NETSPI™

NetSPI's Red Team Operations

Exercise the people, processes, and technologies that comprise your detection, response, and recovery capabilities.

Red Team Operations mimic the tactics, techniques, and procedures (TTPs) of real-world adversaries utilizing a tailor-made approach to each engagement. Red Team exercises are designed to test the people, processes, and technologies of critical business functions and underlying systems against real-world conditions. You might look good on paper, but how do your defenses actually hold up?

NetSPI Red Team Operation Key Goals:

Validate Capabilities

Many teams purchase technologies and prepare for incidents; however, it is critical to validate effectiveness using a customized approach based on your unique objectives, challenges, and maturity level.

Educate Teams

Exercise blue teams to identify gaps, improve coverage within those gaps, and educate organizational teams on what to do if a real-world scenario occurs at any point within the cyber kill chain.

Improve Detection

Discover coverage gaps, determine potential impact, and gain actionable information that proves ROI and justifies budgets.

We are the Adversary

A tremendous amount of time, effort, and money is spent in securing modern environments. NetSPI's Red Team evaluates your assets and environments with an advanced, persistent adversarial lens. Not only do we emulate known, real-world TTPs designed to evade detection and response capabilities, but our dedicated research and development team develops customized payloads, beaconing implants, interactive remote access tools, and more. Utilizing unique attack vectors and novel TTPs, we put your organizational assumptions to the test and push blue teams to think outside the box.

NetSPI has developed and taught red team courses around the globe

Learn more about Dark Side Ops 1 - Malware Development, and Dark Side Ops 2 - Adversary Simulation.

https://www.netspi.com/training/

NETSPI

NetSPI's Red Team Operation Offerings:

Black Box Exercise is designed to simulate a threat actor starting with little to no knowledge of the organization's assets and environments, delivering understanding and measurement of your ability to detect, contain, eradicate, and recover from attacks originating from the internet. We use a combination of attack types customized to your objectives, such as various forms of social engineering, server-level exploits, web application exploits, credential and authentication endpoint abuse, and much more.

Assumed Breach Exercise takes the approach of "not **IF** an organization gets breached, but **WHEN**." Starting from an internal perspective such as an end user being compromised via social engineering or another agreed upon attack scenario, this is designed to simulate a threat actor who has already gained access to your environment or that of a trusted third-party.

NetSPI's Unique Red Team Benefits:

Methodology developed by founding team members from the NSA and DoD, and decades of industry leading security testing expertise.

NetSPI's exclusively developed command and control (C2) framework and post exploitation tools with more than a decade of supporting R&D.

Dedicated full-time Red Team R&D staff focus on developing and integrating new, unique TTPs into our tooling and methodology.

Test and verify that the people, processes, and technologies work together correctly to defend against advanced attacks.

We educate blue teams with novel techniques not seen elsewhere.

We challenge assumptions made by security management and operations personnel about their own environments and capabilities.

Our top priority is your blue team. Exercising and assisting them with identifying gaps in process and technology.

Experienced consultants ready to deliver to internationally regulated standards such as EU-TIBER, CBEST, GBEST & many more.

To learn more about NetSPI's Red Team Operations, or any of our other offerings, visit www.netspi.com or contact us.

Platform Driven, Human Delivered

ASM | BAS | RESOLVE

Attack Surface Management • Breach and Attack Simulation • Penetration Testing as a Service
Application Pentesting • Cloud Pentesting • Network Pentesting • AI/ML Pentesting • IoT Pentesting
Blockchain Pentesting • SaaS Security Assessment • Secure Code Review • Cybersecurity Maturity
Red Team Operations • Social Engineering • Strategic Advisory

About NetSPI:

NetSPI is the global leader in offensive security, delivering continuous and scalable penetration testing, attack surface management, and breach and attack simulation solutions to the world's most prominent organizations.