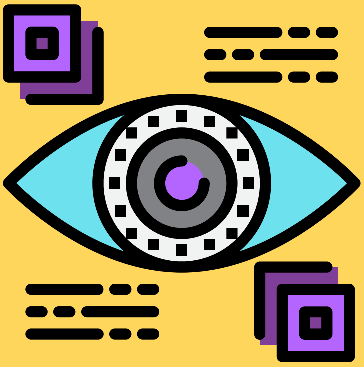

CYBER THREAT INTELLIGENCE

CTI Fundamentals

LetsDefend

CYBER THREAT INTELLIGENCE (CTI)

WHAT IS CYBER THREAT INTELLIGENCE?

If you are working in a defensive area in cyber security, you know that your organization is exposed to many attacks throughout the day.

Intelligence information plays an important role in cyber wars, as in wars. Thanks to the intelligence information, you can build necessary defense mechanisms before attacks and you can get the chance to be one step ahead of attackers.

- If you know others and know yourself, you will not be beaten in a hundred battles.
- If you do not know others but know yourself, you win one and lose one.
- If you do not know others and do not know yourself, you will be beaten in every single battle.

Sun Tzu

Cyber threat intelligence is an intelligence type that collects data from many sources and passes through necessary filters and analyzes to determine the motivations, targets and TTPs of cyber attacks and cyber threat actors that may be against your organization.

CYBER THREAT INTELLIGENCE (CTI)

CTI LIFECYCLE

Cyber threat intelligence goes through the following life cycle.

1. Planning: Determining the purpose, objective and requirements of the CTI
2. Collection: Collecting data from many sources
3. Processing: Processing the collected data and making it ready for analysis
4. Analysis: Analyzing the processed data, transforming the information into intelligence and making it ready for sharing
5. Dissemination: Sharing threat intelligence data
6. Feedback: Determining whether arrangements should be made for future threat intelligence operations by taking feedback from the reports shared.

BENEFITS OF CYBER THREAT INTELLIGENCE

Different threat intelligence services can provide you with different reports. In general, your organization can benefit in the following ways.

- By providing intelligence information on cyber threat actors, it gives you the chance to closely monitor threat actors who could harm your organization.
- By sharing IOC information obtained in cyber attacks against different organizations, it allows you to overcome possible attacks or to check whether you are affected by the cyber incident by using IOC information.
- It allows you to detect shares that may damage brand value.
- It allows you to detect of internal threats.

CYBER THREAT INTELLIGENCE (CTI)

CTI LIFECYCLE

Cyber threat intelligence goes through the following life cycle.

1. Planning: Determining the purpose, objective and requirements of the CTI
2. Collection: Collecting data from many sources
3. Processing: Processing the collected data and making it ready for analysis
4. Analysis: Analyzing the processed data, transforming the information into intelligence and making it ready for sharing
5. Dissemination: Sharing threat intelligence data
6. Feedback: Determining whether arrangements should be made for future threat intelligence operations by taking feedback from the reports shared.

CYBER THREAT INTELLİGENCE TYPES

There are 3 types of cyber threat intelligence.

1) Tactical Cyber Threat Intelligence
Tactical CTI provides more specific details about the tactics, techniques and procedures of threat actors, also known as TTP.

Usually Tactical CTI reports contain IOCs (data such as IP address, hash).

The following people or products usually use the type of strategic cyber threat intelligence.

- SOC Analyst
- Security Products (IPS/IDS/EDR/Firewall)
- SIEM Products

CYBER THREAT INTELLIGENCE (CTI)

2) Operational Cyber Threat Intelligence

Operational CTI; It allows you to understand cyber threat actor's motivations, goals and TTPs.

- Threat Hunters
- Incident Responders
- Security Engineers

3) Strategic Cyber Threat Intelligence

Strategic CTI; is an intelligence type that provides detailed analysis of trends and emerging risks to create an overall picture of the possible consequences of a cyber attack.

- C Level Executives
- Managers

CYBER THREAT INTELLIGENCE (CTI)

CYBER THREAT INTELLIGENCE GATHERING METHODS

Collecting threat intelligence data is the first step. In order to analyze and interpret the data, it is necessary to collect the data first.

Cyber threat intelligence data is divided into a few categories according to the collection methods.

1. OSINT: It is an intelligence typeobtained from open sources.
2. HUMINT: It is an intelligence type obtained from a person in the field.
3. GEOINT: It is an intelligence type obtained using satellite and aerial photographs.
4. SIGINT: It is a type of intelligence obtained by interfering with signals.