SPECTEROPS
Creators of BloodHound

DATASHEET

Cyber Ranges for AI

Enterprise-Scale Cyber Ranges for AI Evaluations

From the Creators of

BLOODHOUND

MYTHIC

NEMESIS

GHOSTWRITER

Trusted by 200+

Fortune 500 and government agencies to inform the tradecraft behind every scenario

As AI models grow more sophisticated, governments and technology companies need rigorous environments to test model capabilities. Traditional testing platforms fall short, offering condensed scenarios that fail to replicate enterprise complexity or scale.

SpecterOps delivers enterprise-scale cyber ranges for AI that provide standardized evaluation environments with known completion paths combined with the realism necessary to validate AI model capabilities under production-like conditions. **Designed by leading attack path exploitation experts, our ranges deliver the complexity and scale necessary for rigorous assessment.**

AI Capability Testing at Enterprise Scale

Government agencies assess whether AI models pose national security threats by testing offensive capabilities in controlled environments, while AI companies evaluate model reasoning, ensure safe deployment, and benchmark performance relative to human completion rates.

Traditional CTF and AI evaluation platforms offer condensed scenarios that favor AI's short-term memory strengths, but real enterprise networks require long-term reasoning and complex attack chain orchestration—areas where current models struggle. **Our significantly larger cyber ranges excel at AI evaluation, providing authentic stress tests that reveal true operational capabilities under realistic constraints.**

Expert Analysis and Guidance

Organizations can leverage quantitative metrics, expert qualitative assessment, custom modifications, and our services offerings to interpret model behavior and develop comprehensive safety frameworks.

The SpecterOps Difference

Objective Evaluation by Design

A neutral, independently operated proving ground trusted by AI developers and government evaluators—with no bias toward any model architecture or vendor ecosystem.

Expert-Built Challenges

Designed by security experts who execute these attacks in real client environments; meaning every scenario represents proven attack paths from actual engagements—our “greatest hits” of enterprise compromise techniques.

Production-Like Scale and Complexity

Our cyber ranges simulate diverse technology stacks and multi-system traversal scenarios that mirror modern enterprise environments—significantly larger and more complex than traditional capture the flag (CTF) and AI evaluation providers. Built to challenge experienced security professionals—not synthetic scenarios designed for automated testing—these environments require long-term reasoning, attack chain orchestration, and lateral movement; conditions where AI limitations become measurable.

Defined Boundaries, Open Methodology

Each scenario is built with defined boundaries and known successful completion paths, enabling organizations to evaluate models against realistic enterprise compromise scenarios without sacrificing the rigor of structured assessment. Organizations can focus on specific obstacles or complete end-to-end scenarios—no prescribed methodology required.

Ready-Made and Custom Offerings

Dozens of ready-made scenarios are available for immediate deployment. For organizations requiring evaluation of specific attack paths or types of technology, we develop custom scenarios tailored to your assessment objectives.

Complete Turnkey Experience

Fully managed cyber ranges with SLA-backed hosting and the ability to deploy concurrent ranges at scales needed for AI use. Organizations focus on evaluation—not infrastructure management.

> **“We are grateful to SpecterOps for their expertise in designing and building the cyber ranges that are foundational to our research on Measuring AI Agents’ Progress on Multi-Step Cyber Attack Scenarios.”**
>
> **– AI Security Institute (AISI)**

Getting Started

Whether evaluating AI model capabilities for safety assessment or benchmarking performance, our enterprise-scale cyber ranges deliver the realism and rigor that other platforms cannot match. For organizations seeking comprehensive security programs, our ranges complement our offensive security services, program development, and training offerings. We also offer Capture the Flag Ranges that train security teams on real-world attack paths including privilege escalation, lateral movement, and cloud infrastructure compromise.

Contact us to discuss your evaluation needs at [specterops.io/contact.](specterops.io/contact)

Learn more at specterops.io/training ›