KPMG

Cyber threat intelligence

Moving cyber security to the heart of our business

March 2017

kpmg.com

Why you should care about Cyber Threat Intelligence?

Cyber Threat Intelligence (CTI) is a collection of data points (e.g. Open source, Social media, Human, Deep Web) and ultimately boils down to three questions:

— What do you have of value or importance?

— Who wants to disrupt your Agency or take what you have?

— What mechanisms and environmental factors exist for attackers to be successful in their attack?

CTI is used to research & analyze trends and technical developments of actors who target a specific organizations. This capability has generally existed within the security operations and incident response teams as analyst and responders seek to understand context of disparate data streams; however more and more, organizations are looking at non-traditional CTI applications which allows for the business to better manage enterprise risk through cyber threat intelligence.

Examples of Threat Intelligence

Cyber Threat Intelligence comes in many different shapes and forms which can include:

Internal Threat Intelligence:

— Identification of a business' critical information data stores

— Mappings of IP addresses to office locations

— Input from other system management systems (e.g. AV, IDS, Hunting tools)

— High value targets (HVTs) who have access to sensitive information or elevated privileges

External Threat Intelligence:

— Lists of bad/malicious IPs or sources linked to incidents

— Hashes, DLLs, executables and other indicators used by attackers

— Physical locations linked to cyber attacks

— Known actors who are targeting the organization

— Botnets and Command & Control servers

As adversaries continue to find new ways into the network and cyber budgets remain constrained, it is critical to ensure cyber capabilities are utilized across the business to manage enterprise cyber risk. KPMG is seeing the re-use and re-purposing of both internal and external threat intelligence as an enterprise risk management tool which helps agencies prioritize the response to threats.

Examples of how threat intelligence can be repurposed and repackaged to support your enterprise risk management include:

Application Security

CTI can be used from an application threat modeling perspective and provide a structured approach helps to identify, quantify, and address the security risks associated with an application. Using various models (for example OWASP), threat modeling using CTI gives the business owner greater understanding of the risks to the system by providing visibility surrounding the likelihood of an attack. By infusing CTI during the threat categorization phase of threat modeling, one can more easily prioritize the likelihood of certain threats above others. For example if an attacker, who targets your agency, uses DDoS as a primary method for denying access to publicly facing server, strong countermeasures including anti-DDoS technology and anti-DDoS emergency response services would be prioritized above other threats identified in the application threat modeling phase. Once a risk ranking is created and mapped to the application-specific threats, it is possible to sort from the highest to the lowest risk and prioritize the mitigation efforts and deploy countermeasures.

Supply chain risk management

Globalization, innovation and a demand for cost-savings have led governments to seek routine goods and services from distant vendors. And, as governments seek to procure innovative, specialized technology solutions – potentially from small niche firms or even start-ups – they find themselves contracting services from new business partners with unfamiliar reputations or unproven security practices. As the links in their supply chains become attractive targets, many governments are incorporating sophisticated, third-party risk management strategies to ensure they and their vendors are ready to prevent, detect and respond to cyber-attacks.

In these programs, it's important to have a continuous view of your third-party risk. CTI can assist with this by providing open source and/or proprietary sources of intelligence to identify potential data leakage, brand impact, financial/operational risk, and regulatory impacts of the vendors and contractors that work for you. To this end, third-party CTI can include identification of leaked credentials or IP associated with that vendor being used for C&C, botnet, spam activity; and website hygiene/DNSSEC misconfigurations. This information can help manage your organization's enterprise risk by identifying those vendors with whom it may be too hazardous to conduct business.

Training & Awareness

Your people are the first and last line of defense from a malicious actor. As such, specific people are often targeted due to their role in the organization (e.g. CEOs, administrative assistants, domain administrators, R&D personnel, etc.) however, those targeted may change over time. CTI provides a lens through which to help view the relative risk these people face as a part of their role with the organization and can be configured as a dynamic process which identifies external events which may elevate the risk specific to an individual.

Additionally, users who have never been targeted in the past may find themselves in the cross-hairs of an attacker due to a new promotion, work assignment, business travel, or other external environmental factors. Therefore, it's important to employ methods for continuous assessment of cyber threats specific to personnel. CIT can assist in creating a focused culture of awareness, action, and communication which improves both incident detection and response. Subsequently, this targeted information can then be used to create new user-specific cyber hygiene rules, or even tailor security controls to increase logging and monitoring for individuals whom are known to be targeted by adversaries so as to reduce the overall organizational risk. An agency's user base that is aware of the real threats targeting the organization becomes more effective in avoiding compromise.

How KPMG can help

We begin by understanding the business goals and operations of our clients. Informed by threat-intelligence and aligned with your exposure comfort level, we build a customized and holistic cyber strategy. This foundation will allow for a tailored security framework, effective human resource management and process flexibility.

KPMG International has been named a Leader in the Forrester Research Inc. report, The Forrester Wave™: Information Security Consulting Services, Q1 2016 achieving the highest score for current offering and strategy (tied).

"KPMG has moved cyber security to the heart of its business,"

according to the Forrester Research report authored by Martin Whitworth and can help you tailor use cases for your threat intelligence so it provides more value for your organization.

Contact us:

Tony Hubbard
Principal
703-286-8320
thubbard@kpmg.com

John Kupcinski
Director
703-286-8000
jkupcinski@kpmg.com

kpmg.com/socialmedia