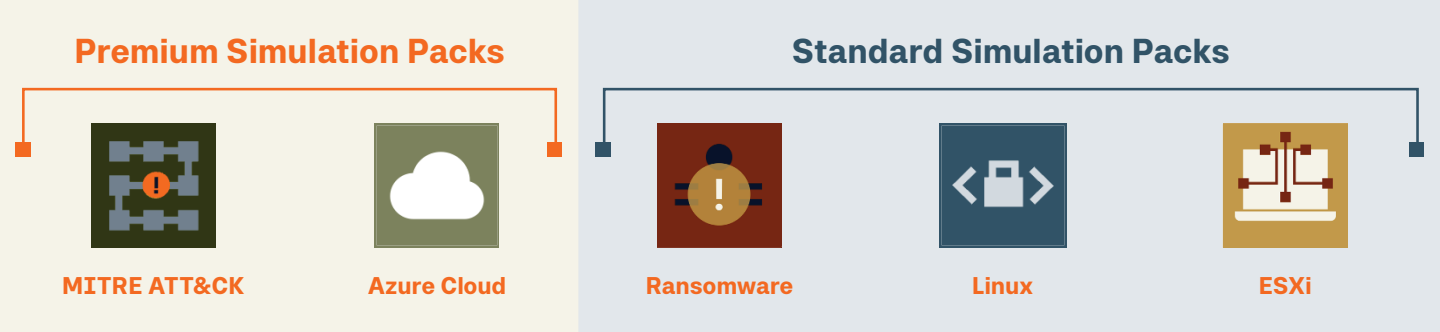
NetSPI™

BAS AS A SERVICE

NetSPI Breach and Attack Simulation (BAS) as a Service Simulation Packs

Focused simulation packs to validate the efficacy of your detective controls in your unique environment.

BAS as a Service uses real-world simulations to validate the effectiveness of security controls across endpoint security solutions, network security solutions, SIEMs, and MSSPs. It identifies critical gaps, including misconfigurations and missed detections, and provides focused testing (simulation packs) to fit your unique environment. The focused simulation packs deliver comprehensive manual testing led by our security experts, who will engage with your security operations team to guide you through the process. You can select individual simulation packs or combine them for discounted pricing.



How It Works

- NetSPI designs the simulation packs and leverages existing BAS procedures and plays.
- NetSPI will work with you in real-time to execute tactics, techniques and procedures (TTPs) that simulate real-world attackers and determine the level of visibility the current controls offer.
- NetSPI will educate your team on the TTPs being executed and the detection opportunities unique to each.
- After NetSPI performs each test, you will determine if the activity generated logs, triggered any detections or alerts, and/or triggered a response.
- Findings will include mappings to MITRE ATT&CK technique IDs. The technique number will be included in the finding references, and directly noted in the finding names provided.
- Requires one point of contact that can be present during testing that can provide feedback on what security events generate logs and alerts.
- Subscription includes access to The NetSPI Platform for one year, where you can leverage, test, and retest attack scenarios based on real-world TTPs outlined in the MITRE ATT&CK framework, and derived from NetSPI's extensive industry experience and research.

Standard Requirements

- Access to a standard company workstation, virtual machine, or virtual desktop infrastructure (VDI) with standard security software policies installed.
- One local administrator account on the provided workstation(s).
- One Active Directory domain user account that can log into the workstation(s). This domain user will also require VPN access and an email account.
- One Active Directory domain user with "Domain Admin" privileges.

Focused Simulation Pack Offerings

MITRE ATT&CK Simulation Pack

The MITRE ATT&CK Simulation Pack enables your organization to gain an empirical understanding of your ability to detect attack scenarios and develop a roadmap to improve those capabilities over time. NetSPI conducts attack simulations focused on TTPs across all domains outlined in the MITRE ATT&CK framework, prioritizing common threat vectors, attacker behaviors, and high-risk threats.

The test plan includes techniques and procedures from the following tactics:

- Discovery, including Active Directory reconnaissance
- Credential access
- Lateral movement, including SMB share scanning
- Command and control
- Data exfiltration
- Impact, including ransomware encryption events
- Initial access
- Command execution
- Persistence, including Active Directory domain persistence
- Defense evasion

Primary Objectives

- Validate that your endpoint, network, SIEM, MDR, and/or MSSP security controls are working as intended.
- Identify and remediate detection gaps, such as missing data sources, misconfigurations, missing detections, incomplete coverage, and cyber kill chain gaps.
- Leverage The NetSPI Platform to continuously improve your ability to detect and prevent common attacks, track progress over time, track gaps in your environment, and achieve your key performance indicators (KPIs).

Azure Simulation Pack

The Azure Simulation Pack addresses authenticated and anonymous attacks against Azure cloud resources and configurations, and helps gather correlations between common cloud attacks and log sources in Azure. NetSPI conducts attack simulations focused on your Entra tenant and against your users, and other cloud resources. It enables your organization to gain an empirical understanding of your ability to detect attack scenarios and develop a roadmap to improve those capabilities over time. The Azure Simulation Pack takes a holistic view across the entire cyber kill chain and incorporates the TTPs across all domains outlined in the MITRE ATT&CK Cloud Matrix.

The test plan includes techniques and procedures from the following tactics:

- Initial access
- Discovery, including Entra ID Tenant reconnaissance
- Command execution across various Azure hosted services
- Virtual machines, automation accounts, app services applications, etc.
- Persistence, including Entra ID tenant persistence and Azure resource persistence
- Defense evasion
- Lateral movement, including Azure RBAC pivoting
- Entra ID privileged actions
- Privilege escalation, including subscription and tenant level RBAC elevation
- Command and control
- Data collection and exfiltration
- Impact, including destructive events simulation

Azure Simulation Pack *(continued)*

Primary Objectives

- Validate that your cloud, endpoint, network, SIEM, MDR, and/or MSSP are working as intended.
- Identify and remediate detection gaps, such as missing data sources, misconfigurations, missing detections, incomplete coverage, and cyber kill chain gaps.
- Leverage The NetSPI Platform to continuously improve your ability to detect and prevent common attacks, track progress over time, track gaps in your environment, and achieve your key performance indicators (KPIs).

Additional Requirements

- Access to a Windows Azure virtual machine with the ability to access the Azure Portal for the Entra ID tenant.
- One local administrator account on the provided workstation(s).
- One Entra ID tenant user account with appropriate RBAC permissions.
- Most of the procedures will require some level of Contributor permissions on the in-scope Azure resources.
- Access to an Entra ID account with the Global Administrator role applied.
- This can be granted via shadowing an existing privileged user, or by utilizing Privileged Identity Management for temporary access.

ESXi Simulation Pack

The ESXi Simulation Pack validates hypervisor-specific security controls to mitigate privilege escalation risks and protect interconnected machines. During the ESXi engagement, NetSPI conducts attack simulations focused on real-world adversarial TTPs common in ESXi environments. This will enable your organization to gain an empirical understanding of your ability to detect attack scenarios and develop a roadmap to improve those capabilities over time.

The test plan includes the following unit test categories:

- Discovery
- Execution, including via PowerCLI and API
- Persistence
- Credential access and defense evasion
- Impact

Primary Objectives

- Validate that your endpoint, network, SIEM, MDR, and/or MSSP security controls are working as intended.
- Identify and remediate detection gaps, such as missing data sources, misconfigurations, missing detections, incomplete coverage, and cyber kill chain gaps.
- Leverage The NetSPI Platform to continuously improve your ability to detect and prevent attacks, track progress over time, track gaps in your environment, and achieve your key performance indicators (KPIs).

Additional Requirements

- Access to one ESXi server with representative controls installed.
- One local administrator account on the provided host.
- One local user account that can be used to log into the virtual machines.

Linux Simulation Pack

The Linux Simulation Pack addresses the challenges that come with the complex environment of Linux and open-source software. During the Linux engagement, NetSPI conducts attack simulations focused on TTPs often used to exploit Linux environments, such as remote code execution, shell configuration modifications, data extraction, and more.

The test plan includes the following unit test categories:

- Discovery, including Local and Active Directory reconnaissance
- File system access events
- Persistence
- Lateral movement, including SSH service scanning and SSH multiplexing
- Defense evasion
- Credential access and defense evasion

Primary Objectives

- Validate that your endpoint, network, SIEM, MDR, and/or MSSP security controls are working as intended.
- Evaluate usage of native controls and data sources to log and detect events such as Auditd.
- Identify and remediate detection gaps, such as missing data sources, misconfigurations, missing detections, incomplete coverage, and cyber kill chain gaps.
- Leverage The NetSPI Platform to continuously improve your ability to detect and prevent attacks, track progress over time, track gaps in your environment, and achieve your key performance indicators (KPIs).

Additional Requirements

- Access to one (preferably two) Linux workstations or servers with representative controls installed.
- One local root account on the provided host.
- One Active Directory domain user account that can be used to log into the workstation(s) (Optional).

Ransomware Simulation Pack

The Ransomware Simulation Pack helps you develop a baseline understanding of your current detective control capabilities against ransomware attacks and create a roadmap for improvement over time. The Ransomware Simulation Pack conducts attack simulations focused on the TTPs and behaviors from real-world ransomware campaigns, including specific threat actors.

The test plan includes the following unit test categories:

- Discovery, including Active Directory reconnaissance
- Credential access events
- Authenticated scanning events
- Lateral movement, including SMB share scanning
- Data exfiltration
- Impact, including ransomware encryption events

Ransomware Simulation Pack *(continued)*

Primary Objectives

- Validate that your endpoint, network, SIEM, MDR, and/or MSSP security controls are working as intended.
- Identify and remediate detection gaps, such as missing data sources, misconfigurations, missing detections, incomplete coverage, and cyber kill chain gaps.
- Leverage The NetSPI Platform to continuously improve your ability to detect and prevent ransomware attacks, track progress over time, track gaps in your environment, and achieve your key performance indicators (KPIs).

Additional Requirements

- Access to one (preferably two) Windows workstations with representative controls installed.
- One local administrator account on the provided workstation.
- One Active Directory domain user account that can be used to log into the workstation(s).

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.