State of Threat Intelligence

Highlights from a Roundtable hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Recorded Future, March 2024

Amidst relentless cyber attacks, government agencies must quickly identify and neutralize the most relevant threats. Participants at this roundtable explored the criticality of threat intelligence on a robust cybersecurity posture. Panelists offered insights into threat landscape strategies and discussed ways to integrate threat intelligence into cyber security programs.

Current Status of CTI

Emerging technologies are rapidly reshaping the Government's cybersecurity landscape. For agencies to successfully guard against threats in this dynamic environment, they must prioritize threat intelligence. Infusing cyber threat intelligence (CTI) into all aspects of cyber operations provides agencies with visibility into ever-evolving threats and the capacity to scale defenses. CTI extends beyond simple threat indicators by offering a comprehensive understanding of the threat lifecycle, which enables agencies to better prioritize cyber security efforts.

> **"It's imperative to take an intelligence infused approach to cyber operations."**

For several panelists, building threat intelligence capabilities starts with a dedicated cyber intelligence team. Unlike other IT professionals, cyber threat analysts bring a distinct analytical mindset to the role and a strategic perspective. This enables them to effectively interpret a complex, ever-evolving threat environment influenced by a myriad of factors, including geopolitical events.

More agencies are adopting a comprehensive approach to threat intelligence and considering its impact across strategic, operational, and tactical levels of the organization. Its imperative agencies understand how threat intelligence integrates into an organization.

One panelist notes that most agencies limit their threat intelligence efforts to fortifying perimeter defenses and identifying threats, but an often overlooked – yet critical – aspect to threat intelligence is the dissemination of intel throughout the organization. Effective dissemination enables valuable feedback that helps to assess the strength of defenses and the quality of the intel itself.

Sharing Intel

Sharing threat intelligence across Federal agencies is a known challenge, but panelists agree that modals for sharing intel are improving. Currently, CISA plays a central role with the Automated Indicator Sharing Sharing Program (AIS), which offers threat data for both government and public audiences.

Some agencies have shifted towards department-level information sharing, which is facilitated through a "team of teams" organizational structure. This has helped the agency cutrate intelligence based on their unique needs and priorities.

One panelist notes that traditional email is an inefficient way of disseminating threat intelligence due to the sheer volume of information. Agencies must be savvy with how they communicate intel due to the threat of information fatigue, and should focus on communicating only the most actionable, relevant insights. It's the actionable insights that lead to tangible improvements in an agency's cybersecurity posture.

Challenges with Federal Government Threat Intelligence

- Keeping pace with a rapidly shifting threat landscape. The sheer volume and dynamic nature of threats pose a significant challenge to federal agencies, regardless of size and resources.
- Lack of actionable data. While agencies excel at data collection, the data is often not relevant to an agency's specific risk profile.
- Data vs. Intelligence. Discerning between data and actionable intelligence is a key challenge for agencies.
- Challenges for smaller agencies. With limited budgets and few personnel, smaller agencies have limited threat intelligence capabilities. However, despite these challenges smaller agencies cannot forgo threat intelligence. Panelists recommend outsourcing to effectively manage CTI.

Using CTI Data to Streamline Data Management

> **"The delineation between data as intelligence is context."**

Panelists were asked if threat intelligence data could help agencies understand what additional information they needed for a more complete threat profile.

One panelist offered a slightly different paradigm to address this question, explaining that they prioritize intelligence gathering based on agency mission. They developed a list of the most relevant threat actors based on their specific mission, and focused their initial CTI efforts on mission-critical threats.

Another panelist recommends pinpointing the types of attacks an agency faces most frequently and to continuously evaluate the effectiveness of the defenses against those threats. As agencies gather threat intelligence unique to their infrastructure and threat profile, they can begin to consistently apply it to strengthen their defenses.

Challenges of Supply Chain Threat Management

Due to its complexity, supply chain threat management is different from managing internal cyber security threats. Supply chain threat management involves assessing risks that lie outside of an agency's direct control, such as geopolitical factors.

Some of the challenges with supply chain threat management include:

- **Lack of visibility.** It's challenging for agencies to gain a comprehensive understanding of their entire supply chain, especially beyond the first few levels.
- **Complexity and scale**. The global, interdependent nature of technology supply chains makes conducting a thorough analysis immensely difficult.
- **Foreign influence.** Supply chain risk assessments must address the complex considerations of foreign ownership, control, and influence, which may be out of scope for an acquisition specialist.
- **Unique risk postures.** Each agency must tailor its supply chain risk management based on its unique mission and attack surface, but also non-cyber related constraints.

Strategies for Assessing Supply Chain Risks

Panelists shared that tackling supply chain risks typically depends on collaboration between organizations due to the complexity and pervasiveness of supply chain threats. Here are specific strategies panelists offered to assess supply chain risks:

- **Information sharing**. Collaborating with other agencies and sharing intel reduces redundant efforts, which is imperative in this rapidly changing environment.
- **Prioritize certain vendors.** Agencies should prioritize vendors with demonstrably strong cybersecurity and cyber hygiene practices.
- **Integrate CTI into the ATO process**. Making threat assessment an integral part of the ATO process helps ensure risk management is incorporated at every level.

Adapting to Emerging Risks

In the wake of ever-evolving threats, panelists discussed strategies to adapt their threat intelligence programs. They recommend continuously assessing an agency's unique threat surface to pinpoint weak areas to base defenses. Shifting towards a risk-based approach to prioritize patches and other security measures can help address more relevant threats to the organization.

Panelists encourage agencies to invest in skills development for cyber teams, particularly for smaller organizations. Similarly, agencies should build threat intelligence teams composed of analysts who think like attackers. These teams should excel in curating multiple sources of intelligence, developing actionable insights, and applying them to other processes.

Key Takeaways

> **"The Government does an excellent job of collecting data. It's imperative we turn that data into actionable intelligence."**

- Investing in dedicated intelligence analysts embedded within cyber programs is critical if agencies are to embrace an intelligence-driven cyber operations model.
- Outsourcing intelligence from companies like Recorded Future can help smaller organizations who lack resources for in-house analysts.
- Adopting an intelligence-driven approach to cybersecurity is no longer optional. Agencies must be proactive with their threat intelligence to reduce vulnerabilities and take action ahead of attacks.
- Agencies must ensure they have not only the right tools, but also the personnel with the expertise to interpret threat intelligence and can translate technical threat intelligence insights into clear, actionable explanations for non-technical stakeholders.