Service Definition

Attack Surface Management

G-Cloud 14

Lot 3 Cloud Support

1. Introduction

Company Overview

Through a combination of technology innovation and human ingenuity, NetSPI helps the world's most prominent organisations discover, prioritise, and remediate security vulnerabilities.

With deep roots in pentesting and robust training programs, we are the most highly skilled manual testing team in the industry.

Our methodology is efficient, rigorous, and consistent. Expect high-quality results that are measurable and actionable.

Our tech provides continuous transparency into your testing engagements and results. Manage the entire vulnerability lifecycle, from discovery to remediation.

The depth and breadth of the NetSPI team is unmatched. We have the resources, experience, and technology to be flexible and enable our customers to innovate with confidence.

We believe pentesting is a vital element of your organisation's security program maturity and innovation goals. NetSPI serves as an extension of its customer teams to help them better understand, prioritise, and mitigate risk to the business.

From project management workflows and practitioner guides to standardised checklists and pentesting playbooks, we have formalised quality assurance and oversight to deliver consistent results.

Service Summary

Many organisations struggle to keep up with an expanding attack surface. Whether they know it or now, organisations are experiencing constant change.

NetSPI's Attack Surface Management (ASM) service improves your visibility, inventory, and understanding of your assets and exposures with. Monitor 24/7/365 with continuous pentesting and leverage our team, technology, and comprehensive methodology to discover and address risky exposures before adversaries do.

NetSPI ASM uses a combination of commercial, open-source, and proprietary techniques to discover and assess internet-facing assets, including known and unknown IPs, domains, Autonomous System Numbers (ASNs), and more. Additionally, we integrate directly with the cloud service providers AWS, Azure, and GCP to monitor cloud accounts for externally facing IPs and domains. Our continuous and comprehensive automated scanning against discovered assets consists of full 65535 TCP port scans with both ping and no ping methods, UDP port scanning, and vulnerability assessments for network and web applications. All services on live assets are then identified and cataloged, enhancing our visibility into the operational landscape of your network. The continuous aspect of NetSPI ASM allows you to know about vulnerabilities as soon as they occur to drastically reduce exposure time and risk

2. Service Details

Identify and Protect the Unknown

You don't know what you don't know. And what you don't know can hurt you. Don't wait for your next pentest to uncover risky exposures.

Attack Surface Management detects known, unknown, and potentially vulnerable public-facing assets, as well as changes to your attack surface that may introduce risk. How? Through a combination of NetSPI's powerful ASM technology platform, our global penetration testing experts, and our 20+ years of pentesting expertise.

Continuous Penetration Testing

Take comfort in the fact that the ASM platform is always-on, working continuously in the background to provide you with the most comprehensive and up-to-date external attack surface visibility. Get proactive with your security using continuous testing.

Asset Discovery with Attack Surface Monitoring

ASM is driven by our powerful automated scan orchestration technology, Scan Monster, which has been utilised on the front lines of our pentesting engagements for years.

We use various automated and manual methods to continuously discover assets and leverage open-source intelligence (OSINT) to identify publicly available data sources. With every asset we equip you with a broad spectrum of details, including domains, DNS records, IP addresses, ports, products, certificates, and more.

Not only can you identify assets before adversaries do, but you can also gain a better understanding of the potential concerns that might impact your insurance premiums or your ability to earn your certificate of insurance.

Manual Exposure Triaging

Modern ASM requires human intuition to provide context around exposures that could cause the most harm to your business. NetSPI's security consultants are a critical component to our Attack Surface Management service. We collaborate with you to:

Triage Exposures

If we notice an asset that looks risky on the surface, our global penetration testing experts will manually investigate it to determine if it exposes your organisation. Then, we'll help you understand the risk to the business and prioritise remediation efforts.

Review Your Results

On an ongoing basis, we will schedule review meetings. During the meetings, your NetSPI team will provide insights into the exposures and details that matter most.

Improve Your Pentests

Attack surface management informs your external penetration testing strategy. Identify key areas that warrant further testing and focus on manual testing techniques to find business-critical vulnerabilities tools often miss.

Boost Productivity and Security with Integrations

NetSPI's offensive security tools seamlessly integrate with your existing technology stack to improve your vulnerability management workflow and save you countless hours of manual effort.

- Jira
- Service Now
- Microsoft Teams
- 1,000+ more

Attack Surface Management (ASM)

NetSPI's Attack Surface Management service is powered by a cloud native, internet-scale application: ASM. The technology enables our global penetration testing experts to find gaps in your security posture that tools miss. It provides an interactive interface for continuous pentesting and efficient ASM features include:

- Immediate and simple set up
- Tracking and trending data over time
- 24/7/365 internet-scale scan coverage
- Asset intelligence
- Slack and email integration
- Open-source intelligence gathering
- Asset and exposure prioritisation
- Port discovery

3. Using the service

Ordering and Invoicing

1. This is a subscription service that does not include travel or other expenses. Services are priced on a subscription basis. For the first Service Term, 100% of the Subscription Total will be invoiced upon contract signature. For subsequent Service Terms, 100% of the Subscription Total will be

invoiced either upon the anniversary of the Effective Date or the occurrence of the first kickoff call for the Services or project planned for the applicable Service Term, whichever is earlier.

2. All prices are shown in GBP and all payments must be made in UK Currency.

3. Pricing is exclusive of applicable sales taxes and any other applicable taxes that may be required. NetSPI will invoice, and Client will be responsible for, all applicable taxes specific to either services or products provided and charged to Client. For the avoidance of doubt, Client and NetSPI shall each bear sole responsibility for all taxes based on its own net income, employment taxes of its own employees (such as payroll and withholding), and for taxes on any property it owns or leases.

4. Pricing, scope and terms are valid for a period of 30 days from the date of submission.

5. Due to NetSPI's allocation of resources, pricing is based on the Client participating in events as scheduled. If the Client cancels, reschedules, or does not participate in scheduled events (e.g., meetings, conference calls, testing or assessment dates) without giving at least ten (10) business days' notice to NetSPI or otherwise does not meet testing requirements in time for a scheduled test, and NetSPI is unable to start testing on the originally scheduled start date due to causes described in this sentence, then NetSPI shall bill the Client a fee of £800 GBP for each day of each scheduled test that cannot be performed (the "Personnel Downtime Fee").

6. If purchased Services under G-Cloud Framework require NetSPI hardware to be shipped to complete the Services being performed, Client will be responsible for returning the hardware to NetSPI no later than 3 weeks after project completion, or a hardware fee of £1,200 GBP per device will be invoiced to Client.

Availability of Trial Service

A full unlimited Proof of Value (POV) is offered for between 2-4 weeks. This will include full access to every feature within the platform. Usage is unlimited and unrestricted within this time to give customers the full experience and value.

A POV is a great way to ensure that NetSPI's ASM solution is the right fit for your needs and delivers value to your security program. Keeping with our culture of innovation, a dialogue about features and feedback is always welcome – whether during the POV process or after you're fully onboarded as an ASM customer!

On-Boarding, Off-Boarding, Service Migration, Scope etc.

A standardised test plan includes:

- Conduct kickoff meeting
- Create security controls inventory and identify detective control boundaries through interviews
- Offline finding analysis, reporting, and quality assurance
- Report delivery

At NetSPI we have a very robust Client Delivery Management (CDM) Function. It is the CDM's responsibility to manage the delivery of all engagements post sale. This includes the following:

- Lead the planning, execution, and closure of client engagements

- Manage stakeholder expectations, engagement scope, timelines, and deliverables
- Monitor engagement progress to ensure on-time, on-budget delivery
- Identify, manage, and escalate risks
- Drive client adoption of the Resolve platform and identify opportunities for platform improvements

Migration of this proposition is N/A.

Training

Full platform training can be provided upon request as standard to facilitate onboarding of the service.

Implementation Plan

A detailed implementation and onboarding plan can be provided to the buyer on request.

Scan Monster™

Scan Monster™ automates and orchestrates NetSPI's vulnerability scanning activities, giving the penetration testers more time to manually test your applications.

Security Automation

Automation enables manual pentesters to focus on finding the hard-to-find vulnerabilities.

We offer bi-directional integrations with ticketing systems, such as Jira and Service Now, ease the remediation process.

Automatic ingestion from your data sources – even NetSPI competitors – correlates all your vulnerabilities to provide single-pane visibility.

Automatically generate and customise reports in Word, Excel, PDF and .CSV formats for easy distribution

NetSPI Open-Source Tools

NetSPI consultants dedicate time and resources to develop open-sourced tool sets that strengthen the infosec community. Here is a selection of tools that our dedicated team have developed:

- **PowerUpSQL** supports SQL Server discovery, auditing for common weak configurations, and privilege escalation on scale for internal penetration testing and red team engagements.
- **MicroBurst** includes functions and scripts that support Azure Services discovery, weak configuration auditing, and post exploitation actions such as credential dumping.
- **PowerHunt** is a modular threat hunting framework written in PowerShell that leverages PowerShell remoting for data collection at scale. Identify signs of compromise based on artifacts left behind by common MITRE ATT&CK techniques.
- **PowerHuntShares** is used to inventory, analyse, and report SMB shares configured with excessive permissions on computers in Active Directory environments. Gain a better

understanding of your SMB share attack surface, how to exploit it, and how to group results to streamline remediation.

- **Inveigh** is a PowerShell ADIDNS/LLMNR/mDNS/NBNS spoofer and man-in-the-middle tool designed to assist penetration testers/red teamers that find themselves limited to a Windows system.
- **InveighZero** is a C# LLMNR/mDNS/NBNS spoofer and man-in-the-middle tool designed to assist penetration testers/red teamers that find themselves limited to a Windows system.
- Our **wiki** is a comprehensive knowledge base for SQL injection. You'll find resources on identifying, exploiting, and escalating SQL injection vulnerabilities across database management systems.
- **PESECURITY** is a PowerShell script that displays whether images (DLLs and EXEs) are compiled with ASLR, DEP, and SafeSEH.
- **Evil SQL Client** (ESC) is an interactive .NET SQL console client that supports enhanced SQL Server discovery, access, and data exfiltration capabilities. While ESC can be a handy SQL Client for daily tasks, it was originally designed for targeting SQL Servers during penetration tests and red team engagements. The intent of the project is to provide an .exe, but also sample files for execution through mediums like msbuild and PowerShell.
- **Burp Extractor** is a one-size-fits-all tool that uses regex for extracting data from HTTP responses – such as CSRF tokens, Auth Bearer tokens, timestamps, etc. – to be reused in HTTP requests sent through Burp.
- **JSON Beautifier** is a Burp Extension for beautifying JSON output, so it is easier to view and modify unparsed JSON strings.
- **AWSSigner** looks for the "X-AMZ-Date" header in Burp requests. If it finds a request, it will update the signature in the request with your access key, secret key region and service.
- **BurpSuite: WSDLR** takes a WSDL request, parses out the operations that are associated with the targeted web service, and generates SOAP requests that can then be sent to the SOAP endpoints.
- **Tokenvator** is a .NET tool used to elevate permissions on Windows. It works by impersonating or altering authentication tokens.
- **WheresMyImplant** is tool to gain and maintain access to a target system. It can also be installed as WMI provider for covert long-term persistence.
- **SQLC2** is a PowerShell script for deploying and managing a command and control system that uses SQL Server as both the control server and the agent.
- **GODDI** dumps Active Directory domain users, groups, domain controllers, and related information into CSV output, in just a matter of seconds. It runs on both Windows and Linux.

- **Java Serial Killer** is a burp extension to perform Java Deserialisation Attacks using the ysoserial payload generator tool.
- **WebLogic Password Decryptor** is a PowerShell and Java tool to decrypt WebLogic passwords and gain access to other systems and Oracle databases
- **Invoke-ExternalDomainBruteForce** is a bruteforce tool for automated password-guessing on managed and federated domains.
- **Get-AdDecodedPassword** uses the Active Directory PowerShell Module to query Active Directory and decode UnixUserPassword, UserPassword, unicodePwd, or msSFU30Password fields.
- **GET-MSSQLALLCredentials** is a PowerShell tool to identify all MSSQL instances on a server, determine the encryption algorithm and automate credential password decryption.
- **DAFT** is a MSSQL database auditing and assessment tool written in C# that can identify non-default databases and database tables, search for sensitive data by keyword and execute SQL commands.
- **PowerSkype** is a PowerShell tool to attack federated Skype for Business instances that allows you to validate email addresses, get Skype availability, send phishing messages and more.
- **Invoke-TheHash** is a PowerShell to pass the hash WMI and SMB tasks. Authentication is performed by passing an NTLM hash into the NTLMv2 authentication protocol.
- **TellMeYourSecrets** is a C# DLL to dump LSA secrets.
- **Powermad** is a collection of PowerShell MachineAccountQuota and DNS exploit tools to launch man-in-the-middle attacks.

Our Team

While we use scanners as a baseline for our penetration testing, NetSPI's expertise is in deep-dive manual penetration testing. All of our consultants are full-time employees of NetSPI. We have over 350+ trained and certified global pentesters available to out G-Cloud clients, boasting an impressive array of industry-leading qualifications.

OFFENSIVE security OSWE
OFFENSIVE security OSCP
OFFENSIVE security OSEP
GIAC EXPLOIT RESEARCHER & ADVANCED PENETRATION TESTER GXPN
GIAC MOBILE DEVICE SECURITY ANALYST GMOB
ZERO-POINT SECURITY RED TEAM OPS
CISSP®
EC-Council CERTIFIED C|EH
CREST REGISTERED TESTER CRT
aws certified Cloud Practitioner FOUNDATIONAL

Service Management

When you work with NetSPI, you get a programmatic approach with strategic guidance. Our white glove customer support and advisory programs work together to help deliver successful outcomes. Our dedicated NetSPI ASM security experts are comprised of in-house pentesters that help augment your security team and prioritise what matters most for remediation.

Accelerate remediation efforts by assigning SLAs and designated remediators to vulnerabilities and manage them through the remediation life cycle. You can supplement NetSPI's assigned severity with your own rating allowing further customisation of the vulnerability management process. Also, when remediations are complete, you can flag a vulnerability "Ready for Retest" which lets our team know it is time to validate remediations were successful.

Service Levels

Service Level Agreements to be agreed depending on contract structure. Typically, our support hours are standard business hours of the region the contract is signed in or where the service is to be utilised, unless agreed otherwise. SLA's will be confirmed prior to an order being placed which will documented in the SOW and T&Cs where applicable.

4. Provision of the service

Customer Responsibilities

No setup or specialised systems required

All we need is one domain, and your company will be on its way to improved security. We scan your external perimeter in the same ways that malicious attackers do, using an external and unauthenticated approach, to discovering assets and exposures. NetSPI ASM does not require downloads, specialised configurations, or any other environment changes to begin working. Our ASM security experts work with you for fast and easy onboarding so you and your team can start using NetSPI ASM almost immediately, delivering a fast time to value.

Technical Requirements and Client-Side Requirements

One point of contact that can be present during testing who can provide feedback on what security events are generating logs and alerts.

1. Provide in-scope IP ranges and/or domains for more comprehensive testing.

2. Provide only your core domain and see what the platform and team can discover with the limited information.

After-sales Account Management

At NetSPI we have a very robust Client Delivery Management (CDM) Function. It is the CDM's responsibility to manage the delivery of all engagements post sale. This includes the following:

- Lead the planning, execution, and closure of client engagements
- Manage stakeholder expectations, engagement scope, timelines, and deliverables
- Monitor engagement progress to ensure on-time, on-budget delivery
- Identify, manage, and escalate risks

- Drive client adoption of the Resolve platform and identify opportunities for platform improvement

5. Our experience

Case Studies

As a practice, NetSPI does not provide references due to the nature of our business; organisations that we work with prefer to keep our collaboration private. That said, we will work with each contract owner to facilitate discussions with our clients if needed. We also have publicly available case studies presented on our website at www.netspi.com/case-studies

Contact Details

For more information or to speak with our G-Cloud team, get in touch today:

E: publicsectorenquiries@netspi.co.uk