SPECTEROPS
Creators of BloodHound

SERVICES

Red Team Exercises

Evaluate and Strengthen Your Detection and Response Capabilities with an Attack Path Simulation

Why SpecterOps

SpecterOps is the organization who brought Red Team Exercises into the commercial market, not just in concept, but through widely available tooling and content used by most providers today. Tools like BloodHound, Mythic C2, and Ghostwriter are in every offensive providers' arsenal. When we say leaders in offensive security, we mean it.

Why Now

You've built (or hired) a SOC. You've bought the latest XDR. You've had a pentest. Now is the time to exercise how all of these efforts work together to detect, respond, and eradicate an attacker from your network.

A Red Team Exercise will evaluate the People, Process, and Technology that gives you confidence in your organization's ability to defend against adversaries.

Benefits

- **Exercise your organization's ability to detect and respond to realistic attacks**
- **Understand the organization's readiness to deal with a potential breach**
- **Gain a deeper understanding of adversary tradecraft and the impact of attack paths**
- **Expose potential gaps in technology, training, and processes within your security program**
- **Receive actionable results to drive immediate improvements and prioritize future resource allocation**

Prepare for the worst-case scenario without the worst-case outcome.

The difference in our approach starts with positioning your Red Team Exercise with the team as a training opportunity for detection and response capabilities.

Whether using novel or well-known adversary tradecraft, our objective is to provide a realistic understanding of the risk posed by an attack by advanced adversaries. We pride ourselves on building meaningful exercise objectives that help the organization close gaps in detection and response technology, processes, and staff training, and ensure our debrief provides the context needed to improve future response.

Trust is fundamental to a successful Red Team Exercise. We ensure that Red and Blue are collaborating leading up to and during the exercise. Regardless of whether the teams are Red or Blue, the goal is clear, to protect the organization. Both sides will understand the approach, how to raise alerts for deconfliction, and when to allow further access. After the exercise, we will provide a full activity log to allow the defenders to map their activities and telemetry to our actions and close any blindspots that exist.

Email info@specterops.io ›

Learn more at specterops.io ›

Real Results

- **Expert security resources:** Our experts, who themselves have discovered the tradecraft, will be the ones evaluating your program.
- **Real-world breach exercise:** Comprehensive, yet controlled, breach simulations while working with your defenders allow for learning and identifying process and telemetry gaps in your defensive capability.
- **Comprehensive and actionable reporting**: Understand the attacks that took place, the detection and response gaps, and actionable next steps to improve your defensive capabilities.
- **Transparent, clear communication:** Fully understand the attack paths and opportunities for detection of adversaries.