NISOS
Webinar Brief

Workshop - Lessons from the Field: Building a Cyber Threat Intelligence Program

Main Takeaways

- Creating an intelligence program foundation can be as straightforward as asking good questions and listening to your consumers of intelligence.
- There are multiple ways to approach structuring your program, which will depend on your personal objectives and your company's needs.

Executive Summary

Intelligence is essential to understanding and mitigating threats. Businesses today are recognizing the value in creating a strong cyber threat intelligence program. By differentiating raw data from organization-specific intelligence, businesses can form a robust foundation that will help security leaders to secure funds and retain/attract personnel. When done effectively, these intelligence programs can become a multiplier for a variety of teams within an organization.

Creating Consumers of Intelligence

Delivering insights and opening communication channels between various stakeholders is essential for navigating the differences between perception and reality around what threat intelligence really is. Starting with the basic definition of what intelligence and using an educational approach can be very effective. Start by developing an understanding of the spectrum of actionability. Next, create internal collateral to help spread awareness. Last, gather insights from your consumers to adapt your future discussions.

Planning Considerations

The depth and complexity of planning can vary greatly from one organization to another; however, it's important to build a strong foundation for your intelligence program in order to

get leadership buy-in, approval for budget, and staffing. Your planning should take into consideration the data collection types you need, the analysis tools and threat intelligence platform you have to support your full team of analysts, and the ways you should deliver this intelligence. The dissemination of intelligence will also be dependent on the capabilities of your organization for the frequency of assessments, monitoring, and investigations.

Collection: Various data sources can contribute to your intelligence program however, not all data sources provide the same value to your unique program. Organizing your data by groups can help you communicate with leadership and internal customers the insights and actionability of each intelligence source.

Analysis: The people and the tools needed to aggregate, conduct analysis, and integrate data collections into your intelligence program will play a large role in how robust your analysis can be. Without the proper talent and tooling, the finished intelligence product can sometimes fail to answer the questions consumers of intelligence need to see the value of these information streams.

Dissemination: Dissemination can be approached in several ways. From low tech and low effort to high tech and with robust insights. How you share will also be dependent on the level of analytic in-house or out-sourced talent you have.

Managing Expectations

Intelligence programs will look different depending on the diverse needs of each organization. Engaging stakeholders across the organization by meeting their needs will help you succeed in developing strong advocates for your initiatives and informed consumers who can support your objectives.

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 cyberattacks, disinformation, and abuse of digital platforms. For more information visit: **www.nisos.com**

This briefing is not legal advice and is provided for general informational purposes only.