NISOS

Services Brief

External Attack Surface Monitoring and Analysis

Outside-In contextualized intelligence that augments your current security and IT teams

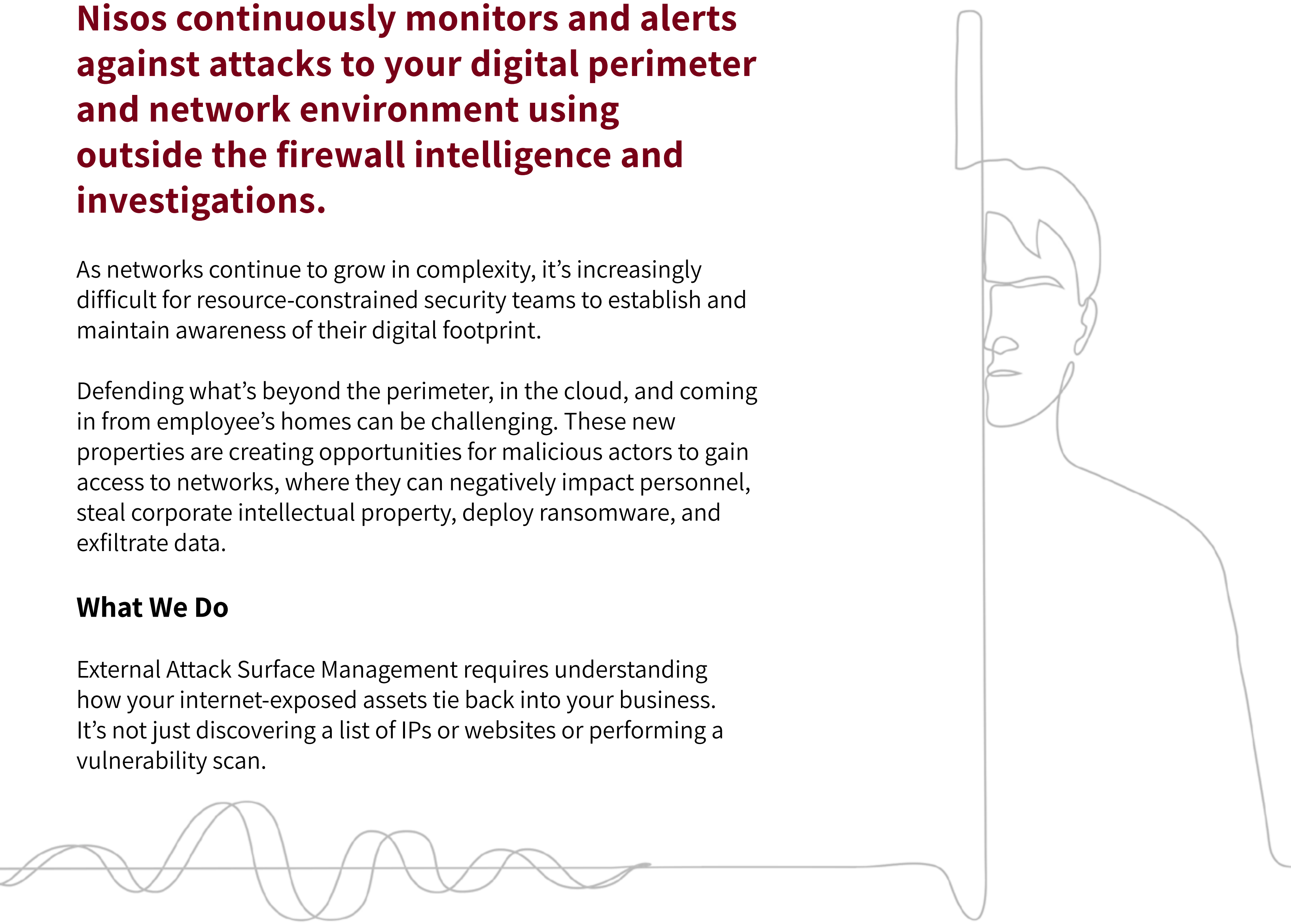
Nisos continuously monitors and alerts against attacks to your digital perimeter and network environment using outside the firewall intelligence and investigations.

As networks continue to grow in complexity, it's increasingly difficult for resource-constrained security teams to establish and maintain awareness of their digital footprint.

Defending what's beyond the perimeter, in the cloud, and coming in from employee's homes can be challenging. These new properties are creating opportunities for malicious actors to gain access to networks, where they can negatively impact personnel, steal corporate intellectual property, deploy ransomware, and exfiltrate data.

What We Do

External Attack Surface Management requires understanding how your internet-exposed assets tie back into your business. It's not just discovering a list of IPs or websites or performing a vulnerability scan.



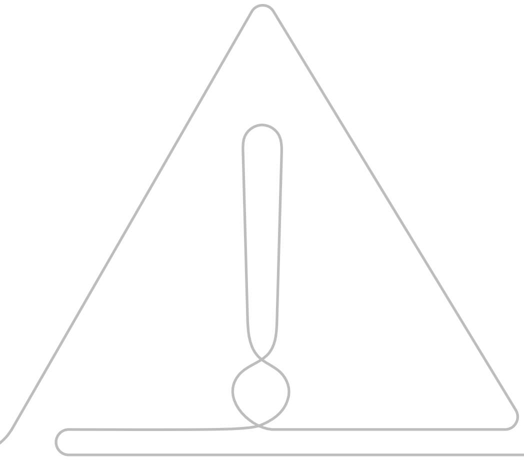
Can you currently answer:

- If an attacker gets in, what infrastructure would they communicate to?
- If an employee uses unsanctioned applications, can you identify which ones they are, which device they've used to access them, and which office from which they were accessed?
- What vulnerabilities exist, where are they, how might they be exploited, and were they exploited in the past?

Remedy Alert Fatigue for IT/Security Teams

A common challenge created by “traditional ASM platforms” is “discovery overload”. These systems find assets and applications and assign individual alerts that require attention and potential remediation. Many vendors leverage the insufficient data to upsell vulnerability management services, continuous attack simulations or red teaming.

Nisos doesn’t flood you with random alerts. We provide a prioritized list of critical alerts so that you can delve deeper into what really matters. Rely on a team of world class analysts with previous experience working at United States Government intelligence agencies.



How it Works and Service Features

- Client-specific monitoring and analysis led by highly experienced human analysts, not one-size-fits-all platforms
- Combination of asset discovery, shadow IT, Threat Actor Infrastructure, and global netflow traffic analysis
- Real-time map office locations with dynamic external IPs/domains to enrich context to attacks that matter to you
- Meaningful reports with a focus on actionability for IT and Security Teams
- Up and running in seconds, gaining insights without requiring network access
- Full picture of external cyber business risk exposure via holistic non-machine-driven workflow and analysis

Domain of Interest Profile

Netflow Review of Domain or IP

IP/Domain Attribution

Threat Actor Infrastructure Profile

External Network Hygiene Assessment

Insider Threat Indicators, including data leakage and individual motivations

Multi-language Support

Data Sources

Nisos enriches data into actionable intelligence that informs and establishes priorities for the SOC, threat hunting, vulnerability management, red team, application security, security engineering team, and business units.

Network & Telephony

- Anonymous Infrastructure
- DNS and WHOIS
- Internet Netflow (90%+ of IPV4)
- Mobile and IP Geolocation
- Threat Feeds

Web & Social

- Deep and Dark Web
- Foreign Media
- Historical Web Content
- Open Web
- Social Media

Human

- Closed Forum
- Deep and Dark Web

Media

- Domestic News
- Foreign Media

Adversaries

- Activist
- Disinformation
- E-Crime
- Nation State
- Political

Breach

- 20+ billion records of legally acquired datasets including PII, selectors, and information/credentials

Businesses

- Business Registrations
- Corporate Filings
- Corporate Profiles
- Public Records

Persons & Groups

- Biographical
- Civil and Criminal Actions
- Email and Identity
- Investigative Databases
- Public Records

External Threat Hunting

Using a combination of over 20 technical datasets we actively hunt for who is targeting you and how future actors could exploit network weaknesses.

This is not a vulnerability scan. It is a research and analysis operation with the objective of identifying and monitoring your digital attack surface and providing contextually derived recommendations for reducing exposure.

It is an active analysis of technical data to identify actual threats you are facing. With this information, you can augment security controls to maintain confidentiality, integrity, and availability of data, systems, and networks.

Use Cases for External Threat Hunting:

Identify ransomware command and control

Track advanced actor reconnaissance over time

Identify insider threat indicators

Uncover negligent out-of-policy data sharing

The Nisos Experience

Discovery and Validation

We automate and positively identify network infrastructure for the client. We discover corporate connections to cloud service providers and distributed infrastructure. We typically inquire about all external domains and IPs owned by the client, but we can execute simply with a domain name. **We do not need any internal network access.**

Vulnerable and Exploitable Services

We monitor for the following external-facing risks for clients:

- Shadow IT or applications used by another department out of corporate policy. This includes internal and external security and IT products that are in use.
- Malicious insider threat traffic flows coming from internal networks.
- Geographic or business unit-based differences in security maturity across the company. This includes domain workstations that appear to be directly connected to the internet with no firewall on a VPN connection.
- Vulnerable applications outside of patch management cycles, which includes insights about patches and security protocol maturity.
- WAN and MPLS network infrastructure mapped by office and employee location. This includes network ingress and egress points and potential insights on the efficacy of malware mitigation strategies.

External Threat Hunting

Nisos reviews for malicious command and control from external actors. This includes malware infection frequency and duration and indicators of current of past breaches. We highlight indicators of compromise and selector enrichment, which includes: infrastructure being used by the actor, information about other organizations possibly affected by the attack, and tool and TTP attribution. We also cross reference OSINT intelligence holdings, plus geopolitical, social media, and geolocational contextual analysis.

Notifications and Alerts

Nisos augments your team, providing additional eyes and ears from an outside-in approach, alerting clients of the potential for malicious activity that is contextualized to your specific risks.

Intended Outcomes

Our definition of success is when your team can take action against each finding and ensure the confidentiality, integrity, and availability of data, systems, and networks as a result. Nisos will identify vulnerabilities and provide details of likelihood/ease of potential exploitation. We will identify actual attacker reconnaissance of your network and provide further context by outlining exploitation or access attempts made based on collection tasking.

Context for On-Network Telemetry, If Necessary

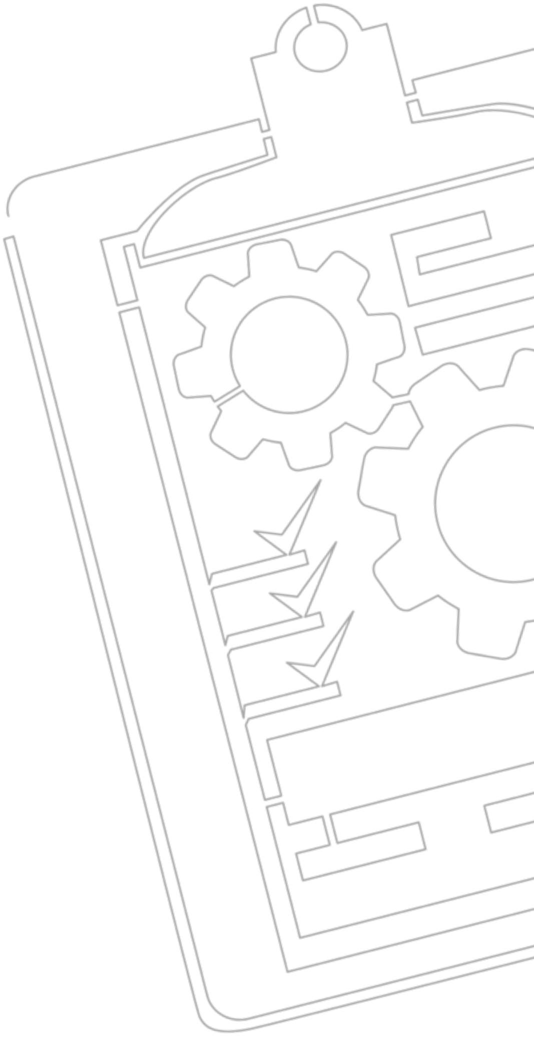
We conduct external threat hunting and forensics investigations on a variety of security events and incidents. By combining our core capabilities with on-network forensics investigations, we have the ability to bring more actionable context, resolution, and remediation to security events before a breach occurs.

Deliverables

Nisos provides subscription monitoring that reduces your alert fatigue and reporting that security practitioners don’t have the time to get to. We also make guarantees of actionability to protect your people, your business, your customers, and your assets with rapid and curated responses to intelligence questions and concerns.

Reports available:

- **Situation Briefing:** Monthly summary status report of trends and activity observed by Nisos researchers and analysts
- **Spot Report:** A supplemental brief used to quickly communicate time-sensitive intelligence for significant events impacting a client



About Nisos

Nisos is the Managed Intelligence Company™. Our services enable security, intelligence, and trust and safety teams to leverage a world-class intelligence capability tailored to their needs. We fuse robust data collection with a deep understanding of the adversarial mindset delivering smarter defense and more effective response against advanced cyber attacks, disinformation, and abuse of digital platforms.

Learn More: nisos.com | email: info@nisos.com | 703-382-8400