AI Adversary Operations

Test Your Defenses. Prepare Your People. Advance with AI.

AI is changing the approach to enterprise security. Adversaries can use frontier AI models to accelerate reconnaissance, develop new tooling, analyze environments, and adapt operations all in service to break into an organization. At the same time, enterprise AI introduces new models, agents, identities, data, and infrastructure that expand the attack surface you need to protect.

The SpecterOps AI Adversary Operations Platform combines AI-enabled Red Teams, AI Red Team Enablement, and enterprise-scale Cyber Ranges for AI to help organizations understand these capabilities, test against them, and build the internal expertise to defend themselves.

Our approach addresses all aspects AI security: how adversaries can use AI against your organization, how your own AI systems can introduce new security risk, and how your team can use AI to accelerate defensive capability.

AI Red Teaming

Test Against the AI-Enabled Adversary

SpecterOps AI Red Teams combine offensive security expertise with emerging AI tooling and tradecraft to test how modern adversaries can operate against your organization.

We simulate AI-enabled adversary techniques against traditional enterprise environments and AI systems, including models, agentic workflows, identities, APIs, pipelines, and supporting infrastructure. Attack path analysis connects individual weaknesses to determine what an adversary can reach and how initial access can lead to broader business impact.

Engagements can span design through production, and include threat modeling, direct model assessments, penetration testing, and full red team operations run against live systems.

Test AI systems and enterprise defenses against the techniques shaping modern adversary operations.

AI Red Team Enablement

Build AI-Native Capability Across Your Team

SpecterOps AI Red Team Enablement transfers the expertise we've built to your team. Applied AI security research, AI-assisted tooling, secure red team infrastructure, practitioner-developed AI skills, and hands-on training help operators incorporate AI into modern offensive security workflows.

Dedicated red team infrastructure provides isolated, per-project environments that deploy quickly and consistently, with role-based access controls and activity logging built in. Operators spend less time managing infrastructure and more time conducting the engagement.

Teams learn how emerging AI-assisted techniques work by using them, giving security and detection practitioners practical experience they can apply to future testing and defense.

Build expertise that continues working for your organization after the engagement ends.

Cyber Ranges for AI

Evaluate Frontier Models at Enterprise Scale

SpecterOps builds enterprise-scale cyber ranges that allow organizations and AI developers to rigorously evaluate advanced models against realistic security environments.

Ranges combine interconnected enterprise technologies, known completion paths, multi-step attack paths, and extended reasoning requirements to determine whether individual model capabilities translate into meaningful outcomes at enterprise scale.

Our work evaluating frontier models also strengthens our Red Team and Enablement offerings, giving SpecterOps practitioners firsthand insight into what advanced AI systems can accomplish and how those capabilities are evolving.

Measure AI capabilities against the complexity of real enterprise environments.

The SpecterOps Difference

Adversary Expertise

Decades of offensive security operations, research, training, and tooling provide the foundation for how SpecterOps approaches AI security.

Frontier AI Experience

Our practitioners work directly with advanced cyber models and frontier AI organizations. That firsthand insight into emerging offensive capabilities and risks shapes the tradecraft we bring to engagements.

Research Turned Into Tradecraft

We translate what our researchers learn into practical techniques, tooling, training, and testing methodologies that organizations can put to work.

Capability That Lasts

SpecterOps can test your organization against AI-enabled threats while helping your people develop the expertise to continue testing and defending against them.

Comprehensive AI Adversary Readiness

The fundamentals of defense haven't changed, but the timeline has. Adversaries can compress the time an exploit takes down to hours, and security teams need to get ahead of those techniques, not just respond to them. AI Red Teaming tests your defenses. AI Red Team Enablement builds your team's capability. Cyber Ranges for AI advance the understanding of what frontier models can accomplish.

Together, they give organizations the adversary perspective, practical expertise, and frontier-model insight needed to operate securely as AI capabilities advance.

AI Red Teaming | AI Red Team Enablement | Cyber Ranges for AI

Test against what is coming. Build the capability to defend against it. Start building AI adversary readiness.

specterops.io/contact ›

SPECTEROPS ©2026 Specter Ops, Inc.