NISOS
Webinar Brief

The World Has a Threat Intelligence Problem

Executive Summary

Starting around 2010, combating cyber crime and nation state cyber-driven espionage became a national priority. This initiative was a shared responsibility. A third of it was owned by the US intelligence community, a third by federal law enforcement, and a third by the private sector. As a result, the private companies in the threat intelligence industry now account for a market capitalization in excess of $6 billion according to Gartner analysis.

The threat intelligence market emerged, consisting largely of vendors building datasets and feeds that offer insight into existing threats, but offer minimal differentiation.

Unfortunately, these feeds are large and generic and do not address client-specific threat requirements. They generate a lot of "noise" and rarely deliver a justifiable return on investment for enterprise security teams. The need for customized, but scalable, threat intelligence solutions has emerged as a requirement for mature intelligence consumers. As a result, risk-based approaches to address client-specific requirements for threats are more critical than ever, paving the way for more automated and managed intelligence services.

Information and Data are Not Intelligence

Outside of the financial sector, which has hired experts and modeled cybersecurity risks, most enterprise security teams do not have standardized intelligence requirements.

Intelligence feeds, which consist of data and information are typically not useful without an understanding of the unique needs of the business. Until recently, threat intelligence vendors have operated on an "editor in chief" model of providing generalized intelligence that appeals to the broadest spectrum of potential customers and industries. The model has provided insight for organizations focused on known threat actors and known TTPs, advanced espionage activities, or common ecrime attacks. This model does not address more nuanced and client-specific requirements. However, there is a new intelligence model emerging that addresses problems unique to individual organizations.

Scaling Risk-based Approach to Threat Intelligence Needed for Consumers

Some vendors are now adapting threat intelligence solutions to risk-based approaches that identify and analyze threats targeting specific businesses or platforms. This new model allows clients to direct the focus of intelligence and is supported by vendors that analyze and correlate a wide range of appropriate datasets. The capabilities required by the client are evolving and are at various stages of maturity. Key capabilities include:

- **IOCs to SIEM:** Indicators of compromise being funneled to a SIEM to determine network device compromise. This is currently addressed by many vendors.
- **Control Pressure Index:** Security controls likely to be targeted and used over a time period based on threat actor activity. This is maturing by vendors and ripe for managed services.
- **Digital OSINT and External Attack Surface Monitoring:** Monitoring a company's perimeter and attack surface as well as it's reputation on the open and dark web.
- **Requests for Information:** The ability to deliver customized reporting in a moment's notice that answers a client's specific needs. This is maturing by vendors and ripe for managed services.

The Need for Increased Automation and Managed Services

Enterprise intelligence needs are growing and becoming more clearly defined, thus as a result we are seeing increased automation and the emerging vendors that are delivering intelligence as managed services. For many enterprises, security operations has become a cost center and as a result, companies are increasingly price-conscious while also concerned about the conflicting requirement to gain access to highly-specialized and skilled intelligence analysts and experts.

Solving the Intelligence Problem with Managed Services

Given the abundance of data feeds, the increasing need for automation, and the worldwide cybersecurity and intelligence skills shortage, Managed Intelligence is the most viable option for many organizations, regardless of size. Managed Intelligence capabilities have expanded and now address problems present in virtually every intelligence domain including: cyber threat intelligence, protective intelligence, platform intelligence, fraud intelligence, reputation intelligence, third-party and supply chain intelligence, and merger and acquisition diligence.

About Nisos

Nisos is the Managed Intelligence Company™. Our services enable security, intelligence, and trust & 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. For more information visit: **www.nisos.com**