SPECTEROPS
Creators of BloodHound

DATASHEET

Services & Tradecraft

Defend Against Advanced Threats with Expert Adversary Insight

Adversaries use advanced tactics to exploit vulnerabilities and misconfigurations across your environment, from identity systems to applications to infrastructure, that traditional security tools miss. Effective defense requires the expertise and ability to expose these weaknesses and translate adversary tradecraft into action and improvement.

SpecterOps combines deep expertise, industry-defining research, and proven methodologies refined through thousands of real-world engagements.

Our services—from red team engagements and penetration testing to program development and maturity assessments—identify critical risks and build sustainable capabilities that demonstrate measurable impact and improvements.

200+ customers
including Fortune 500 companies and federal agencies across defense, finance, and healthcare sectors

400+ security community contributions
and nearly 100 open-source tools created by our industry-recognized team

10,000+ students
trained in adversary tactics by our expert practitioners

The SpecterOps Difference

Research that Drives the Industry

Our team discovers the attacks others will face tomorrow. We created BloodHound, the industry-standard tool for attack path analysis, plus GhostPack, Rubeus, Ghostwriter, Mythic, Misconfiguration Manager, SCCM Hunter and more. Our research—including Certified Pre-Owned, The Renaissance of NTLM Relay Attacks and SCCM adversary tradecraft—informs defensive strategies and validates security investments.

Operational Expertise at Scale

Foremost experts in adversary tactics and exploitation techniques, with proven methodologies refined through thousands of engagements across Fortune 500 and government organizations.

Long-Term, Trusted Partnerships

We build sustainable security capabilities owned by your organization. We aim to empower your teams, not build a dependency on consultants. Our mission: enable defense through education, visibility, and proactive countermeasures.

Key Outcomes

- Expose critical security gaps that traditional tools and approaches miss and demonstrate real-world impact through advanced adversary tactics and expert support
- Develop evidence-based remediation strategies that address critical findings and demonstrate measurable risk reduction
- Build audit-ready security programs with maturity assessments and capability development that create defensible, repeatable operations
- Reduce breach likelihood through training with adversary simulation that improves detection and response readiness without production risk

Offensive Security Services

Red Team Exercises: Train detection and response teams through realistic adversary simulation across traditional and AI-enabled systems. Validate efficacy and readiness while building confidence and institutional knowledge.

Penetration Testing: Identify viable attack paths to sensitive data and management systems across network, application, and specialty environments with objective-based testing. Translate technical vulnerabilities into business risk with findings that outline critical data impact and justify security investments.

Web Application Security Assessments: Evaluate web applications, including AI systems exposed through a web interface, using OWASP methodology from authenticated and unauthenticated perspectives. Identify exploitable vulnerabilities and demonstrate business risk and impact.

Attack Path Assessments: Comprehensively map chains of abusable privileges across critical assets, including AD and Entra ID. Eliminate attack paths through prioritized remediations—17,000 per fix on average—with step-by-step guidance that strengthens security posture.

Accelerate Attack Path Management: BloodHound Scentry provides ongoing advisory support with monthly analysis, remediation guidance, and expert reviews that drive continuous security improvement.

Security Program Development & Maturity Services

Build defensible security operations and develop resilient programs with documented processes, trained staff, and measurable outcomes that withstand audit scrutiny, scale with organizational growth, and demonstrate continuous security improvement.

Program Development: Build or revamp security operations with robust prevention, detection, validation, and response capabilities. Whether developing red team capabilities—including skillset development, operational training, and technical maturation—or standing up purple teams and detection programs, we partner to create sustainable capabilities with documented processes, attainable goals, and clear handoffs.

Maturity Assessments: Establish defensible baselines and identify gaps in people, processes, and technology across both offensive and defensive security programs. Prioritize improvements and develop capability roadmaps to demonstrate due diligence and drive measurable program growth.

Purple Team Assessments: Evaluate preventative and detective controls using comprehensive test cases representing real attack variations. Our layered testing model is designed to expose gaps where detection logic relies on inaccurate assumptions about attacker tradecraft, command-line patterns, process names, or native logging. Working alongside your SOC and IR teams, we deliver actionable recommendations that strengthen detection efficacy and justify your security investments.

Custom Solutions: We bring elite offensive security expertise and an adversary's mindset to any technology—no matter how unique or emerging. Custom assessments, AI security evaluations, and advisory services deliver actionable outcomes, knowledge transfer, and measurable security improvements.

Public and Private Training: Build team capabilities through adversary tactics training from front-line practitioners, including public courses, private organizational training, custom curriculum, and realistic lab and CTF environments.

Capture the Flag (CTF) Challenges: As the industry leaders in attack path exploitation, we're the experts in creating and hosting CTF ranges for humans and Cyber Ranges for AI, providing enterprise-level environments for continuous skills testing, practice, and training.

Learn more at specterops.io/training.

It is our vision at SpecterOps to create a more secure world by demystifying adversary tradecraft and promoting actionable approaches accessible to all.

Learn more at specterops.io/services ›

SPECTEROPS