Nowadays, one of the most booming topics in the cybersecurity market is Cyber Threat Intelligence. Jeroen de Wit, Cyber Defense Manager at KPMG and lead of KPMG Threat Management Services in the Netherlands, however notes a pollution of the term intelligence as used in the market. To further discuss this topic, he met with Joep Gommers to exchange ideas and thoughts. This conversation is recorded in this article and broken down into Cyber Threat Intelligence itself, its current challenges in the market and concludes with best practices for organizations to adequately deal with this highly relevant topic.

Cyber Threat Intelligence

Interview with Joep Gommers, founder & CEO of EclecticIQ

Interview by Jeroen de Wit

Joep Gommers is the founder and CEO of EclecticIQ, an applied cyber intelligence technology provider, enabling enterprise security programs and governments to bootstrap a threat intelligence practice.

Prior to EclecticIQ, Joep served as Head of Global Collection and Global Intelligence Operations at Cyber Threat Intelligence market-leader iSIGHT Partners (acquired by FireEye). Having worked around the world for large and small firms, Joep has acquired a depth and breadth understanding of market demands and the cyber intelligence industry. His vision of security programs is informed by the power of real threats and an ambition to build products that allow a leap forward in an organizations' cyber security efforts.

Joep, to start: what do you define as Cyber Threat Intelligence?

At its core, intelligence is about reducing uncertainty. When uncertainty involves conflict around business objectives, intelligence serves to decrease business risks. Cyber intelligence reduces uncertainty in dealing with threats such as electronic crime, hacktivism, terrorism and espionage.

Reducing this uncertainty, and therefore managing these cyber risks, requires information that cyber adversaries prefer to conceal. Intelligence analysts need to uncover this concealed information using direct and indirect means of collecting and analyzing available information. Intelligence analysts proceed by

All stakeholders should be comfortable with the plan for threat intelligence

establishing facts and then developing precise, reliable, and valid inferences for use in decision making. The resulting conclusions and predictions are extremely useful in operational planning for security operations, incident response, vulnerability management, risk management and board-level decision making.

Cyber Threat Intelligence follows the methods of traditional intelligence to focus on operational, tactical and strategic responses to cyber threats.

What trends are you seeing in the market of Cyber Threat Intelligence?

You might indeed say that the Cyber Threat Intelligence market is nowadays somewhat "polluted". Organizations use the term to denote any type of data they sell in their feeds. This means that one organization offering solely technical indicators of an attack [e.g. hash values and known bad IP addresses] and another which is offering a strategic analysis of hacktivist group Anonymous or the involvement in cyber incidents by the Chinese government both use the term Cyber Threat Intelligence to denote their information.

However, we also see an increase in organizations that are nowadays able to properly define what type of information they are interested in. Furthermore, analysts such as Gartner are also better able to categorize Threat Information Providers based on the actual content they are delivering. As such, comparing these providers has become easier, similar to being able to compare firewalls or IPS/IDS providers, thereby allowing a better matching of providers to your needs. That is, once you have actually defined your needs, which is something that quite a few organizations are still doing wrong or at least insufficiently.

What would be the typical mistakes, or misjudgments, you see occurring in the field?

In general this would be organizations realizing that Cyber Threat Intelligence is a hot topic, possible even a required topic to be successful in Cyber Defense, and trying to get into execution before defining what and how they are exactly going to handle it.

Dealing with Cyber Threat Intelligence requires the understanding that there is a difference between (1) merely buying intelligence as a product and by means of a project and/or in an ad hoc manner include intelligence into your procedures and processes to add value at that moment versus (2) implementing a process, team and responsibility within your own organization to integrate intelligence in procedures for different layers within the organization. By merely doing the former, therefore with the absence of a continuous integrated process, applying threat intelligence is merely done on an ad hoc, spur of the moment basis. A snapshot of sorts.

So how should organizations approach Cyber Threat Intelligence in your view?

From our years of experience we have, amongst others, developed a Cyber Threat Intelligence Maturity Model[1] which may provide guidance for those aspects that need taking into account. Above all, we have deduced the following seven best practices for organizations to take into account. Use them to your advantage!

1. Build for stakeholders

Creating business value from threat intelligence relies on the ability to understand the information needs and requirements of key stakeholders in the organization. These stakeholders are ultimately responsible for the deterrence, defeat and prevention of cyber threats. Start by understanding who the key stakeholders are, how and in what tone they prefer to consume intelligence, and what key intelligence requirements they need answered.

2. Drive urgency of organizational awareness of cyber threats

The potential application of threat intelligence spans across a wide range of operational, tactical and strategic issues that require both immediate action and long-term planning. Stakeholders have to be aware of the scope of threat intelligence, and how it can help them to control their exposure to the changing threat landscape. Successfully implementing a threat management capability requires buy-in by decision makers, and their appetite to invest will be proportional to how well internal stakeholders understand the value of threat intelligence.

3. Achieve organizational buy-in

All stakeholders should be comfortable with the plan for threat intelligence, including a shared vision, timing for a phased roll-out, known constraints and the expected measurable results. The key to any successful project is to cultivate an understanding of how much you want to accomplish, at what pace, in what steps and with what business constraints, whether in timing, resources or other factors. Make promises to the organization you can keep. Whether large or small.

4. Establish a Threat Management practice separately from IT Security

A Threat Management practice implements a threat intelligence

1 https://www.eclecticiq.com/resources/white-paper-threat-intelligence-maturity-model

process. To successfully plan, implement and operate such a practice requires specific intelligence competencies.

Threat intelligence is adjacent and related to IT Security, but it is a distinct competency with clear lines of demarcation. A separate Threat Management practice ensures the availability of the relevant competencies needed to architect, plan and implement threat intelligence processes and procedures, including the acquisition and analysis of threat intelligence feeds. The IT Security and Threat Management teams should work together as a well-balanced, cross functional team during the roll-out of any changes to existing of new processes and procedures. Otherwise, they should have separated responsibilities.

5. Strengthen capabilities in Analysis and Production

In threat intelligence, analysis and production represent the key enablers in understanding the cyber threat. Threat intelligence best-practices for analysis and production can be established at several levels of maturity. An organization should strive to advance capabilities through each successive level. We go into more detail in our whitepaper "Applying the Threat Intelligence Maturity Model to your organization".[2]

6. Bootstrap with threat intelligence platform technology

Threat Intelligence Platform (TIP) technologies have emerged to support common challenges with implementing or improving CTI capabilities. TIP provides an easy way of bootstrapping core workflows and processes as part of a successful threat management practice. When selecting a TIP for your organization, ensure that workflow functionality is available. By doing so, you can ensure that your TIP enables the centralization and consolidation of threat intelligence and the subsequent analysis, production, dissemination and integration of intelligence data into security controls, orchestration and other key processes.

7. Integrate technical indicators into security controls

Organizations commonly use technical indicators associated with intelligence to improve detection, prevention and response capabilities of security controls. This approach improves response times for threat detection and remediation."

Do you have any closing words on how organizations should go about implementing these best practices?

Something we have seen on numerous occasions would be to set clear and realistic goals whereby you do not expect to grow from maturity 1 to maturity 5 within a year, nor create too much of an imbalance on different axes of our maturity model.[2]

Take one step at a time, growing your threat intelligence practice in a manner visible to all stakeholders. Do so by having clear, predefined goals and results which will assist the entire organization on this journey, such that they are able to effectively process the intelligence you provide and thereby avoid disappointment in the result.

2 https://www.eclecticiq.com/resources/white-paper-threat-intelligence-maturity-model