NetSPI™

NetSPI Detective Controls Validation

NetSPI Detective Controls Validation simulates system, network, and cloud-based cyberattacks to validate the efficacy of your detective controls. NetSPI's experts help inventory and benchmark security controls through simulated attacks that mimic tactics, techniques, and procedures (TTPs) used by threat actors, including ransomware techniques, malware techniques, advanced persistent threats (APTs), data exfiltration, and more. This helps you gain visibility into meaningful detective and preventative control gaps in your environment that represent real risk.

Detective Controls Validation uses real-world simulations to validate the effectiveness of security controls like endpoint security solutions, network security solutions, SIEMs, and MSSPs. It identifies critical gaps, including misconfigurations and missed detections, and provides focused testing to fit a customer's unique environment. Customers can select individual attack simulation packs or combine them for discounted pricing.

Build on insights 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 detective controls. Track and share key performance indicators and efficacy of your detection capabilities over time with timelines and dashboards mapped to the MITRE ATT&CK framework.

Benchmark Existing Detective Controls

Detective Controls Validation offers focused attack simulation packs that deliver comprehensive manual testing led by our security experts, who will engage with your security operations team to guide you through the process. The controlled attack simulations will be conducted within your environment to generate and analyze security events with you. These simulations are typically executed against non-production systems that are representative of your production environments. They often use golden system images to ensure no operational interruptions. This process helps validate the effectiveness of your existing detection controls and internal configurations, as well as provides an analysis of your coverage level.

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

- Inventory known detective and preventative controls
- Manually simulate attacks across all stages of the cyber kill chain
- Monitor security events with your security operation team to determine level of detection (logged, detected, alerted, responded, prevented)
- Identify major control gaps and misconfigurations, including missing or misconfigured logs, security tool rules, alerts, and responses
- Provide actionable feedback and prioritized recommendations to help you identify quick wins and long coverage goals that take the context of your environment into account in a meaningful way

This crucial process validates whether security controls are effectively implemented and operating as intended. After a simulation pack is completed, you will receive a detailed report that offers in-depth insights into identified gaps and detection trends, along with prioritized remediation recommendations to strengthen your defensive posture.

NetSPI Detective Controls Validation focused attack simulation packs include:

MITRE ATT&CK

- Provides a holistic view of detection controls across the entire network.
- Simulates TTPs across the cyber kill chain, prioritizing common threat vectors, attacker behaviors, and high-risk threats identified by our expert analysis.

Azure Cloud

- Helps gather correlations between common cloud attacks and log sources in Azure.
- Addresses authenticated and anonymous attacks against Azure cloud resources and configurations, including command execution, credential guessing, sensitive data gathering, and more.
- Simulates attacks on your Entra tenant and against your users, and other cloud resources.

Ransomware

- Fine-tune security configurations to detect ransomware early in the kill chain, preventing lateral movement, privilege escalation, and encryption of data.
- Simulate TTPs and behaviors from real-world ransomware campaigns, including specific threat actors such as CLOP, BlackCat, and Fin7.

Linux

- Addresses the challenges that come with the complex environment of Linux and open-source software.
- Focuses on tactics often used to exploit Linux environments, such as remote code execution, shell configuration modifications, data extraction, and more.

ESXi

- Validate hypervisor-specific security controls to mitigate privilege escalations risks and protect interconnected virtual machines.
- Simulate real-world adversarial tactics, such as brute force, ransomware, and threat vectors that are common in ESXi environments.

Data Sources

To determine if security controls are functioning effectively, it is crucial to identify the events and data that generate telemetry (logs) for identifying potential malicious behavior in your environment. NetSPI Detective Controls Validation evaluates your network, applications, databases, endpoints, and much more to understand where you may be missing critical telemetry. Without the appropriate data sources, you cannot generate the necessary detections and alerts that your response team needs.

Examples of Common Data Sources[1]

Network Events

- Network traffic data such as packet capture and flow data
- Firewall events
- DNS query events
- LDAP query events
- DHCP events

Application Events

- Native application, system, and security event logs
- User account creation, modification
- Group creation, modification
- Active Directory audit events
- Dangerous object creation, read, update, and deletion events

Cloud Events Azure

- Azure activity logs
- Entra ID audit logs
- Resource/diagnostic log

Endpoint Events

- Security events: AV, EPP, EDR, MDR, XDR
- Process creation, read, update, and deletion events
- Script events: AMSI, WMI, PowerShell
- File creation, read, metadata read, update, and deletion events
- Windows Registry creation, read, update, and deletion events
- Service creation, read, metadata read, update, and deletion events
- Scheduled task creation, update, deletion events
- Image load
- Driver load
- Named pipe creation, read, update, deletion events

[1] A full list of MITRE ATT&CK Data Sources can be found at https://attack.mitre.org/datasources/

The NetSPI Platform

Use the NetSPI Platform to independently conduct attack simulations, review results, and monitor performance. You can access, search, and filter through all TTPs that you want to test. All procedures include deep context, such as step-by-step instructions, potential business impacts, prevention guidance, and more. You have the flexibility to run these tests on demand or automate (schedule) them to occur at your preferred frequency. These tests verify that your security control configurations function as intended, both before and after adjusting the detection settings.

Examples of what you can test in your environment:

- SIEM
- EPP, EDR, MDR, and XDR
- MSSP coverage
- Data loss prevention
- IDS/IPS
- Access control mechanisms
- Network security controls
- Firewalls

Deploying NetSPI Detective Controls Validation in Your Environment

Detective Controls Validation, powered by The NetSPI Platform, 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 the file on an 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 testing, and develop tailored playbooks to meet your unique requirements. The Detective Controls Validation on The NetSPI Platform 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.

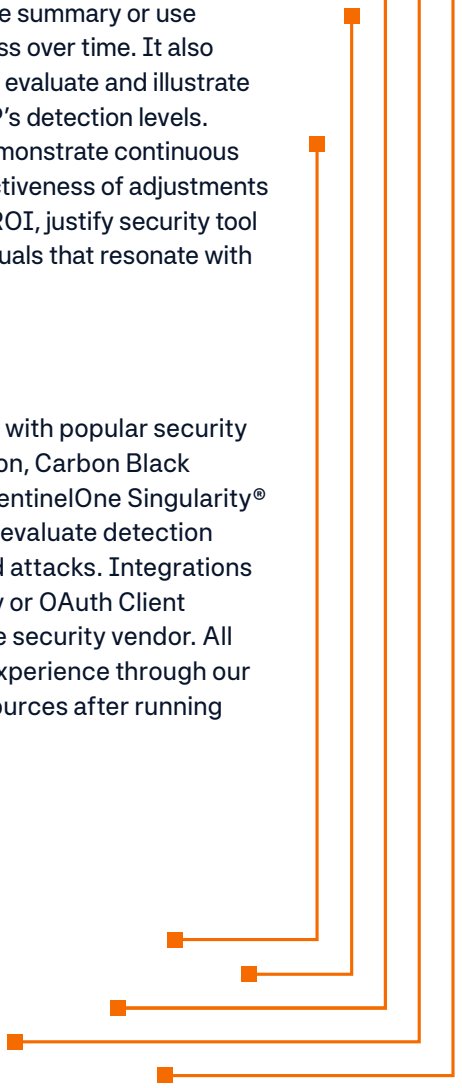
Additionally, you can create custom playbooks by selecting the TTPs you wish to test, and use them to maximize your red/purple team exercises. This comprehensive and adaptable approach identifies security detection gaps throughout the cyber kill chain, so you can improve your defenses against cyber threats.

Reporting and Visualization

NetSPI provides visuals and mapping coverage gaps within a MITRE ATT&CK matrix. Utilize this tool to develop a strategic roadmap for areas needing improvement and review step-by-step mitigation instructions. After conducting simulated attacks, you can view the overall coverage summary or use the timeline view to track progress over time. It also features a vendor comparison to evaluate and illustrate your security tools' and/or MSSP's detection levels. 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.

Integrations

The NetSPI Platform integrates with popular security tools, such as CrowdStrike Falcon, Carbon Black Cloud, Splunk Enterprise, and SentinelOne Singularity® to help your team automatically evaluate detection levels associated with simulated attacks. Integrations are easy to add through API key or OAuth Client credentials, depending upon the security vendor. All integrations facilitate a better experience through our event viewer, as you add data sources after running tests on The NetSPI Platform.



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**.