NISOS

Capability Brief

Threat Landscape Assessment

Analysis of the external threats you face to provide an assessment of the level of risk and identify methods of mitigation

As your enterprise security team grows, you have an increasing need to understand risks beyond your network perimeter. Nisos' assessment looks at these risks based on the activity of your adversaries.

We use our intelligence collection and analysis expertise to increase visibility, identify risk, and prioritize mitigation steps. Nisos' threat assessments provide unparalleled visibility beyond the perimeter into physical security, cybersecurity, fraud, and trust and safety threats to provide actionable intelligence and prioritize mitigation recommendations.

Our Approach

Unlike the traditional threat intelligence approach of delivering large datasets which are not customized to your threat surface, Nisos uses our vast multi-source collection capability to uncover threats specific to your business. Then we perform expert analysis on the risks most relevant to your organization.

This approach provides unique visibility into the activities of a wider range of adversaries that includes threat actors not traditionally tracked by threat intelligence collection methods.

Providing these insights into your threat landscape allows you to set intelligence priorities, identify collection strategies, track mitigation activities, and reduce risk.

Nisos Assessments are Different.

We possess a broad and differentiated collection capability that , when coupled with our expert adversarial mindset, provides you with the intelligence necessary to detect and disrupt your adversaries.

Even when lacking an obvious internal starting point, we are able to combine our external telemetry with client-specific internal telemetry to provide insight.

What We Do

Security teams are constantly confronted with new and evolving threats in the areas of physical security, cybersecurity, fraud, and trust and safety. A Nisos Threat Landscape Assessment identifies digital and physical threats enabling you to establish a baseline and a plan for ongoing threat mitigation.

Digital Threat Assessment

Brand and Product Threats

- Fraud
- Violation of acceptable use (hate groups)
- Rogue applications and account takeover
- Domain and application spoofing

Breach and Data Leaks

- Exposed credentials and key personnel
- Solicitation or sale of stolen IP
- Breach and network compromise threats
- Code or data in file sharing sites

Technical Threat Analysis

- Cybersecurity asset identification and attack surface mapping
- Vulnerability Management
- Malicious network traffic identification
- Attack emulation

Physical Threat Assessment

Negative Sentiment Analysis

- Disinformation
- Ideological opposition groups
- Sentiment that inspires real-world harm

Country Risk Indicators

- IP theft
- Digital surveillance
- Criminal activity

People and Property Threats

- Threats to executives and key personnel
- Threats to physical locations
- Insider threat indications

Deliverables

A comprehensive Threat Landscape Assessment Report addressing the digital and physical threats outlined above. The vulnerabilities and threats identified will be categorized by the level of severity and impact. We will also identify methods for mitigating these threats. Our goal is to provide tangible and practical data that will assist clients in prioritizing resources as they expand their security programs.