Cyber Threat Intelligence

Yudistira Asnar
yudis@itb.ac.id

Cyber Threat Intelligence (CTI) - Definition

- gathered by processing and analyzing current and potential threat data from various sources, such as network traffic, malware samples, open-source intelligence (OSINT), and threat feeds
- Objectives
  - **Establish proactive cyber defens**e by anticipating and preventing cyberattacks, rather than reacting to them after they occur.
  - **Improve risk management** by identifying and prioritizing the most relevant and severe cyber threats to their assets and operations.
  - **Enhance incident response** by providing actionable and timely information to contain, eradicate, and recover from cyber incidents.
  - **Reduce cyber vulnerability** by uncovering and addressing the weaknesses and gaps in their cybersecurity systems and processes.

Types of CTI

- Strategic CTI - high-level and long-term insights into the cyber threat landscape, such as the trends, motives, and objectives of threat actors and campaigns. It need to provide understanding the big picture and the implications of cyber threats for their organization's strategy, policy, and risk management
  - senior executives and decision-makers
- Tactical CTI - detailed and short-term information about the tactics, techniques, and procedures (TTPs) of threat actors and malware, such as the indicators of compromise (IOCs), attack vectors, and vulnerabilities exploited. It helps to detect, analyze, and respond to cyberattacks, as well as to improve their security controls and defenses.
  - security analysts and operators
- Operational CTI - specific and actionable information about ongoing or imminent cyberattacks, such as the targets, timing, and methods of the attackers. It supports various tasks such as: contain, mitigate, and investigate cyber incidents, as well as to hunt for and disrupt threat actors and activities.
  - incident responders and threat hunters

(Some) Main Sources

- Network Data
- Malware Data
- OSINT
- Threat feeds

Strategic CTI - Objective

- **Identification and Understanding**: To recognize and comprehend the entities behind cyber threats, their motives, objectives, capabilities, and methods, as well as the associated risks and impacts on the organization.
- **Guidance for Security Strategy**: To inform and shape the organization's security strategy and decision-making, including policies, procedures, controls, resource allocation, and prioritization.
- **Risk Assessment and Mitigation**: To evaluate and reduce the cyber risks to an organization by considering the likelihood and severity of threats, as well as the organization's exposure, vulnerabilities, and resilience.
- **Communication and Education**: To inform and educate key organizational stakeholders, such as executives, board members, and customers, about cyber threats and the necessary security measures.

Strategic CTI – Type of Threats&Vuln

- **Advanced Persistent Threats (APTs)**: Targets critical organizational assets with sophisticated methods to avoid detection.
- **Emerging Threats**: Exploits security gaps using new technologies and trends.
- **Geopolitical Threats**: Impacts the organization's reputation and compliance, influenced by global political and economic events.

Strategic CTI – Results

- **Threat landscape report** - an overview and summary of the current and emerging cyber threats, actors, and campaigns, as well as their trends, motives, and objectives.
- **Threat assessment report** - a detailed and in-depth analysis and evaluation of the cyber threats, actors, and campaigns, as well as their TTPs, IOCs, and impacts.
- **Threat intelligence brief** - concise and timely update and alert on the cyber threats, actors, and campaigns, as well as their activities, developments, and indicators.

Strategic CTI – Technique

- The open source intelligence (OSINT) that collects and analyzes the data and information that are publicly available and accessible, such as news articles, academic papers, government reports, or online communities
- The closed source intelligence (CSINT) that collects and analyzes the data and information that are privately owned and restricted, such as commercial vendors, industry partners, or confidential sources
- The internal source intelligence (ISINT) that collects and analyzes the data and information that are generated and collected by the organization itself, such as logs, alerts, incidents, or feedback
- The threat modeling and frameworks that structure and categorize the data and information into meaningful and useful groups, such as Abuse Case, Attack Surface Analysis,the Kill Chain, the Diamond Model, or MITRE ATT&CK
- The threat intelligence platforms (TIPs) that store, manage, and access the data and information, and that create and present the intelligence products, such as reports, briefings, alerts, or indicators

Strategic CTI – Relation

- Strategic CTI provides the direction and guidance for the operational and tactical CTI, by defining the intelligence requirements, topics, and priorities, and by establishing the roles, responsibilities, and processes
- Strategic CTI relies on the feedback and input from the operational and tactical CTI, by measuring and evaluating the effectiveness and efficiency of the intelligence products, and by identifying and implementing the lessons learned and best practices

Tactical CTI - Objective

- **Identification and Understanding**: To pinpoint and comprehend the methods and locations of cyber threats, including the tools, techniques, targets, and indicators used by threat actors, along with their technical attributes and signatures.
- **Guidance for Security Operations**: To inform and steer the security operations and responses of an organization, which encompasses the detection, identification, containment, and remediation of cyber threats, as well as the setup and adjustment of security tools and systems.
- **Communication and Education**: To convey information to and educate security practitioners and analysts within the organization, such as SOC staff, incident responders, or threat hunters, about cyber threats and the corresponding security measures.

Tactical CTI – Type of Threat & Vuln

- **Advanced Persistent Threats (APTs)**: These are sophisticated, stealthy attacks by skilled actors, often backed by nation-states, targeting specific entities for espionage or disruption.
- **Ransomware**: This type of malware encrypts victim data or systems, demanding a ransom for decryption and threatening data deletion or exposure if unpaid.
- **Malware**: Various malware types compromise organizational files, systems, or networks, employing techniques like encryption, obfuscation, or polymorphism to evade detection.
- **Phishing and Social Engineering**: These threats manipulate individuals through deceptive tactics that exploit human vulnerabilities, such as spoofing or impersonation.
- **Network and Web Application Threats**: Attacks that exploit network or web application vulnerabilities, using methods like scanning, brute-forcing, or injection.

(Some) Tactical CTI - Result

- **Malware Signatures**: Unique identifiers for malicious software.
- **IP and URL Blacklists**: Lists of known malicious IP addresses and URLs.
- **Traffic Patterns**: Analysis of network traffic to identify suspicious behavior.
- **Log Files**: Records of events that occur within an organization's systems.
- **Credentials**: Information found in campaigns such as Advanced Persistent Threats (APTs), ransomware, and phishing attacks.

Tactical CTI - Technique

- All as in Strategi CTI, and …
- **Malware Analysis**: This involves dissecting and reverse-engineering malware to understand its purpose, behavior, and origins, and to extract Indicators of Compromise (IOCs) like file hashes, domain names, and IP addresses.
- **Network Analysis**: This is the practice of scrutinizing network traffic to spot communication patterns, protocols, and ports indicative of threat actors, and to identify and segregate malicious or unusual network activities.
- Security Tools and Systems: These include solutions like antivirus, firewalls, IDS/IPS, EDR, and SIEM systems that gather, process, analyze, and act upon data and information to maintain cybersecurity.

Tactical CTI – Relation

- Tactical CTI supports and implements the strategic CTI, by providing the technical details and evidence for the strategic intelligence, and by executing the security strategy and decisions of the organization
- Tactical CTI relies on and feeds the operational CTI, by providing the raw data and information for the operational intelligence, and by receiving the analysis and guidance from the operational intelligence

Tactical CTI - Illustration

- APT: how to use OSINT, malware analysis, and network analysis to identify and attribute an APT campaign targeting a critical infrastructure sector, and how to use the Cyber Kill Chain, the Diamond Model, and the MITRE ATT&CK to understand and exploit the TTPs and IOCs of the threat actor, and to devise and implement effective defensive and offensive strategies.
- Ransomware: how to use malware analysis and network analysis to detect and analyze a ransomware infection affecting a large enterprise, and how to use the Cyber Kill Chain, the Diamond Model, and the MITRE ATT&CK to understand and exploit the TTPs and IOCs of the threat actor, and to recover and restore the encrypted data and systems, as well as to prevent future attacks.

Operational CTI - Objective

- **Threat Identification**: To detect and comprehend the specifics and timing of cyber threats, including the indicators, events, or alerts, and their present or impending occurrence and impact.
- **Security Guidance**: To inform and direct the detection and prevention measures within an organization, including the configuration and fine-tuning of security tools and systems, and the application and enforcement of security controls, policies, or procedures.
- **Communication and Training**: To inform and train security operators and technicians, such as administrators, engineers, or analysts, about cyber threats and the necessary security measures.

Operational CTI – Type of Threat & Vuln

- **Active Threats**: Known and unknown threats that circumvent security measures and operate within the network, like malware and phishing.
- **Accuracy Issues**: False positives and negatives from security tools that lead to incorrect alerts or overlooked threats.
- **Adaptive Threats**: Threats that modify their methods to evade detection, utilizing new technologies and trends for attacks, including zero-day exploits and APTs.

Operational CTI - Result

- **Alerts and Warnings**: Notifications about current or imminent threats.
- **Threat Feeds**: Streams of data related to threat indicators.
- **Security Orchestration, Automation, and Response (SOAR) Platforms**: Tools that help automate the response to cyber threats.
- **Incident Response Platforms**: Systems that manage and mitigate the effects of cyber attacks.
- **Vulnerability Management Tools**: Software that identifies, categorizes, and helps remediate vulnerabilities.

Operational CTI - Technique

- Same as Tactical and …
- The indicators of compromise (IOCs) that provide pieces of digital forensics that suggest that a file, system, or network may have been breached or attacked, such as IP addresses, domain names, URLs, email addresses, network traffic patterns, filenames, paths, or hash files
- The threat feeds that provide sources of data and information that provide IOCs and other threat intelligence, such as threat actor profiles, tactics, techniques, and procedures (TTPs), or vulnerability reports, from various sources, such as open source, commercial, or internal, and in various formats, such as reports, alerts, or APIs

Operational CTI - Illustration

- DDoS attack: how to use SIEM, TIP, and SOAR to detect and analyze a DDoS attack targeting the organization's website, and how to use the intelligence requirements, the intelligence cycle, and the TLP to understand and exploit the TTPs and IOCs of the threat actor, and to devise and implement effective defensive and offensive strategies.
- Web application attack: how to use SIEM, TIP, and SOAR to detect and analyze a web application attack exploiting a SQL injection vulnerability, and how to use the intelligence requirements, the intelligence cycle, and the TIP to understand and exploit the TTPs and IOCs of the threat actor, and to devise and implement effective defensive and offensive strategies.

Operational CTI - Illustration

- Credential stuffing: how to use SIEM, TIP, and SOAR to detect and analyze a credential stuffing attack targeting the organization's online service, and how to use the intelligence requirements, the intelligence cycle, and the TIP to understand and exploit the TTPs and IOCs of the threat actor, and to devise and implement effective defensive and offensive strategies.

Legal and Ethical Issues

- Privacy
- Accuracy
- Attribution
- Responsibility

Best Practices

- Define intelligence requirements
- Follow a “standardized” cycle/framework
- Embrace data analytics technologies

Some Pitfalls

- Data overload
- Bias
- Uncertainty
- Issues related to ethics & legality
- Adversary adaptation

CTI - Lifecycle

- Planning and Direction – defining the scope, objectives, and requirements for the CTI program, and establishing the roles, responsibilities, and processes for the CTI team.
- Collection – gathering and acquiring data and information from various sources, such as open source, commercial, or internal, that are relevant to the CTI requirements.
- Processing – transforming and enriching the collected data and information into a standardized and structured format that can be easily stored, searched, and analyzed.
- Analysis – interpreting and evaluating the processed data and information to generate intelligence that can answer the CTI requirements and provide insights into the threat landscape.
- Production – creating and presenting the intelligence products, such as reports, briefings, alerts, or indicators, that can communicate the key findings and recommendations of the analysis to the intended audience.
- Dissemination and Feedback – delivering and sharing the intelligence products to the relevant stakeholders, such as security teams, management, or customers, and soliciting and incorporating their feedback to improve the CTI process and products.

Indicators of Compromise (IOC)

- Indicator of Compromise (IoC) is a piece of digital evidence that suggests a network or system may have been breached.
  - a clue in digital forensics that helps information security professionals identify malicious activity or security threats, such as data breaches, insider threats, or malware attacks.

IOC - Usages

- Detection: IOCs can be used to scan and monitor files, systems, or networks for signs of compromise, such as malicious or anomalous behaviors, events, or artifacts.
- Identification: IOCs can be used to attribute and characterize the threat actor behind the compromise, such as their name, alias, affiliation, motivation, skill, resource, or method.
- Response: IOCs can be used to contain and mitigate the compromise, such as blocking, isolating, or removing the threat actor’s access, tools, or data.
- Prevention: IOCs can be used to prevent future compromises, such as patching, hardening, or updating the files, systems, or networks, or implementing security controls, policies, or procedures.

IOC - Noteworthy

- IOCs can provide
  - actionable and relevant information that can help security teams to detect and respond to cyber threats faster and more effectively
  - help security teams to understand and anticipate the threat actor's motives, capabilities, and tactics, and to improve their security posture and resilience
  - help security teams to leverage the collective knowledge and experience of the security community and industry, and to benefit from the shared and distributed threat intelligence.
- IOCs can be
  - noisy, incomplete, inaccurate, or outdated, and may require validation, verification, and prioritization before use
  - easily changed, obfuscated, or evaded by the threat actor, and may not be able to detect unknown or advanced threats.
  - sensitive, confidential, or proprietary, and may require proper handling, protection, and governance before sharing or using.