Deloitte.

cyber 101

Cyber Threat Intelligence

Information to insight

June 2019

Cyber Threat Intelligence

What is it?

What is Cyber Threat Intelligence?

Cyber Threat Intelligence (CTI) primarily focuses on analysing raw data gathered from recent and past events to **monitor, detect and prevent threats to an organisation**, shifting the focus from reactive to preventive intelligent security measures.

Ideally, CTI should become the foundation on which a firm builds its secure, vigilant and resilient capabilities.

Why is it important?

CTI ensures organisations are informed and up to date with the volume of threats, including methodology, vulnerability, targets and actors within the space.

Based on Deloitte-NASCIO Cybersecurity Study 2018, threat monitoring (audit logging, CTI, and security operations centre) has also increasingly become the top function covered by the cybersecurity budget in recent years.

The potential benefits of CTI

1. Prevent data loss
Monitor attempts of communication with malicious domains and gather intelligence data

2. Detect breeches
Detect viruses, intrusions, and protocol non-compliance

3. Threat analysis
Offer insights into the necessary defence mechanisms and other measures that may be required

4. Data analysis
Reveal additional information regarding the threat, such as the attacker's motives etc.

5. Incident response
Provide guidance in the event of a breach regarding its magnitude, and method of operation

6. Threat intelligence sharing
Create awareness about the existence of other threats in the industry

http://www2.bain.com/Images/BAIN_BRIEF_Why_cybersecurity_is_a_strategic_issue.pdf

https://www.forbes.com/sites/forbestechcouncil/2018/05/22/real-time-cyber-threat-intelligence-is-more-critical-than-ever/#518403c317fb

Cyber Threat Intelligence

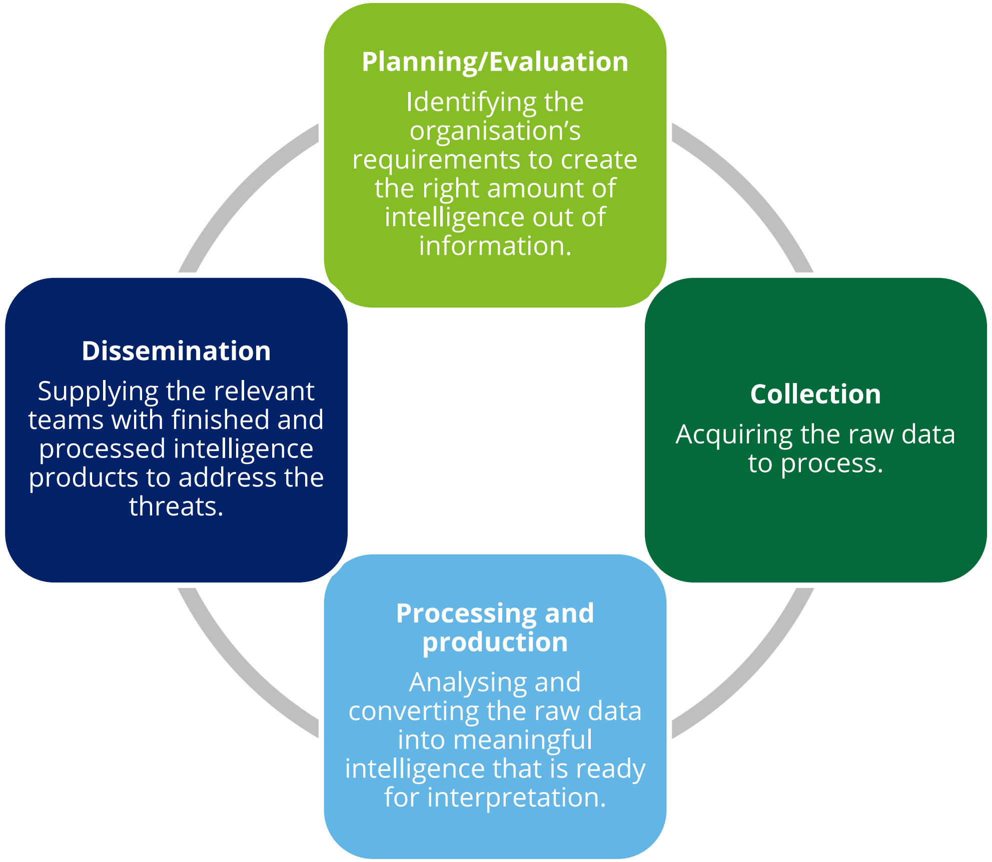
Leveraging the CTI process

How do you leverage CTI?

CTI, instead of being an end-to-end process, is a cyclical process, referred to as the intelligence cycle. The requirements for the cycle is planning and collection of data, analysis of results, production of intelligence from the results, dissemination of the intelligence, and re-evaluation of the intelligence in the context of new information and feedback.

CTI is also the ability to derive meaningful and actionable insights from structured and unstructured sources, both internal and external, through direct human involvement and/or automated means.

To be actionable, threat data should be understood in a context that is meaningful to the organisation. As a company develops greater maturity in its data gathering and processing capabilities, automation can be leveraged to better filter and highlight information that is directly relevant to important risk areas.



Planning/Evaluation
Identifying the organisation's requirements to create the right amount of intelligence out of information.

Collection
Acquiring the raw data to process.

Processing and production
Analysing and converting the raw data into meaningful intelligence that is ready for interpretation.

Dissemination
Supplying the relevant teams with finished and processed intelligence products to address the threats.

https://www.cisecurity.org/blog/what-is-cyber-threat-intelligence/

https://securityintelligence.com/what-are-the-different-types-of-cyberthreat-intelligence/

https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-cyber-threat-intelligence-cybersecurity-29102014.pdf

Cyber Threat Intelligence

By the numbers

cyber 101

Among the key findings of the Bandura CTI Report 2018 are that organisations are increasingly making CTI a key part of their security programmes. Other important findings include:

Which cyber threats are you most concerned about?

56%
Phishing attacks

47%
Zero-day attacks (Against publicly unknown vulnerabilities)

46%
Insider attacks (Malicious or careless insiders)

What are the top use cases for your CTI data?

58%
Detecting threats and attacks

49%
Incident response

45%
Vulnerability management

What are the most important features of a CTI platform?

56%
Rapid identification and remediation of attacks

54%
24/7 threat intelligence, monitoring and analysis

41%
Ability to assess risk and prioritise threats

https://banduracyber.com/wp-content/uploads/2018/10/2018_Threat-Intelligence_Report_Bandura-10-26.pdf

Cyber Threat Intelligence

Indicators of Compromise

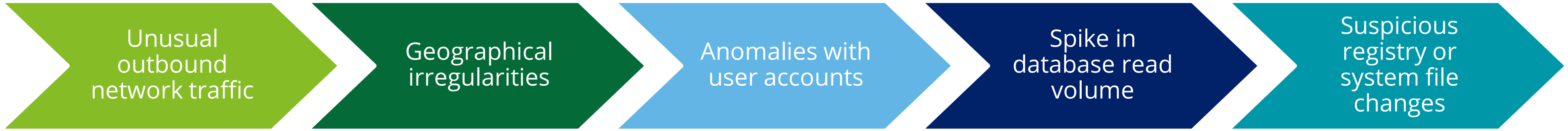
What are Indicators of Compromise?

CTI is often presented as Indicators of Compromise (IoCs), either in the form of tactical, operational or strategic intelligence:

- **Tactical intelligence (short-term):** Information from known attacks, which has the potential to immediately influence cybersecurity decision-making.
- **Operational intelligence (mid-term):** Offers insight into threat actors'[1] motivations, capabilities and objectives, and helps teams assess specific incidents relating to events and investigations, and guides and supports incident response.
- **Strategic intelligence (long-term):** Broader and higher-level abstracts of the data to identify threats associated with foreign policy, global events etc., and focuses on the long-term impacts of cyber threats.

IOCs serve as important artefacts that enable organisations to detect malicious activities, which can prevent an eventual breach from happening. They also provide actionable threat intelligence that can be used to improve an organisation's incident response strategy.

What are some common IoCs to monitor?



Unusual outbound network traffic

Geographical irregularities

Anomalies with user accounts

Spike in database read volume

Suspicious registry or system file changes

[1] Threat Actor: An individual or organization that is responsible for an incident that impacts or has the potential to impact an organization's security.

https://www.forcepoint.com/cyber-edu/indicators-compromise-ioc

https://securityintelligence.com/raise-the-red-flag-guidelines-for-consuming-and-verifying-indicators-of-compromise/

Case study 1

Deloitte utilises CTI to secure client's global energy network

Challenges

With a globally-distributed power plant network forming the core of their business, the client was interested in building a comprehensive **attack surface map** that not only considered cyber threats, but also broader hybrid attack vectors crossing the boundary between the cyber and physical realms which threatens their critical infrastructure and place human lives in harm's way.

Methodology

The Deloitte team conducted an in-depth fingerprinting exercise, used to identify and profile users for potential threats across a wide range of information sources including the deep and dark web. Additionally, the team conducted on premise social engineering campaigns at power plant locations to assess the likelihood of extracting sensitive information from on-site employees.

The information collected enabled the team to build a comprehensive map of the client's attack surface and exposures which aided the client to remediate pressing findings and remove online malicious content.

Outcomes

- The global exposure map enabled the client to identify the greatest pain points and prioritise remediation efforts by geographic area, specific power plants and technology assets.
- The broad spectrum of intelligence collection techniques allowed a much deeper understanding of the threats the client is facing compared to a fragmented approach that focuses on technology-related risks alone.

What is an attack surface map?

An attack surface is the areas of risk faced by the organisation – this is the organisation's exposure, reachable and exploitable vulnerabilities.

Mapping the attack surface allows the organisation to compile all aspects of the organisation's risk and security positioning in one consolidated matrix. This allows organisations to prioritise and mediate high-risk areas.

Threat Vector - Understanding the Attack Surface and How to Defend It

Case study 2

Deloitte defends against hacktivists in areas of political unrest

Challenges

The clients were based in a region that became embroiled in a broadly-impacting crisis caused by political unrest. The clients sought assistance in implementing a 24/7 situational awareness program to help them keep abreast of chatter and attack planning activities by hacktivist groups in the region who were targeting companies based on their perceived political leanings.

Methodology

Deloitte assembled a team of professionals working around-the-clock to monitor the situation for the duration of the crisis. During the initial stage, the team conducted reconnaissance activities to identify the most prominent hacktivists and their likely targets.

By ramping up the staff dedicated to monitoring the situation, the team was able to identify certain targets before they were declared as such. The team also identified and reported on tools, techniques, infrastructure and malware leveraged by the hacktivist groups.

Outcomes

- The team consisting of multi-disciplinary skillsets across crisis management, CTI, social engineering and criminology were able to provide in-depth situational awareness during the crisis.
- The valuable information provided the client with actionable intelligence during a period when timely action was of the essence.

What is a hacktivist?

Hacktivist is a blend of hacking and activism for a political or social cause. Unlike cyber criminals who hack and exploit for monetary gain, hacktivists see themselves fighting injustice.

Although they perceive themselves as fighting for a just cause, their means, similarly to cyber criminals, are illegal. Targets of hacktivists include governments, corporations and individuals.

NY Times – What is a "hacktivist"?

Case study 3

Apple Federal Credit Union uses CTI to prevent fraud

Challenges

Apple Federal Credit Union (Apple FCU) is a US-based credit union with more than US$2b in assets and 180,000 members. The challenge for Apple FCU was to understand the behaviour of cyber attackers to get ahead and prevent any information or assets being stolen from their members.

Methodology

Apple FCU engaged Surfwatch Cyber Advisor, a CTI solution to better address trending cyber risks. Surfwatch Cyber Advisor used a combination of analytics, programs and security experts to build and continuously monitor the organisations risk profile against trending threats and generates meaningful, actionable reports for key stakeholders.

Outcomes

- With intelligence reports, Apple FCU understood the motives and methodologies of current threat actors to anticipate attacks and execute security programs to repair exposures and mitigate threats.
- Apple FCU was also able to identify stolen credit card stacks being traded and sold on the **dark web**, which allowed them to get ahead before fraud or identify theft are committed.
- Threat reports generated were not only useful for the cybersecurity experts, but also utilised by other departments and branches in the organisation.

https://www.surfwatchlabs.com/releases/2016/06/29/new_cyber_threat_intelligence_case_study_for_financial_services_released_by_surfwatch_labs

https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html

What is the dark web?

The dark web is a part of the internet that is not visible to search engines and requires a specialised program to access.

This is intended to keep website operators and users anonymous or untraceable.

Of the 2,723 websites that were examined, 57% of those websites hosted illicit material such as buying and selling of credit card information, drugs, guns and counterfeit money.

CSO Online - What is the dark web? How to access it and what you'll find

Cyber Threat Intelligence

How to build an effective CTI framework for your organisation

Define what is important

Understanding what you need to protect and why, is an integral part of picking out the right CTI solution for your organisation.

Take some time to inventorise your data, systems and other assets, this will help you to understand what is at risk and who may potentially be targeting your data and systems. This will help your organisation build a risk profile to understand what is at risk.

Set specific goals you want CTI to achieve

Defining clear, specific goals helps your organisation understand the current gap to identify the tools needed for your organisation to bridge the gap to achieve the desired target.

Some examples of specific goals may be: (1) improve your incident response time; (2) automate key aspects of incidence response; (3) gather forensic data for post-breach attack investigation.

Continuously refine your CTI feeds

As criminals leverage new and improved methods of attack, organisation must constantly upgrade and refine CTI tools and threat feeds to address the new changes.

Data that was once relevant today, may become white noise tomorrow. It is important for organisation to constantly redefine and evaluate their CTI framework to provide current and relevant insights.

Get expert help

Knowing what goals to set, which assets need protecting, and how best to achieve the goals and optimise your CTI feed is not always easy and may require expertise.

Building an experienced cybersecurity team may not always be feasible. Instead, many organisations choose to hire third-party managed security service providers to gain an entire team of cybersecurity experts at a fraction of the cost.

https://www.compuquip.com/blog/build-an-effective-cyber-threat-intelligence-framework

https://www.crowe.com/cybersecurity-watch/using-threat-intelligence-effectively

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 286,000 people make an impact that matters at www.deloitte.com.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities provide services in Australia, Brunei Darussalam, Cambodia, East Timor, Federated States of Micronesia, Guam, Indonesia, Japan, Laos, Malaysia, Mongolia, Myanmar, New Zealand, Palau, Papua New Guinea, Singapore, Thailand, The Marshall Islands, The Northern Mariana Islands, The People’s Republic of China (incl. Hong Kong SAR and Macau SAR), The Philippines and Vietnam. In each of these, operations are conducted by separate and independent legal entities.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.