MENU

Why "Cyber Threat Intelligence-Informed Services" Should Be Part of Your Cyber Security Strategy

25 MAY 2020 on SOC, CTI, Tactical CTI, Strategic CTI, Operational CTI, Cyber Threat Intelligence

The last couple of years **Threat Intelligence Platforms (TIP)** have been increasingly more popular in many global Security Operation Centers (SOC). With this technology there comes a unique value that can be provided to Cyber Security Services within an organization. With the support of a TIP platform and a Cyber Threat Intelligence-informed focus it allows to be combined into a "Cyber Threat Intelligence Program" which provides Intelligence (as a process and product) to inform decisions within a series of cyber security services of the organization. Within this blog post I illustrate how that value might look like including some critical factors.

Why have a Cyber Threat Intelligence Program?

A. Cyber Threat Intelligence (CTI) helps with the collection and analysis of information about threats and adversaries. Producing threat models that provide an ability to make **knowledgeable decisions** for prediction, preparedness, prevention, detection, hunting, response and forensic actions against various cyber-attacks.

B. Cyber Threat Intelligence (CTI) focuses on threat modeling, **supporting leadership** to evaluate and make informed forward-leaning strategic, tactical, and operational decisions on existing or emerging threats to the organization.

C. Cyber Threat Intelligence (CTI) helps the organization's to **identify and mitigate various business risks** by converting unknown threats into known threats and helps in implementing various advanced and proactive defense strategies

D. With the constant innovative TTPs used by threat actors, cyber

threats are becoming major risks to any business sector. To thwart these threats, it is important for the organizations to incorporate and leverage actionable Cyber Threat Intelligence (CTI) to **strengthen their existing security posture**.

What are popular Cyber Threat Intelligence (CTI) strategies?
As a general start point, the organization should develop their Cyber Threat Intelligence (CTI) Strategy based on their business risk levels and regulatory, compliance or business requirements. Popular words used in common literature when it comes to CTI might include:

- Cyber Threat Intelligence **driven** Security Services
- Cyber Threat Intelligence **lead** Security Services
- Cyber Threat Intelligence **centric** Security Services
- Cyber Threat Intelligence **informed** Security Services

The first three seem to suggest that CTI is the primary driver for making decisions within it's cyber security organization. I believe this is the wrong perception and focus should be shifted to using intelligence to **inform policy not drive it**.

"The role of intelligence is to inform the decision-making process, support the policies, and provide knowledge and decision advantages for the policy maker" - **Amanda J. Gookins**

This was also of my argument with publishing the SPEED Use Case Framework where I highlighted that a threat-centric biased approach is risky and should be augmented with:

- **General asset-centric baseline controls**

(and critical assets with enhanced baseline controls)

- **Self protection of assets**

(tampering alerts, visibility loss, technical compliance Management)

- **Compliance driven countermeasures**

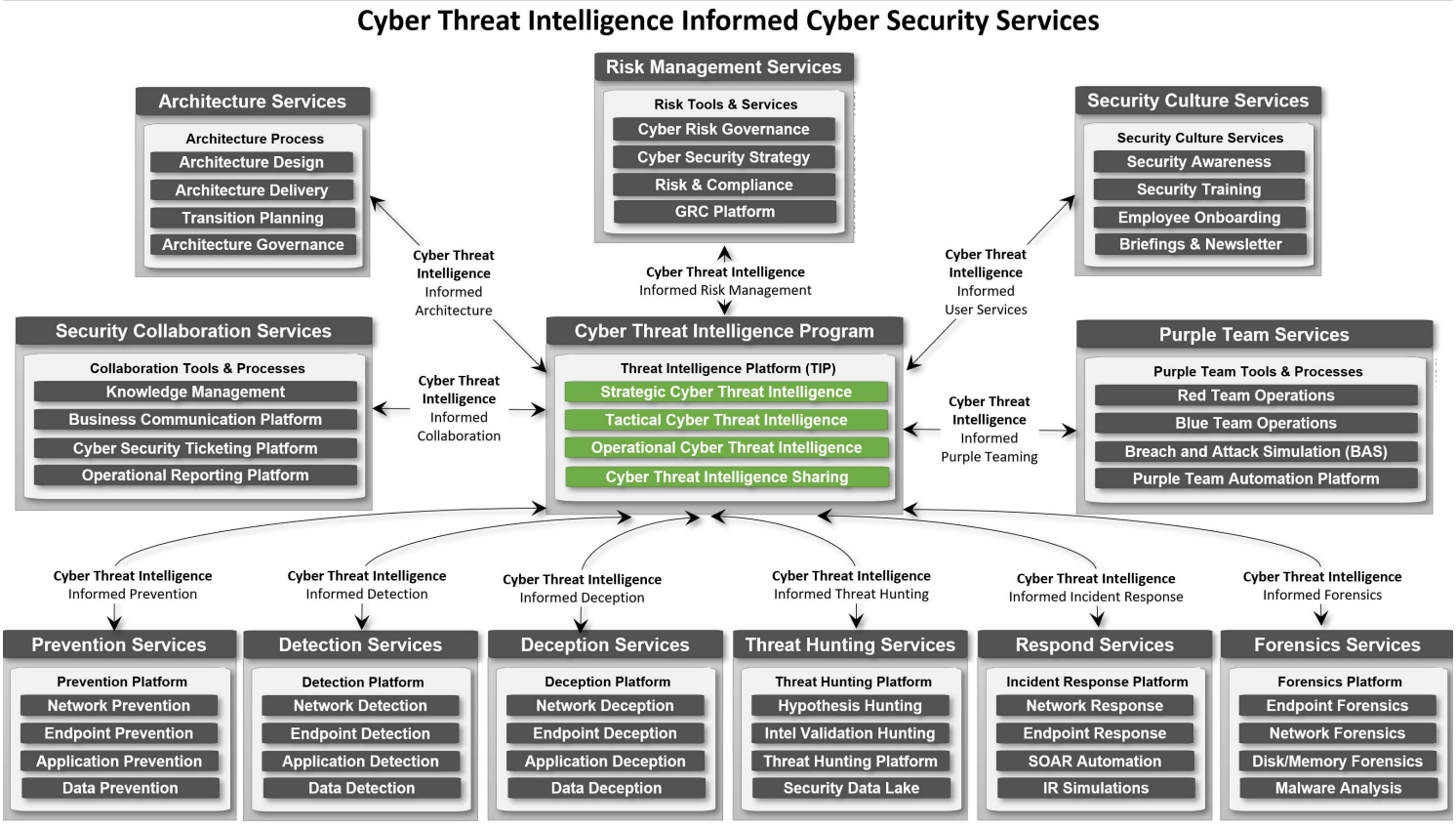
(sometimes you just need to comply to audit standards)

- **Split between CTI feeds, Quantitative and Qualitative threat models.**

(just dumping everything in one threat model, doesn't work)

"You will never reach your destination if you stop and throw stones at every dog that barks." **—Winston Churchill**

In the following diagram I made an attempt to visualize this core concept:



What must be highlighted before starting a Cyber Threat Intelligence program is that there should be a foundational core SOC context in place to be able to profit of the value of a Cyber Threat Intelligence Program:

1. Established **Security Incident Management** process.
2. Established **Core SOC technologies** (Example: SIEM, SOAR, EDR, IDS, IPS).
3. Established Technologies should be **able to receive and apply automated** Indicator of compromise (IOC's) feeds.

To illustrate more in detail the spectrum of CTI's business value, the following diagram is created:

Critical points:

- This is an over-simplification of the types of CTI, in reality the implementation of these types may vary per organization.
- Within the literature of SANS and EC-Council Operational and Tactical is swapped around (i suspect this has to do with the military origin of most of these conceptual frameworks.) Due to my background primarily in business i flipped these around to make it more logical for myself (and generally the business crowd I present to)
- SANS talks about Strategic, Tactical and Operational, but EC-Council also talks about Technical CTI for the sake of simplicity

this has been left out of the diagram.

Conclusion:

A Cyber Threat intelligence-informed SOC strategy is highly beneficial for your cyber security organization in terms of combating targeted cyber threats but do not forget that it's CTI job to inform policy not create it.

Jurgen

Please connect with me on LinkedIN.

https://linkedin.com/in/jurgenvisser/

Share this post

READ THIS NEXT

How to strategically use the OODA Loop and SCRUM within a SOC

I recently created a blog post where I proposed the OODA loop

YOU MIGHT ENJOY

An OODA-driven SOC Strategy using: SIEM, SOAR and EDR

The last few years within the Cyber Security Operations Center (SOC) Domain, several new

as part of a central SOC strategy....

technologies having been trending that...