NetSPI™

BAS

NetSPI Breach and Attack Simulation (BAS)

NetSPI BAS simulates network and system cyberattacks to validate the efficacy of your security detection controls by blending industry-leading technology with human intelligence. Perform a security readiness assessment by leveraging pre-built simulated attacks that mimic tactics, techniques, and procedures (TTPs) used by threat actors, including malware techniques, advanced persistent threats (APTs), data exfiltration, and more. This helps you gain visibility of your environment and identify detection and prevention gaps.

Build on insight from our security experts to educate your SOC team and simulate real-world attacker behaviors. Learn from step-by-step instructions to identify and mitigate potential threats as you fine-tune your detection controls. Track and share the efficacy of your security capabilities over time with timelines and dashboards mapped to the MITRE ATT&CK framework.

Assess existing detective controls

NetSPI BAS starts with a comprehensive manual assessment led by our security experts, who will engage with your security operations team to guide you through testing. During this period, they will simulate attacks on your environment to generate security events. This process will validate your existing detection controls, assess the effectiveness of your internal configurations, and determine your coverage level.

Our assessment is based on the MITRE ATT&CK framework and industry best practices. Throughout the assessment, we will:

- Inventory known controls
- Manually simulate attacks across the entire cyber kill chain
- Monitor security events and alerts with your security operation team
- Identify major control gaps and misconfigurations, including missing or misconfigured logs, security tool rules, alerts, and responses
- Provide actionable feedback and recommendations, including log sources, indicators of attack/compromise, rules guidance, and mitigating controls recommendations

This crucial process assesses whether security controls are effectively implemented and operating as intended. After completing the initial assessment, you will receive a detailed report that offers in-depth insights into identified gaps and detection trends, along with prioritized remediation recommendations to enhance your defensive posture.

Data sources

To determine if security controls are functioning effectively, it is crucial to identify the events and data that generate telemetry for identifying potential malicious behavior in your environment. NetSPI BAS evaluates your network, applications, databases, and endpoints to confirm what is and isn't triggering telemetry (logs). Without the appropriate data sources, you cannot generate the necessary detections and alerts that your response team needs.

BAS verifies the following data sources:

- NetFlow data between internal subnets
- Windows Event Logs on workstations
- PowerShell logging
- Critical events from windows event logs
- DNS logs

Common data sources

Network devices
- Netflow & packet data
- Auth & traffic logs
- Security alerts

Endpoint anti-virus & EPP
- File hashes
- Domains
- IP addresses
- Packet data

Endpoint, ADS, app, and DB event logs
- Default events
- Non-default events
- Third party events

Endpoint EDR
- Process (ETW)
- Scripting engines (AMSI)
- File system (ETW)
- Registry (ETW)
- Image/driver loads (ETW)
- API & system calls (ETW)

Sysmon endpoint event logs
- Process create
- Process terminate
- Network connections
- Driver/image leading
- Create remote thread
- Raw disk access
- Memory access
- Registry access
- Named pipes
- WMI
- DNS
- File create timestamp changes

Security control validation using The NetSPI Platform

Following the initial assessment, you can access your instance of The NetSPI Platform to review results and conduct attack simulations independently. It includes a custom playbook with detailed, step-by-step instructions to replicate initial tests, and provides extensive guidance on building effective detections. You have the flexibility to run these tests on demand or automate them to occur at your preferred frequency. These tests verify that your security control configurations function as intended, both before and after making adjustments to the detection settings.

Examples of what you can test in your environment:

- EPP and EDR
- SIEM
- IDS/IPS
- Access control mechanisms
- Network security controls
- Firewalls
- Data loss prevention

Deploying NetSPI BAS in your environment

NetSPI BAS uses a non-persistent agent, that can be deployed to Windows or Linux endpoints. There is no installation process – you simply download the agent and execute it on your endpoint. To remove it, you close it and delete the agent from the system. There is no limit to the number of agents you can deploy.

Customized attack simulation and advanced scenarios

Customize and automate your attack simulations, conduct advanced assessments, and develop tailored playbooks to meet your unique requirements. BAS is engineered for flexibility, catering to advanced users who wish to execute technical tasks, such as deploying payloads, running arbitrary commands, executing custom code, and replaying packet captures.

Additionally, you can create custom playbooks by selecting the TTPs you wish to test, and using them to maximize your purple team exercise. This comprehensive and adaptable approach identifies security detection gaps throughout the cyber kill chain, so you can improve your defenses against cyber threats.

Ransomware prevention

Detecting ransomware early and improving detection capabilities are key to stopping intrusions from escalating into a full-scale incident. NetSPI BAS provides a pre-built ransomware playbook that mimics our security experts' observations of TTPs and patterns that specific ransomware operators use. You can create playbooks to emulate a specific threat actor, such as CL0P, BlackCat, and Fin7. Your security team will verify how well your security tools can detect ransomware, so you can act on prevention guidance and continuously fine-tune detection controls. This ongoing approach strengthens your defense against ransomware.

Reporting and visualization

The BAS workspace serves as your central hub, offering visuals and mapping coverage gaps within a MITRE ATT&CK matrix. Utilize this tool to develop a strategic roadmap for areas needing improvement, and receive step-by-step mitigation instructions. After conducting simulated attacks, you can review the overall coverage summary or use the timeline view to track progress over time. These graphs can effectively demonstrate continuous improvements, validate the effectiveness of adjustments to your security controls, prove ROI, justify security tool spend, and provide impactful visuals that resonate with executives and the Board.

You deserve The NetSPI Advantage

250+ In-house security experts

Intelligent process

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).