NISOS

Webinar Brief

The Technology Stack: Requirements, Data Acquisition, Vendor Evaluation, Analysis, and RFIs

Executive Summary

In this webinar, cybersecurity leaders from IBM, Expedia Group, Thomson Reuters, and Nisos discuss the challenges and opportunities they see with today's technology stacks as it pertains to successfully launching and maintaining a robust threat intelligence program.

From engaging and wrangling stakeholders, to recruiting and keeping the right people, to vetting sources of information, to weighing the pros and cons of working with inhouse talent or outsourcing to a Managed Intelligence provider - this panel of experts discussed the opportunities and challenges faced today in getting answers to Requests for Information and survival in today's evolving threat landscape.

Understand Business Requirements

When launching an enterprise intelligence program, there are many things you need to assess, such as revenue drivers, technologies, processes that drive the technologies, and the strategic direction of the business are all critical aspects to include in your planning.

The requirements of different departments and community stakeholders are also going to be different and may compete with one another for priority. Stakeholders within groups responsible for incident response, vulnerability management, payment card and supplier fraud, marketing, as well as your general counsel must be engaged.

Expectations must be set and challenges outlined. Retail customers might care about common TTPs of ransomware actors while energy clients might be concerned with a threat actor's ability to impact operations. Compromise and prioritization for what the enterprise needs most will be crucial.

Identify Appropriate Skill Sets

Diverse skill sets are important to any intelligence program. Successful intelligence teams often combine analysts from both the public and private sectors. Teams can also benefit from skills related to journalism, data engineering, forensics, network analysis, and computer network exploitation.

Personalities also play a role as teams often benefit when people who are risk averse interact with people that are natural risk takers. Similar benefits are realized when both strategic and technical individuals play a role.

Determining the optimal makeup of your team is based largely on the goals of your program. If a program is going to be focused on Security Operations Center cybersecurity requirements, you will require highly technical skill sets. If a program is going to be focused on broad geopolitical or competitive intelligence threats (ex. Chinese interests in AI technology), the team will require more strategic thinkers.

Cross training is both a benefit and a requirement for any successful intelligence program. A good intelligence analyst, particularly a good cyber threat intelligence analyst, must be able to contextualize what is important to an organization. Therefore skills ranging from security engineering knowledge to investigative experience, to journalist-level writing skills all play a role in an intelligent team's success. Engineering diversity is also important as the abilities to collect, ETL, and present data in a front-end user interface require very different skillets.

Evaluate Data Options

Organizations must consider the specific intelligence needs of their business, the risks they wish to pursue, and the degree to which they will pursue them. Once goals and requirements are established, an intelligence program must identify the proper datasets and feeds to meet those needs. Then the datasets must be ingested, aggregated, and engineered before an analyst can query or set alerts.

Data needs to be augmented with internal telemetry. This provides finished intelligence as well as the raw data from an API and/or GUI. The cost and return on investment for all datasets should be diligently tracked to ensure the team optimizes resources and budgets.

Data categories that are relevant across all risk types and against all threat actor types include:

- **Business:** Information about U.S. and foreign corporations
- **Network and Telephony:** External telemetry such as PDNS, malware samples (Virus Total), dark web, open web, domains, netflow, mobile data, and false positive aggregator (events not worth an analyst's attention)
- **Persons and Groups:** Data solutions providers specializing in custom, scalable investigative and risk management tools for due diligence, threat assessment, identity verification, fraud prevention and debt recovery
- **Web and Social:** Social media, dark web, news media, and foreign media

Consider Buy vs. Build

Building an internal intelligence team is a daunting proposition that will be driven by 3 parameters:

- The level of threats to the business
- The resources to fund the program and
- The ability to staff and retain the required roles

For many organizations, outsourcing managed intelligence to a managed service provider is attractive for the following reasons:

1. Many customer-oriented threat intelligence programs (not solutions providers) are not a profit-and-loss driver
2. Managed service providers can offer early "wins" while the intelligence program attempts to hire the required analytical and engineering skill sets internally

3. Intelligence expertise is in high demand and difficult to hire and retain. Specialized providers can provide this experienced and diverse talent.

4. Feeds and datasets are expensive and differences between vendors can be difficult to quantify. Specialized providers have already done the evaluation, built an optimized dataset, and have experience using it.

5. Best-in-class providers allow the client to drive information requests that are client-specific and valuable to the organization. They can provide the unique answers you seek in professional custom reports.

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**