NetSPI™

Red Team Operations

Test the people, processes, and tech of your organization's detection, response, and recovery capabilities

The most trusted products, services, and brands are secured by NetSPI

The Challenge

Many organizations struggle to keep their security teams, processes, and systems on pace with the evolving threat landscape. To address these challenges, they must adopt robust cyber defense strategies, such as business-wide red teaming exercises.

Deciding between in-house or third-party services can be tough. Third-party exercises may oversimplify threats or be too advanced for meaningful learning, while in-house exercise can lack realism and fresh ideas.

With significant time and budget involved, red team exercises must align with organizational objectives, use resources efficiently, and account for the maturity of the organization's security culture, capabilities, and technology.

The Solution

NetSPI's Red Team addresses these challenges by simulating and emulating organizational threats. Our expert operators work with organizations across all industries to emulate advanced adversaries, such as nation-state groups, advanced persistent threats, and sophisticated ransomware groups. Our experts, with decades of experience, conduct cutting-edge research and use proprietary tools to deliver realistic scenarios. We recreate and develop innovative tactics, techniques, and procedures to validate how people, processes, and technologies work together, while meeting compliance and complex business needs. This approach empowers your team to strengthen cyber defenses.

With NetSPI Red Team Operations, you can:

- Comply with regulatory requirements and frameworks, including EU's DORA, TIBER-EU, Bank of England CBEST, STAR and STAR-FS, iCAST, CORIE, and more.
- Test cyber and operational resiliency, and measure detection and response improvements.
- Gain strategic security insights with actionable recommendations to mitigate risks and improve defenses.
- Educate your blue team with the successful attack chains mapped to MITRE and through custom, post-operation workshops.

> **"73% of organizations consider the red team role as a significant or highly significant contributor to security operations goals. However, only 28% of organizations have at least one full-time red teamer."[1]**

[1] Gartner. *Improve Cyber Resilience by Conducting Red Team Exercises*. September 9, 2024.

NetSPI's Approaches to Red Team Operations

NetSPI offers several approaches to red team exercises. All engagements are customizable for your unique needs, provide comprehensive analysis with tailored remediation strategies, and deliver valuable technical insights.

Assumed Breach & Scenario-Based Testing (SBT)

This exercise assumes a bad actor breached your environment, with realistic threat scenarios tailored to your business.

- A balanced approach of pentesting and red teaming focused on key business areas.
- Custom scenarios targeting specific areas of the NIST Cybersecurity Framework that are most relevant to your needs.
- Targets a wider set of systems with less complexity and a cost-effective scope.

Black Box

Test your organizational security capability end-to-end by having our experts mimic a bad actor.

- Experience the full impact of a bad actor exploiting your network.
- Validate assumptions by testing all controls and capabilities as an attacker would.
- Challenge business resilience and response with an exercise that mirrors a real-world attack of unknown origin.

Threat Intelligence-Led Red Team

NetSPI supports compliance with DORA by testing digital operational resilience through red teaming and/or threat-led penetration testing aligned to frameworks such as Bank of England CBEST, TIBER-EU and DORA, and more.

- Focus on predefined scenarios that test key Important Business Services (IBS) composed of Key Supporting Systems (KSS) aligned to threat intelligence data.
- Leverage NetSPI's expertise and third-party threat intelligence to create realistic, evidence-based testing that reveals who is targeting you, how they operate, and their likely technology capabilities.
- Demonstrate regulatory adherence and ensure your clients and the public remain safe.

You Deserve The NetSPI Advantage

300+ In-House Security Experts

Intelligent Processes

Advanced Technology

Your Proactive Security Partner

NetSPI is the proactive security solution used to discover, prioritize, and remediate security vulnerabilities of the highest importance. NetSPI helps its customers protect what matters most by leveraging dedicated security experts and advanced technology, including Penetration Testing as a Service (PTaaS), External Attack Surface Management (EASM), Cyber Asset Attack Surface Management (CAASM), and Breach and Attack Simulation (BAS) as a Service.