CYBER THREAT INTELLIGENCE OPERATIONALIZATION

INTELLIGENCE REQUIREMENTS, THREAT MODELLING AND COLLECTION MANAGEMENT

APRIL 5, 2022

TTCSIRT
Author: Rick Logan-Stanford

It is said that knowledge is power. However, greater knowledge comes from knowing what to do with the knowledge. Once obtained, it drives the responsibility of action. Intelligence, like data, is not enough. Intelligence has to attain structure in order to be predictive, identifying potential attacks in order to give the organization or State entity the profound ability to defend or ultimately prevent an attack. It is a better alternative than outing fires in the wake of an attack.

While an organization or even a nation acquires information on its cyber landscape, it may become overwhelming without clearing the noise that helps in understanding existing threats. This information, once assimilated, assists in identifying vulnerabilities and resilience capabilities. It gives the entity leverage to prepare and prevent present and potential threats while lowering the effects of zero-day exploits. The most valuable and effective strategy to date to accomplish this is through the way of operationalization.

Cyber Threat Intelligence is an evidence-based knowledge approach used to inform decisions for the mitigation of an attack which includes prevention. Through operationalization of cyber threat intelligence, there are several aspects an organization or government entity will have to focus on in order to have maximum effectiveness for countermeasures and protection.

Three of the aspects to reign in focus are:

- Intelligence requirements
- Threat Modelling
- Collection Management (with relation to the data being gathered, stored and assimilated)

By defining the threat requirements, time invested in information gathering and research can be efficiently used to prioritize the most relevant and critical information. This prevents the loss of crucial data in the noise or the processing of unnecessary noise. Understanding which type of information is not only of interest but relevant to the cyberspace in which the organization or entity operates. For example, an organization in the financial sector would not have any need for information relevant to the energy sector or even SCADA systems. This prevents the wasting of time on irrelevant information gathering and processing.

Intelligence requirements can be defined and refined by examining groups as High level, Functional and Capacity/Visibility requirements. The High-level requirements focus on defining the type of threat actor that is a threat to the business or State entity while understanding business operations. Business operations extend to Countries of Operation, Business Industries of Operations and Business Top Critical Assets while answering two key questions: [1]What type of Adversary may be targeting the business or State? and [2]Who will consume the intelligence collected and produced?

Further examination into Countries of Operation shows that granularity is key in determining the regions of operation of organizations, their presence in each country, related business partners and the country they operate in. Here, an organization operating in the Caribbean with no presence or ties to the US, a threat actor targeting US-based organizations using a particular infrastructure would not be of particular interest to Caribbean organizations. Knowing your environment and your cyber diaspora will assist in filtering through the noise and keeping a focus on the relevance to the organization and its operations.

With Business Industries of Operation, the core operations of the organization are in focus. Within this level of the High-level requirement, the organization has to now focus on understanding all their secondary and still relevant industries that may possess sensitive information critical to the organization itself.

While examining the Business's Top Critical Asset aspect of intelligence requirements, an organization or even a State entity will need to have a more concerning focus on both critical data and Operational Systems. This will impact the availability of business and services. Critical data can encompass but is not limited to Credit Card information, Financial accounting data, Personal Identifiable Information Intellectual Property, Confidential business processes or communique, Credentials or IT System Information that can harm or impede business function or compromise integrity. A compromise of these assets could cost an organization and even a State, not only financially but also functionally.

Just by examining the High-Level requirement of defining threat intelligence, the picture of the importance and scope of cyber threat intelligence comes into focus with a bit more clarity. Defining threat intelligence is paramount because, as mentioned previously, the definition of intelligence assists in eliminating the noise and refining the data to make it more potent for effective and efficient operationalization.

During this requirement definition, two key questions are critical to keeping in mind at all times. [1]"What type of Adversary may be targeting the organization or State entity? ", be it a Hacktivist, Corporate/International Espionage or even Non-State actors. [2]"Who will consume the Intelligence collected and the data produced? ", be it either SOC analysts or CISO but not limited to both. By answering the second question, the organization or State can then know which form of intelligence processing will be beneficial and more useful; either Technical, Tactical or Strategic.

With the Functional requirement of cyber intelligence, the organization or State entity mainly examines their exposure. The scope is focused on Physical external or perimetral and Physical internal exposure. An organization's external exposure takes into consideration any servers on their infrastructure external/public facing networks along with devices, connected to their network, which can be accessed externally. Internal exposure relates more to systems being used on the internal network, the OS and software versions. Examining internal exposure gives greater insight for the organization or State entity to identify unpatched vulnerabilities as well as their patch management policies. The main scope for network infrastructure is the backbone. It is also critical to identify the type of attachments allowed on the network via download. Finally, the organization or State entity needs to answer the question, "What type of attack or Threat is most concerning or critical to operations and services?".

The final intelligence requirement mentioned is the Capability and Visibility requirement. This results from gathering data from an organization or State entity's own environment, lending to a higher visibility which leads to the acquisition and utilization of tools to process the information more efficiently and effectively. Several resources are essential to give this level of visibility on any network in order to satisfy this requirement. These resources are in the form of artifacts such as Email logs, Network infrastructure documentation and monitoring logs and Passive DNS (DNS resolutions made by any device connected to the network). Aside from logging, other artifacts such as external feeds from communities and forums dedicated to sharing cyber intelligence are also essential to aid with data collection. Endpoint visibility and centralized storage and correlation work together to not only collect information from nodes but make integration with other internal tools possible to allow automation easier.

Following the requirements phase, Threat Modelling is key in order to make your Threat Intelligence more valuable and pronounced, because it optimizes the application, digital platform and even the business process security resilience. This process identifies, enumerates and prioritizes potential threats in light of vulnerabilities from an attacker's perspective; the hypothesized attacker is

identified in the High-level requirement phase of operationalization. The identification of these vulnerabilities lays the groundwork for appropriate and effective countermeasures to prevent and even mitigate against the effects of identified potential threats.

Threat modelling focuses on any lack of defense mechanisms or controls, security requirements within an entity's lawyered defense system and business processes. To effectively achieve the aforementioned outcome, the modeling process requires a cooperative and collaborative effort from stakeholders ranging from Security Architects, Security Operations, Network Defenders, SOC and the Threat Intelligence team; each understanding the other's designated roles, responsibilities, purpose and identifying challenges in collaboration. Basic steps to threat modelling can be seen as follows:

- Identify the Assets
- Outline Architecture
- Break Down the Application in review
- Identify Threats
- Classify & Structure Threats
- Rate Severity of Threats identified

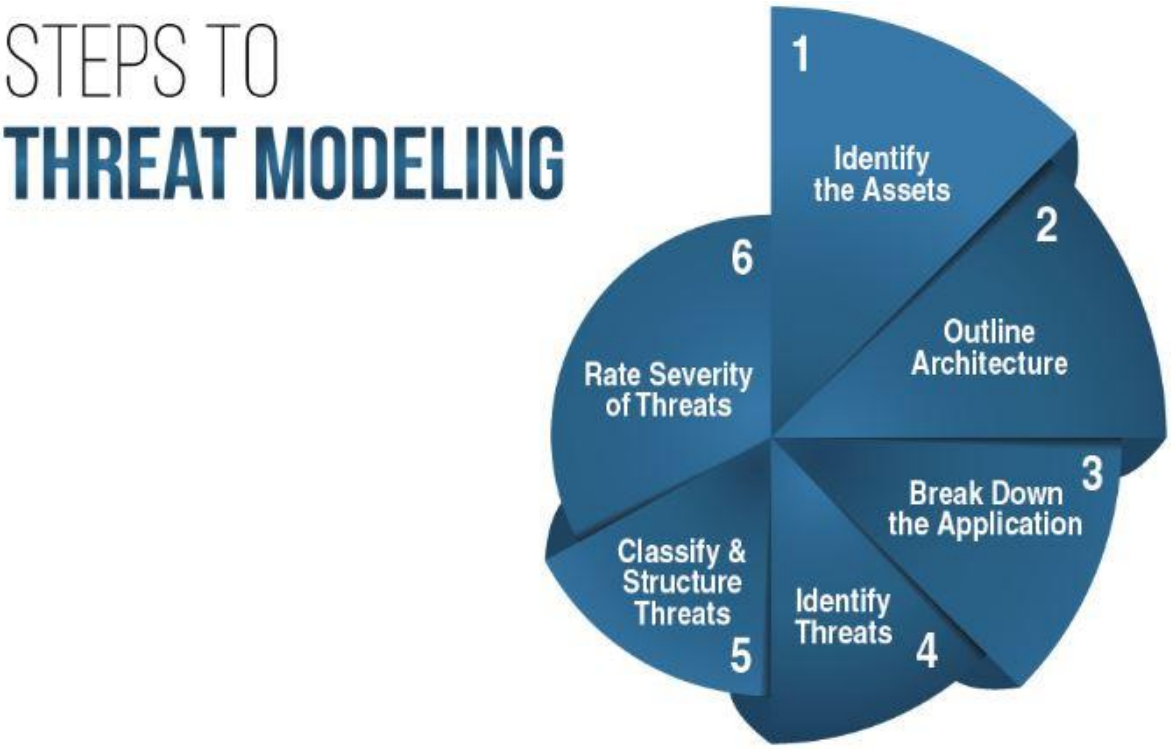

Illustration by eccouncil.org

Keeping in mind there are several industry-known threat models, an organization or State entity isn't limited to using the exact model format. Instead, they can examine the most relevant model and customize their own using it as a guided template. Such top models are:

- STRIDE – designed to focus on IT-related threats
- PASTA – a risk-centric model which is adaptable and allows for threat simulation
- LINDDUN – focuses on Data and Privacy related threats
- OCTAVE – is focused on Risk Management and organizational impact
- VAST – scales across infrastructure focusing on the attacker

Creating a threat model from scratch, an organization or State entity can look to five best practices and even customize an existing threat model. The best practices follow:

- Define the scope and depth of analysis
- Gain a visual understanding of what is being threat modelled
- Model attack possibilities
- Identify threats (steaming from potential attacks)
- Create a traceability matrix of missing or weak security controls

There can be misconceptions about threat modelling when either in the process of creating one or updating an existing model to suit your needs. One misconception is that pen testing and code reviews can substitute for threat modeling; while both are very effective for finding bugs, threat modeling is better at revealing design flaws.

Another misconception is that threat modeling is an exercise and isn't necessary after the deployment of an application or cyber service. Threat modeling will assist and influence future security architecture strategy and deployment to allow for faster and more effective remediation. A third misconception is very much the biggest and ends up being a deterrent, threat modeling is complicated. Threat modeling appears to intimidate many developers at first glance, but once broken down, it's soon seen to be simply workable.

It is essential, even pivotal to the security of an application that threat modeling be made part of the development process. Building an application or mapping a business process, without anticipating the potential for threats and mitigating processes, or focusing on corporate or industry security policies and privacy regulations, is like exposing your Achilles heel without any concern of it being targeted. As threat modeling brings to light foresight of the impact of potential threats, the severity map will give better bearings to the controls to be implemented. Threat modeling helps weave security in the project during the development process and holds during maintenance.

All of the requirements or modeling are worthless without structured and decisive data collection management. Firstly, there has to be an understanding of the data sources identified and available to the organization or State entity to satisfy the defined requirements. The data collected can be accessed by analysts in a simple format like an Excel spreadsheet or as convenient as an internal data store via hyperlinked pages.

Two critical characteristics of data in threat intelligence are quantity and quality. Both aspects will reduce noise from unnecessary information as well as reduce the number of false positives and more importantly will not allow a serious threat to be overlooked. While collecting, it is crucial to consider your internal and external blind spots along with the technical and automated techniques that suit the need of the organization or State entity. One valuable but highly risky source to consider is cybercriminal forums and the dark web on the whole. Though the payoff for collecting data on the dark web can be high, the risk of being compromised is also highly probable.

The employment of a collection management framework will be needed at this point to validate the data collected from the sources. In validation, the relevance, reliability, accuracy and completeness of the data are all evaluated for processing in order to produce effective and actionable results.

With proper CTI, more clarity can be achieved when looking at the big picture of an entity's cyber presence and environ. Without examining the bigger picture, an organization or State entity will not exactly know what they are looking at, much less know what exists out in their cyber landscape. Operationalizing CTI, like an emergency light, disperses the dark and gives sight to what was not

initially observed. The more visibility and perspective, the greater the chances of defending against or mitigating attacks. Know your adversary and better understand your own capacity and capability to defend your cyber equity.

In cyberspace, the threat landscape is ever-morphing and evolving with the development of new applications and operation processes. Operationalization shortens the reaction and action time of the organization or State entity's cyber defensive maneuverability. As powerful as this is, the lifeline of operationalization is an investment. It empowers an organization or State entity to harness the benefits of threat intelligence management and reap the rewards of pure intelligence leading to effective and efficient actioning; actionability is the goal of cyber threat intelligence operationalization.

Threat intelligence management needs to focus on the collection and correlation of data from identified sources in a centralized management solution. With data being centralized, advanced analytics can now be implemented to arrogate and interrogate the data to give more meaning. An oversight of operationalization is the ability to customize the solution as well as to integrate with existing and emerging security technologies while adapting to new techniques. One mistake to always avoid is building a CTI program with point tools and manual processes as the fundamental foundation.

According to Gartner 2021, organizations are overwhelmed with data and information to the point of drowning in it. With this abundance of unstructured data, no intelligence is obtained and poor operational use is the end result. In the report, it was also found that threat intelligence solutions were considered a luxury and were not thought to be pivotal or essential during development, security operations and even business cyber risk exercises. One other finding was the neglect of threat modelling was noticeable.

Based on a SANS 2021 survey on threat hunting utilizing CTI, it was mentioned that with a more comprehensive understanding, organizations or State entities can see the effectiveness and usefulness of threat hunting out of CTI to improve overall security and resilience maturity. SANS reported a 25% improvement in organizations' security posture, with organizations highlighting the positive impacts.

Security and risk management leaders mostly, often, look at the ROI or the initial investment required to operationalize CTI resources, finance and human resource wise. To help with this hurdle, the very Gartner report recommends budget justification, focusing on the value of CTI and how crucial it is to the success of security programs as well as the fundamental protection of the business while strengthening the controls already in place. Justification can be done by looking at use cases such as telemetry enrichment and vulnerability prioritization.

It is not enough though to use intelligence sources. Contributing is just as useful in growing awareness and community. Crowdsourcing is a powerful approach to improve defense against threat actors while supporting concerns of privacy and data exposure.

CTI needs to be looked at not as a herculean task, but as just one piece of the puzzle involving cyber security defense to make an organization or State entity more secure. Once CTI is taken into consideration and incorporated as part of the development foundation it will be carried throughout the process and what seems to be intimidating would now be integrated from the start.

Operationalizing CTI can aid in the creation of new SIEM rules to improve detection. Sysmon queries can also be crafted in more detail to find malicious behaviour or exactions that may otherwise go undetected.

In a 2022 white paper published by DomainTools, in 2021 numerous organizations reported a shortage of internal cybersecurity skills, affecting an organization or State entity's ability to translate data into intelligence and effective operationalization of cyber threat intelligence. Supported by the aforementioned SANS 2021 survey, a lack of trained personnel is present but decreased from 57% to 54% due to a lack of funding increasing as slightly (indicated by the graph below). The report also indicated the use of multiple point tools used by organizations, but not mapped to alerts between these tools to give context to reveal the scope of events or indicators.

Illustration from SANS 2021 survey

With the lack of resources within organizations and most State entities, it may be possible that CERTS/CIRTS can be more than just a source of data feeds. One example is the Trinidad and Tobago Cyber Security Incident Response Team (TTCSIRT) in recent operations. There was an incident where through regular operations, intelligence was collected pointing to a vulnerability found with Fortinet firewalls, namely a release of credentials on the dark web.

TTCSIRT, small but established was able to take the intelligence and quickly analyze the information with timely action. Organizations and State entities were quickly identified and contacted to inform them of the indicators identified. Some entities, who were without internal skills, were guided and even assisted by the CSIRT staff. This intelligence was also shared throughout the CSIRT community, improving the defense of the cyber landscape internationally.

This approach not only bolsters the effectiveness and efficiency of threat intelligence but also shows its value. CSIRTs like TTCSIRT are in a position to operationalize threat intelligence because they are a source of themselves of alerts and are a pathway of data sharing. By operationalizing CTI, CSIRTs can help organizations and State entities facing challenges due to a lack of skills and funds. With CSIRTs being leveraged by organizations and State entities, disinformation and misinformation would not be an issue as the information will be digested, analyzed and made actionable.

In conclusion, CSIRTs can be more assertive with the intent of being more proactive within their constituency. As they already possess the necessary skills and resources. CSIRTs are not only capable of filtering through information for intelligence and passing it along, but they can also give assistance

to organizations or State entities with further support. For the example with TTCSIRT, the information was sorted from a feed of 40,000 unique IP addresses compiled by a threat actor and refined to 36 localized addresses. The 36 identified entities were then systematically contacted and informed of the vulnerability along with their information being posted on the dark web. The entities were also guided through the necessary mitigation processes and best practices. Those entities who were not able to carry out mitigation were assisted by TTCSIRT.

Not all organizations or State entities are one size fits all when it comes to intelligence requirements or threat modelling. CSIRTs are in a unique position to be part of the operationalization of threat intelligence while working with entities who require operationalization but this is lacking in some aspects. Working together, the entire cyber community can collectively make cyber space much more secure.