SPECTEROPS | OpenAI

DATASHEET

AI-Enhanced Red Teaming with SpecterOps and OpenAI GPT Cyber Models

Combine OpenAI GPT Cyber Models with SpecterOps' adversary expertise for authorized red team assessments.

Through OpenAI's Daybreak Defense Network, SpecterOps combines OpenAI GPT Cyber Models with its adversary tradecraft to support vulnerability research, exploit validation, and penetration testing within an authorized scope. Its operators use the models to explore attack scenarios and validate their impact during red team assessments.

Recognized for industry-leading security research, consulting services, and the adversary tradecraft behind BloodHound, SpecterOps employs teams of offensive security consultants with real-world experience protecting Fortune 100 organizations. **Our expert advisors work alongside your team to integrate OpenAI GPT Cyber Models into authorized assessment workflows, from an initial engagement to a repeatable practice.**

What a Daybreak Activation Engagement Looks Like

AI-Enhanced Red Team Assessments

SpecterOps operators use OpenAI GPT Cyber Models alongside adversary tradecraft to support authorized attack simulations. Your security operations team gains experience responding to the scenarios defined in the engagement scope. We validate real-world impact and deliver prioritized findings your team can act on.

Scoping defines the supporting evidence, remediation guidance, detection recommendations, and any retesting included in the engagement, which concludes with a formal outbrief led by SpecterOps.

Who is this option best for?
For teams that want an expert-led offensive security assessment of a defined environment, with AI integrated into assessment delivery to augment operator analysis and execution. The takeaway is a Findings Report and a prioritized remediation plan.

Operational Infrastructure for AI Red Teaming

SpecterOps designs the assessment environment and operational controls around your authorized operations. This includes dedicated infrastructure and tooling for assessment delivery, with isolated engagement environments, individual operator identities and role-based access controls, standardized deployment of approved offensive infrastructure, comprehensive command and activity logging, secure team collaboration and file storage, and integrated access to AI enabled workflows for tasks such as tool development, code analysis, and exploit generation. Environments are ephemeral and destroyed at the conclusion of each assessment.

Who is this option best for?
For teams that need infrastructure for authorized red team operations. The takeaway is access to isolated assessment environments and supporting tooling managed by SpecterOps during the engagement.

Advisory Services

As a Daybreak Red-approved partner, SpecterOps is well-positioned to help your team build a sustainable program for AI-enhanced offensive security. We identify priority use cases, integrate OpenAI GPT Cyber Models into authorized red team and detection-engineering workflows, and define measures of progress. These may include time to validate findings, confirmed attack paths closed, and detection gaps addressed.

Who is this option best for?
For teams determining where AI-assisted security fits in their program. The takeaway is a roadmap or similar deliverable with priority use cases, prerequisites, owners, and ways to measure progress.

Getting Started

SpecterOps can help teams explore AI-enhanced red team assessments, infrastructure, and advisory services. Engagements begin with a collaborative session to assess your current program, identify high-value use cases, and build a plan across assessments, infrastructure, and program maturity.

To learn more, contact your OpenAI representative. Additional questions? Drop a note:

partners@specterops.io ›

SpecterOps Services for Daybreak enable your team to:

- **Gain experience**
  responding to scoped, AI-assisted attack simulations.
- **Use AI**
  to support attack-scenario analysis and detection development alongside your red team.
- **Plan AI-assisted assessments**
  with defined use cases, prerequisites, and measures of progress for offensive security.
- **Transform offensive findings**
  into new and improved detections.
- **Operate AI-enabled testing**
  with defined access controls and activity logging.
- **Communicate outcomes**
  to stakeholders in business-relevant terms.

SpecterOps combines OpenAI GPT Cyber Models with its offensive security expertise to support authorized assessments, validate findings, and help teams prioritize remediation.

About SpecterOps

SpecterOps pioneered the concept of Attack Path Management for Identity and created BloodHound, the industry-leading platform for identity security. Our Consulting Services team has guided hundreds of organizations in building and maturing offensive and defensive security programs, and our Training courses have guided more than 10,000 info-sec students to deepen knowledge of adversary tradecraft. SpecterOps is a trusted partner for leading AI companies. Its offensive security services are leveraged by the largest enterprises and government agencies, and BloodHound has been recommended by the FVEY intelligence alliance, the U.S. Department of Homeland Security, PricewaterhouseCoopers, and many others.

SPECTEROPS ©2026 Specter Ops, Inc. OpenAI, the OpenAI logo, and Daybreak are the property of OpenAI.