International Government Agency Strengthens Cyber Security Program with Intelligence-Led Services

Government networks and their infrastructures are under an unending barrage of ever-changing attacks from hacktivists, nation states, and cyber criminals. Attacks evolve daily, tasking government cyber defense programs to advance their capabilities.

With a comprehensive cyber threat intelligence (CTI) function, an organization can anticipate, prepare for and respond more effectively to sophisticated cyber attacks. Threat intelligence increases an organization's knowledge and understanding of attacker profiles, motivations, intentions, characteristics and methods.

Breach discovery prompts CTI assessment

During an investigation of the cyber-criminal underground, evidence of a government agency breach was discovered. While the agency had a security operations center (SOC) in place, and recently formed an ad-hoc CTI function, this unexpected incident caused the CISO to become aware of the existing cyber security program's limitations.

Recognizing the importance of establishing a structured CTI function to inform security operations, the agency engaged Mandiant, a FireEye company, to assess the maturity level, operational state, processes and strategy of its CTI capabilities. The objectives of this engagement were to:

- Enhance the agency's foundational CTI practices, including business-related cyber intelligence consumption, processing, analysis and production, along with dissemination to stakeholders
- Implement a sustainable model for using threat intelligence
- Train the agency's security team to operate as an effectively coordinated unit

The project, conducted over four months, involved tactical and strategic resources from the following functions across the enterprise: security operations (including incident response and vulnerability management), cyber threat intelligence, governance, compliance, engineering and network infrastructure.

Prioritizing threats

As an initial step, Mandiant consultants profiled all cyber threats facing the agency, providing a clear understanding of which critical assets they needed to protect. Together, Mandiant and the agency outlined specific areas of the agency's operations that attackers would most likely pursue, including payment processing systems, personally identifiable information (PII) and intellectual property (IP).

This profiling exercise helped the agency prioritize attack types that allowed Mandiant consultants to make sound recommendations for aligning security resources and technologies that support the identified high-priority assets.

The resulting findings and recommendations allowed the CISO to better align security resources across the function — without increasing headcount or budget.

FireEye

Applying a requirements-driven approach

The agency's original security posture was reactive — they only engaged attacks after one was identified. This drastically hampered the team's ability to consistently produce usable cyber intelligence for the larger organization. To develop proactive, structured and repeatable processes, Mandiant experts introduced a CTI function framework for the agency to implement.

Their existing framework was evaluated against a CTI function maturity model containing six core domains to identify areas of improvement (Fig. 1). For example, the agency's internally-built CTI function lacked visibility into the larger organization's intelligence requirements — which meant that the collection of threat intelligence was ineffective and did not meet the agency's specific needs. This functional assessment shed light on the need to align their data collection process with stated requirements, and helped eliminate nonessential data sources from daily operations.

Improving stakeholder engagement

The agency's existing cyber security function was created in isolation, without engaging other areas of the organization. Therefore, the team was unable to reach or properly work with other business functions to effectively resolve cyber events. After exploring the differing needs of various business partners, Mandiant experts created a stakeholder analysis framework designed to improve engagement by highlighting how CTI could be used across the organization.

This stakeholder framework created internal partnerships between functions such as security architecture, operations, risk management and other related teams.

These strategic partnerships allowed teams to share information more effectively and gave the CTI function a better view into the larger organization's daily operations.

As a result, the agency's CTI function better aligned its processes with organizational goals and was able to provide proactive, relevant and usable intelligence to business lines and stakeholders. The function is now embedded in strategic areas of the organization and positions the security team as a proactive, intelligence-led function.

Aligning program resources

The agency's CTI team estimated that more than 80% of their time was spent on vulnerability management activities — not only researching vulnerabilities, but also performing vulnerability scans and maintaining the respective technology. While the CTI team needed to inform the vulnerability management processes with, for example, high-priority threat data, actual scans of the environment and search tool maintenance was outside of their remit. The agency was seeking CTI team headcount to address these needs; Mandiant consultants recommended they refocus their team and agency mission around cyber intelligence instead.

The workflows and processes of the agency's CTI function were assessed to gauge existing resource allocations. The assessment findings allowed the CISO to better align resources across the comprehensive security function — without increasing headcount or budget. This new alignment transformed their approach by rallying the team around a modified strategic mission — to provide senior leadership and key stakeholders with cyber threat intelligence that enables better decision-making and reduces overall business risk.

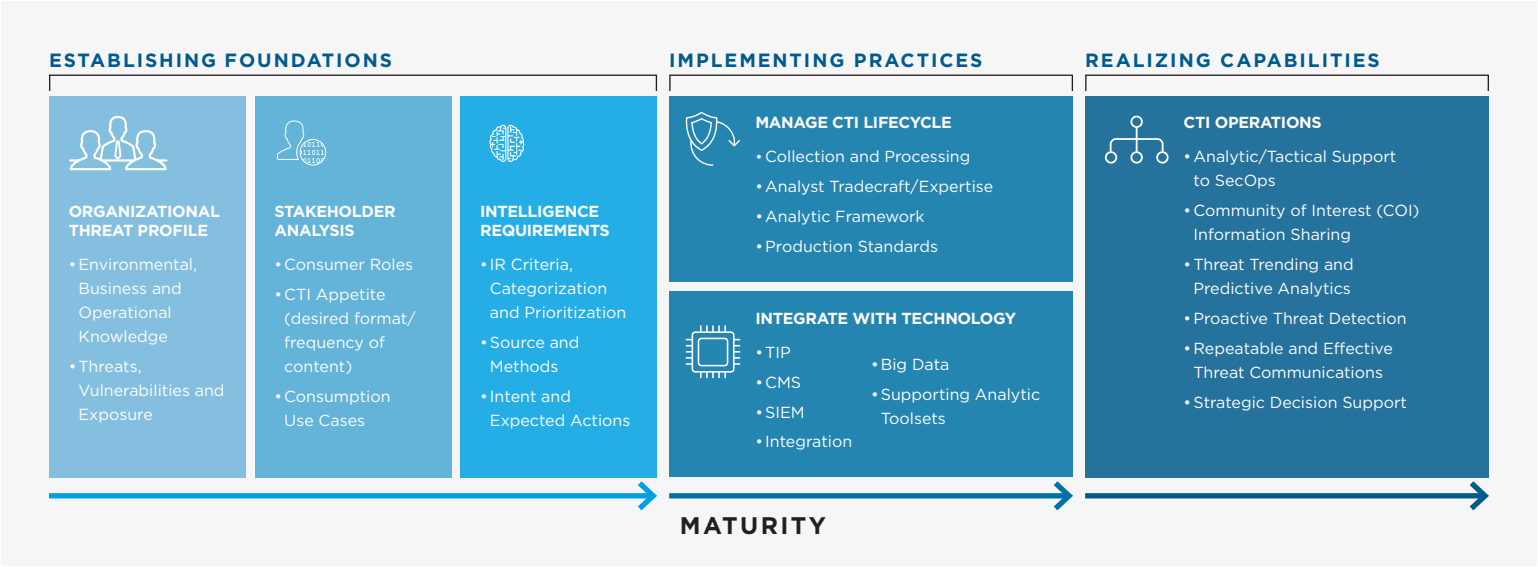

Figure 1. The CTI function framework ensures structured and repeatable collection, analysis and dissemination of threat intelligence.

Implementing a mission-focused structure

Originally, the agency's CTI function reported to the SOC director. This approach wasn't necessarily wrong, but in this case, the agency focused solely on SOC departmental needs instead of larger organizational concerns, with unclear staff roles and responsibilities.

Mandiant consultants recommended that the security team's CTI function should report directly to the CISO. Restructuring under the CISO better integrated the CTI team with the rest of the organization and refocused CTI roles and responsibilities to align with the agency's security practices. With a coordinated, intelligence-led mindset, and a leader (the CISO) who established CTI as a security priority, cyber incidents could now be scoped more effectively by better understanding potential impact and allowing incident response (IR) teams to execute the right remediation activities.

To sustain the new organizational structure, Mandiant experts created a skills and capabilities matrix aligned to the agency's functional requirements. This ensured the team's skillsets and subject matter expertise continued to mature.

Enhancing analytical and tactical skills

During the four-month engagement, Mandiant conducted workshops on analytic tradecraft and hunt mission tactics for the CTI team. Analytic tradecraft helped the agency use analytic techniques and standards to identify relevant threats and communicate those threats consistently across the agency. Hunt mission tactics enhanced the agency's threat detection capabilities, forging a repeatable process that leveraged intelligence to identify threat activity within the specified environment.

To optimize operational integration of these new methodologies, Mandiant experts defined specific threat hunting use cases. These use cases helped the agency's CTI team become more confident in their ability to detect and remediate cyber incidents that could lead to breach of confidential payment systems, personally identifiable information (PII), and intellectual property (IP).

In Conclusion

Before their engagement with Mandiant, the agency struggled to manage an effective CTI function that could contribute to operational success. They lacked the ability and reliable processes required to identify, manage and communicate useful cyber intelligence to security operations and the broader agency.

Mandiant experts developed a CTI function blueprint that formalized the agency's cyber security initiatives and strengthened its overall cyber security posture. As a result, the CISO and team:

- Refocused their strategic mission on providing senior leaders with better decision-making and risk-reducing intelligence
- Employed enhanced and long-term foundational CTI practices to align CTI consumption with agency threat realities and individual stakeholder needs
- Created a model for maturing and sustaining the newly shaped CTI function
- Optimized the identification, prioritization, and detection of cyber threats
- Enriched threat communications across the business to meet stakeholder needs and concerns
- Implemented a new reporting structure to align security responsibilities with the larger organization
- Adopted sophisticated techniques for identifying, communicating and remediating various threats

Today, the agency is fully prepared to gather and utilize cyber threat intelligence to help combat the ever-evolving cyber attacks that threaten organizations each and every day.

For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035 tel: 408.321.6300 / 877 FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye® is the leader in intelligence-led security-as-a-service. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye