response readiness:** Regular exercises build muscle memory and refine response processes, ensuring faster, more effective reactions to future threats.

In today's fast-evolving AI landscape, traditional safeguards fall short. Without proactive security, you risk exposing sensitive data and system vulnerabilities. CrowdStrike's AI Red Team Services prepare you to defend your AI systems against adversarial attacks before they start.

About CrowdStrike Services

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

We help our customers assess and enhance their cybersecurity posture, test their 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