NetSPI™

Red Team: Threat Intelligence-Led Red Team Operations

Enable attack resilience of important business services and key supporting systems for global critical economic and national infrastructure

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

The Challenge

The global economy relies on finance and government to maintain resilience to threats. Monetary authorities and regulators are working globally to address this challenge by creating frameworks that address cyberattack resiliency. These include the Digital Operational Resilience Act (DORA) Act in the European Union, Critical National Infrastructure Banking Supervision and Evaluation Testing (CBEST) in the United Kingdom, and Threat Intelligence Based Ethical Red-Teaming (TIBER-EU) in Europe.

Complying with these regulations requires forethought and planning beyond that of a normal red team operation. These requirements and frameworks focus specifically on the confidentiality, integrity, or availability of key systems used to perform essential business operations. They are aligned to regulators' needs and use custom threat intelligence specific to the client and their profile. The challenge for organizations that must align to these frameworks is how to safely test their environments while effectively simulating advanced attackers and their methodologies.

The Solution

NetSPI's Threat Intelligence-Led Red Team Operations allows organizations to meet their requirements and formulate appropriately targeted evidence-based scenarios that are most likely to affect their business.

Our team is accredited for those frameworks that require it, such as CBEST, and can provide testing for TIBER-EU and other standards. We work with regulators and threat-led intelligence firms to ensure you meet compliance requirements.

NetSPI uses threat intelligence data from threat actors who have shown interest in similar organizations. This includes validated threat data, evidence of breaches past and present, active vulnerabilities, access brokerage, and numerous other sources. This data is analyzed, and applicable tactics, techniques and procedures (TTPs) are collated to provide information for an engagement plan. These TTPs and target systems are combined to form scenarios used for the operation with firm guidelines and processes to ensure realistic simulation.

The financial services sector has suffered more than 20,000 cyberattacks, causing $12 billion in losses, over the past 20 years.[1]

[1]Rising Cyber Threats Pose Serious Concerns for Financial Stability

Align With Security Frameworks and Regulations

NetSPI red team operations are designed to work with threat intelligence vendors

Our red team experts understand how to deliver a threat intelligence-led red team operation including the ability to:

- Identify the attack resilience of critical business services, processes, and systems
- Understand the key supporting systems related to those key services
- Create pre-defined real-world scenarios for complex and highly technical structured red team engagements

Improve Your Organization's Ability to Detect and Respond to Risk

Our operations help you measure and improve your planning, response, and overall defense of risks to your key functions and processes

NetSPI ensures that your organization is put to the test and measures capabilities including:

- Measure your ability to identify, protect, detect, respond, and recover from a specific threat across your entire business and supply chain
- Gain depth of understanding of real-world scenarios and methodology for response
- Identify unique attacker activities like long-term covert access to critical systems

Accelerate Risk Reduction By Remediating Where You Are Susceptible to Proven Threat Sources

Gain detailed analysis and recommendations for mitigating findings as well as insight into tactical and strategic fix objectives

Our experts align with industry proven and approved, highest quality threat intelligence to ensure targets and scenarios are the most impactful real-world scenarios for your environment. Guidance includes:

- Dedicated and experienced pentest/red team planning documentation
- After action, after care and post execution learning workshops
- Detailed analysis and recommendations for mitigation of findings to technical, managerial, and stakeholder groups
- In-depth explanation of potential impact to your environment, your organization, and the economic ecosystem in which you operate, including your clients, the public, and downstream supply chain
- Documented narrative with timestamps for scenario testing activity, including opportunities for new controls and in-depth technical insights

About NetSPI

NetSPI® pioneered Penetration Testing as a Service (PTaaS) and leads the industry in modern pentesting. Combining world-class security professionals with AI and automation, NetSPI delivers clarity, speed, and scale across 50+ pentest types, attack surface management, and vulnerability prioritization. The NetSPI platform streamlines workflows and accelerates remediation, enabling our experts to focus on deep dive testing that uncovers vulnerabilities others miss. Trusted by the top 10 U.S. banks and Fortune 500 companies worldwide, NetSPI has been driving security innovation since 2001. NetSPI is headquartered in Minneapolis, MN, and available on **AWS Marketplace**. Follow us on **LinkedIn** and **X**.