# PRACTICAL 1

**DATE: 23/01/2025**

**AIM:** To Understand the concept and Importance of cyber threat Intelligence and hunting.

## Understanding Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence (CTI) refers to the collection, analysis, and dissemination of information about current or potential cyber threats. The goal is to provide actionable insights to organizations to protect their systems, networks, and data from cyberattacks.

## What is CTI?

Cyber threat intelligence (CTI) is a cybersecurity field that involves collecting, analyzing, and sharing information about cyber threats. CTI helps organizations understand and respond to cyber threats by identifying vulnerabilities and threat actors.

## Importance of CTI in Real Life?

Cyber Threat Intelligence (CTI) plays a crucial role in modern cybersecurity by providing actionable insights to proactively identify, prevent, and respond to cyber threats. Here's how CTI is important in real-life scenarios:

**Proactive Threat Identification**

- Example: CTI helps organizations recognize indicators of compromise (IoCs) such as suspicious IP addresses or malware signatures. This allows them to patch vulnerabilities before an attack occurs.

**Enhancing Incident Response**

- Example: During a ransomware attack, CTI provides insights about the ransomware family, its attack vectors, and decryption methods.

**Reducing False Positives**

- Example: Security tools often generate numerous alerts, many of which are false positives. CTI refines this data by prioritizing alerts based on verified intelligence.

**Tailoring Security Defenses**

- Example: CTI identifies industry-specific threats (e.g., healthcare ransomware attacks) and helps organizations adapt their defenses accordingly.

**Enabling Threat Actor Profiling**

- Example: By analyzing CTI, organizations can understand attacker motives, techniques, and tools.

## Understanding Cyber Threat Hunting

Cyber Threat Hunting is a proactive approach to identifying and mitigating threats within an organization's environment. Unlike reactive methods (e.g., responding to alerts), hunting involves actively searching for hidden threats that evade traditional security measures.

## Importance of Threat Hunting

1. **Identifying Advanced Threats:** Finds sophisticated threats like zero-day attacks and APTs that bypass traditional defenses.
2. **Reducing Dwell Time:** Shortens the time attackers spend undetected within a network.
3. **Improving Defenses:** Insights gained during hunts are used to strengthen an organization's security posture.
4. **Complementing Automation**: While automation handles routine threats, hunting focuses on advanced adversaries.

# PRACTICAL 2

**DATE: 23/01/2025**

**AIM:** To gain Knowledge about framework, tools, and Technique for CTI and Threat- Hunting Operation.

## What is CTI?

Cyber threat intelligence (CTI) is a cybersecurity field that involves collecting, analyzing, and sharing information about cyber threats. CTI helps organizations understand and respond to cyber threats by identifying vulnerabilities and threat actors.

## Importance of CTI in Real Life?

Cyber Threat Intelligence (CTI) plays a crucial role in modern cybersecurity by providing actionable insights to proactively identify, prevent, and respond to cyber threats. Here's how CTI is important in real-life scenarios:

**Proactive Threat Identification**

- Example: CTI helps organizations recognize indicators of compromise (IoCs) such as suspicious IP addresses or malware signatures. This allows them to patch vulnerabilities before an attack occurs.

**Enhancing Incident Response**

- Example: During a ransomware attack, CTI provides insights about the ransomware family, its attack vectors, and decryption methods.

**Reducing False Positives**

- Example: Security tools often generate numerous alerts, many of which are false positives. CTI refines this data by prioritizing alerts based on verified intelligence.

### Tailoring Security Defenses

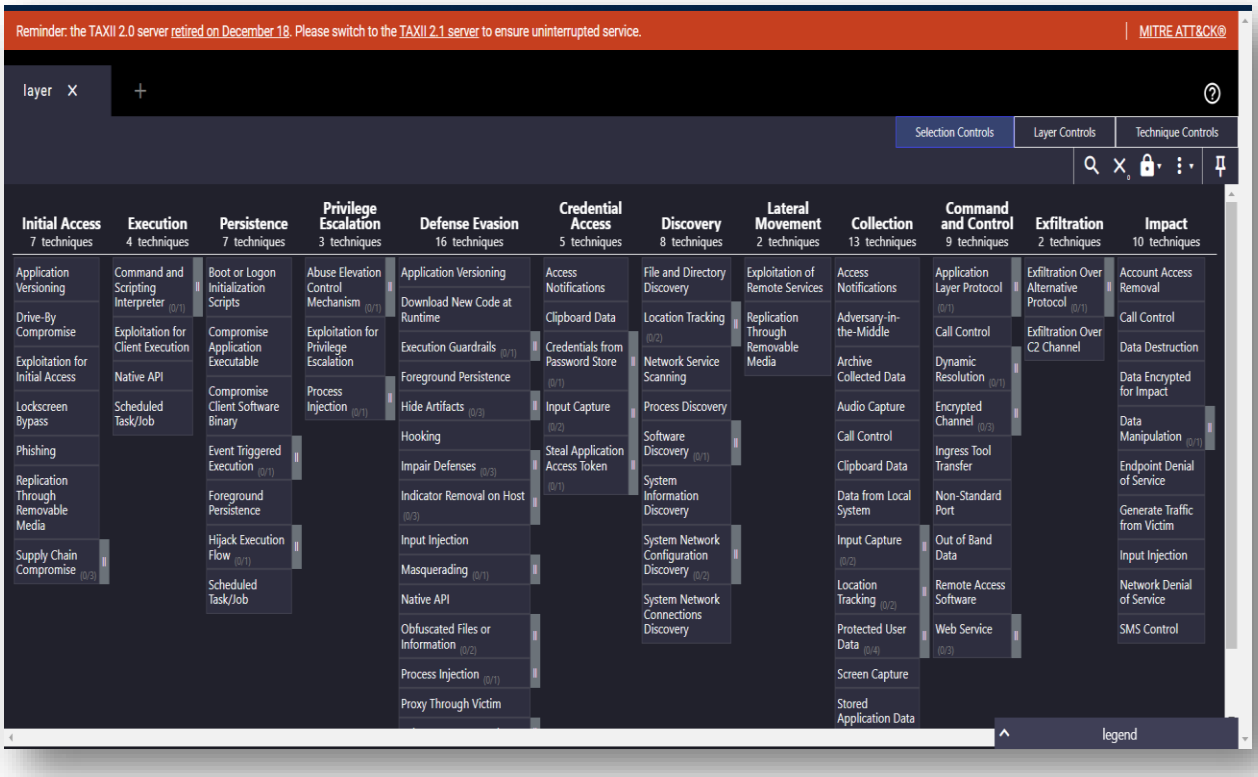
- Example: CTI identifies industry-specific threats (e.g., healthcare ransomware attacks) and helps organizations adapt their defenses accordingly.

### Enabling Threat Actor Profiling

- Example: By analyzing CTI, organizations can understand attacker motives, techniques, and tools.

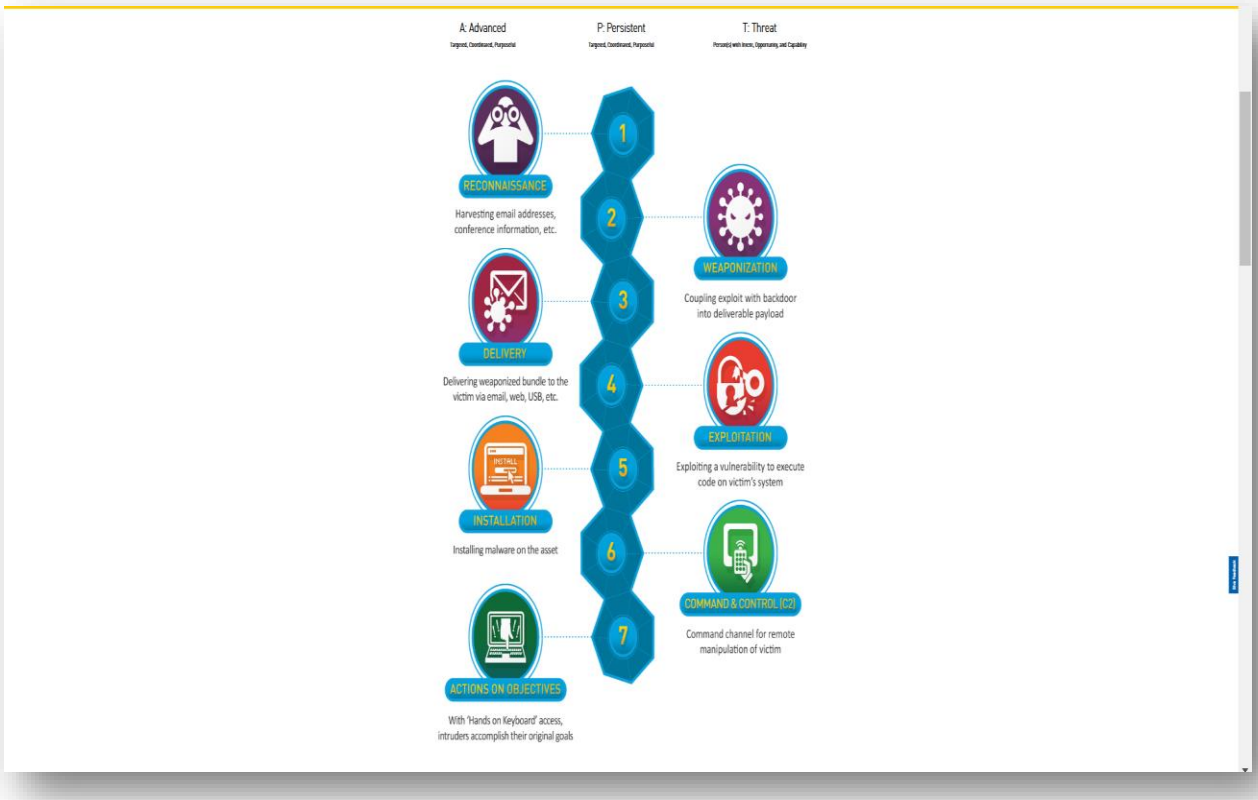
## CTI Frameworks:

1. **MITRE ATT&CK:**
   - Mainly Used in China and Iran.



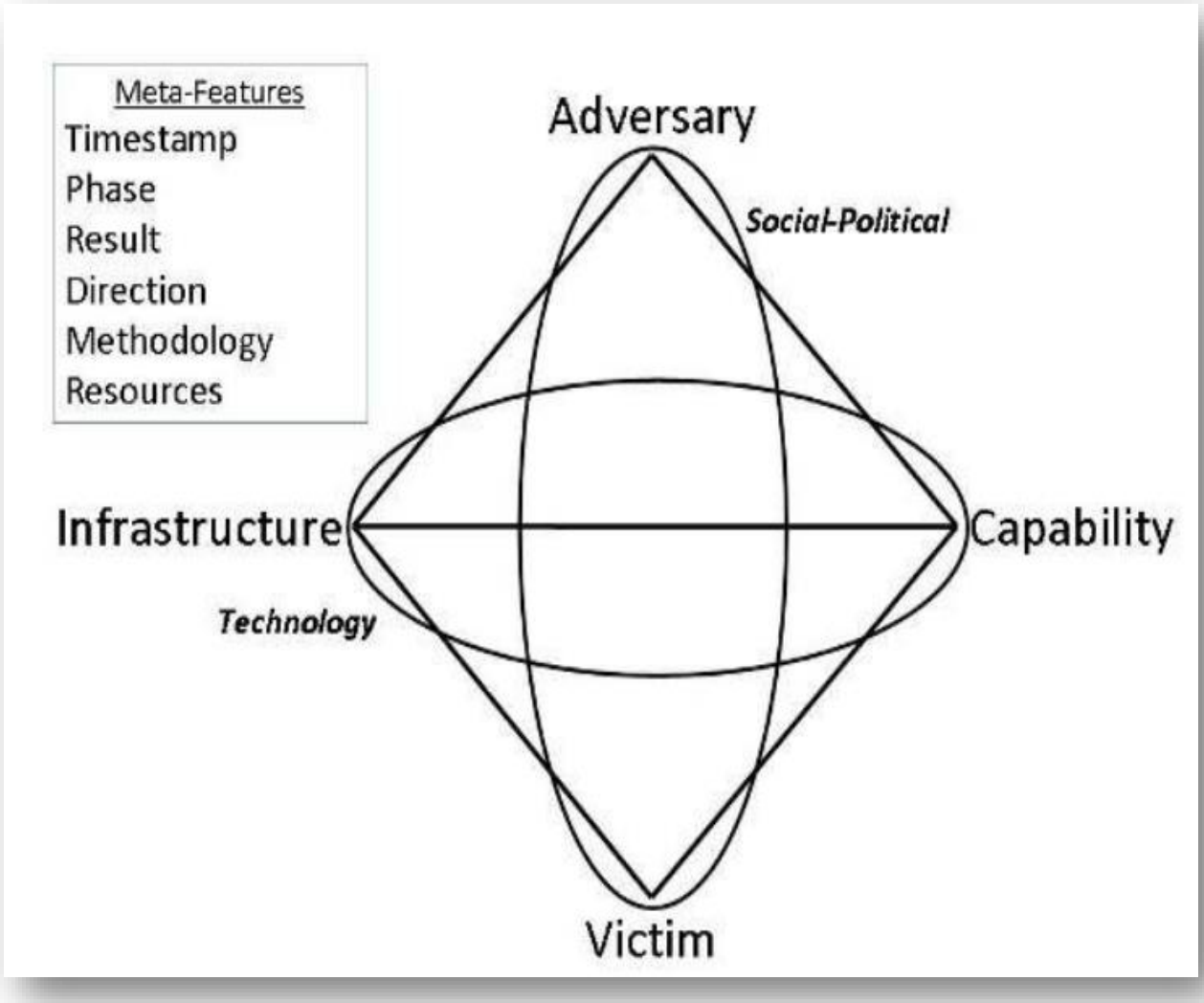
## 2. LOCKHEED MARTIN CYBER KILL CHAIN:

- Mainly Used in United States.



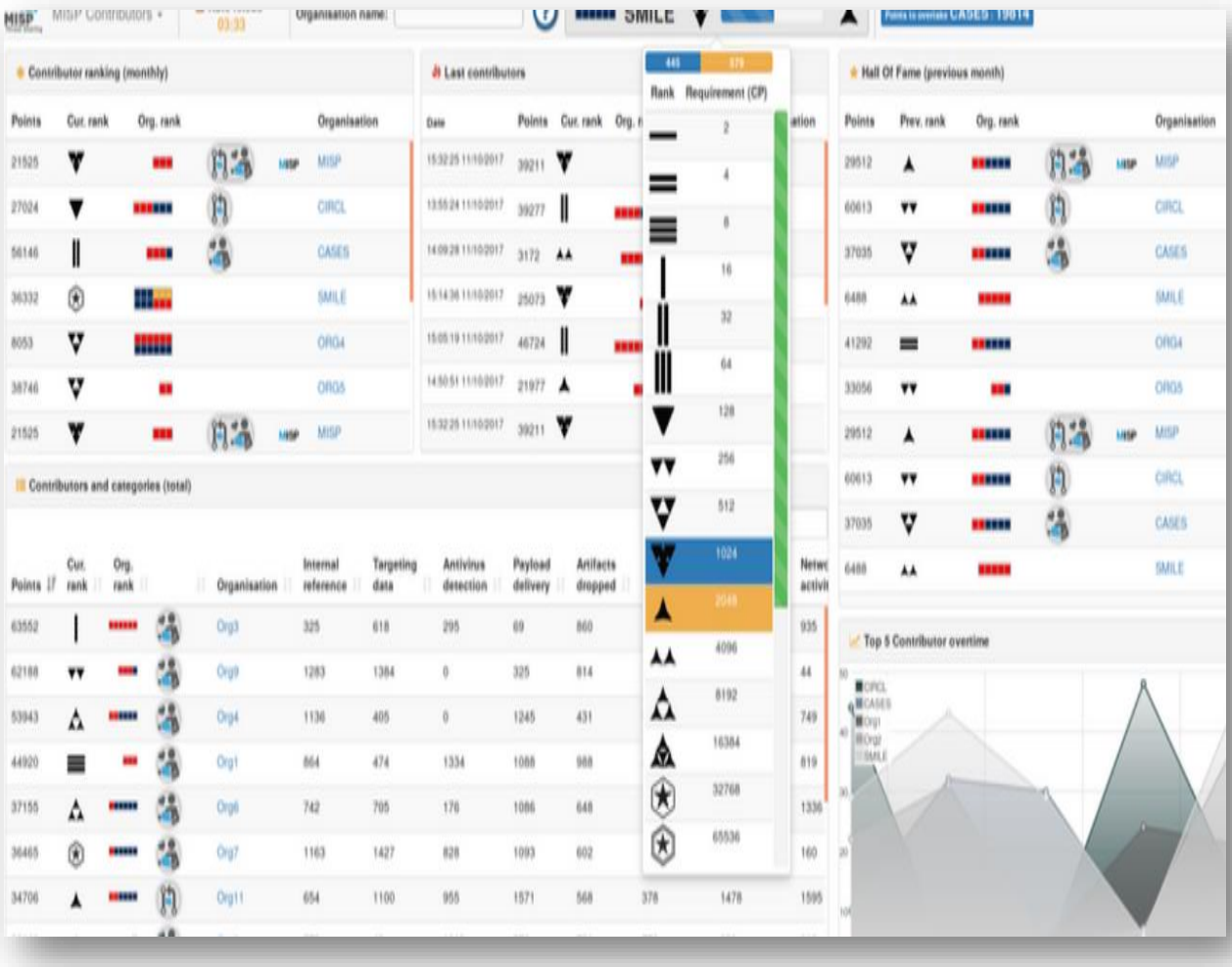
## 3. DIAMOND MODEL OF INTRUSION ANALYSIS:

- Mainly used in United State.

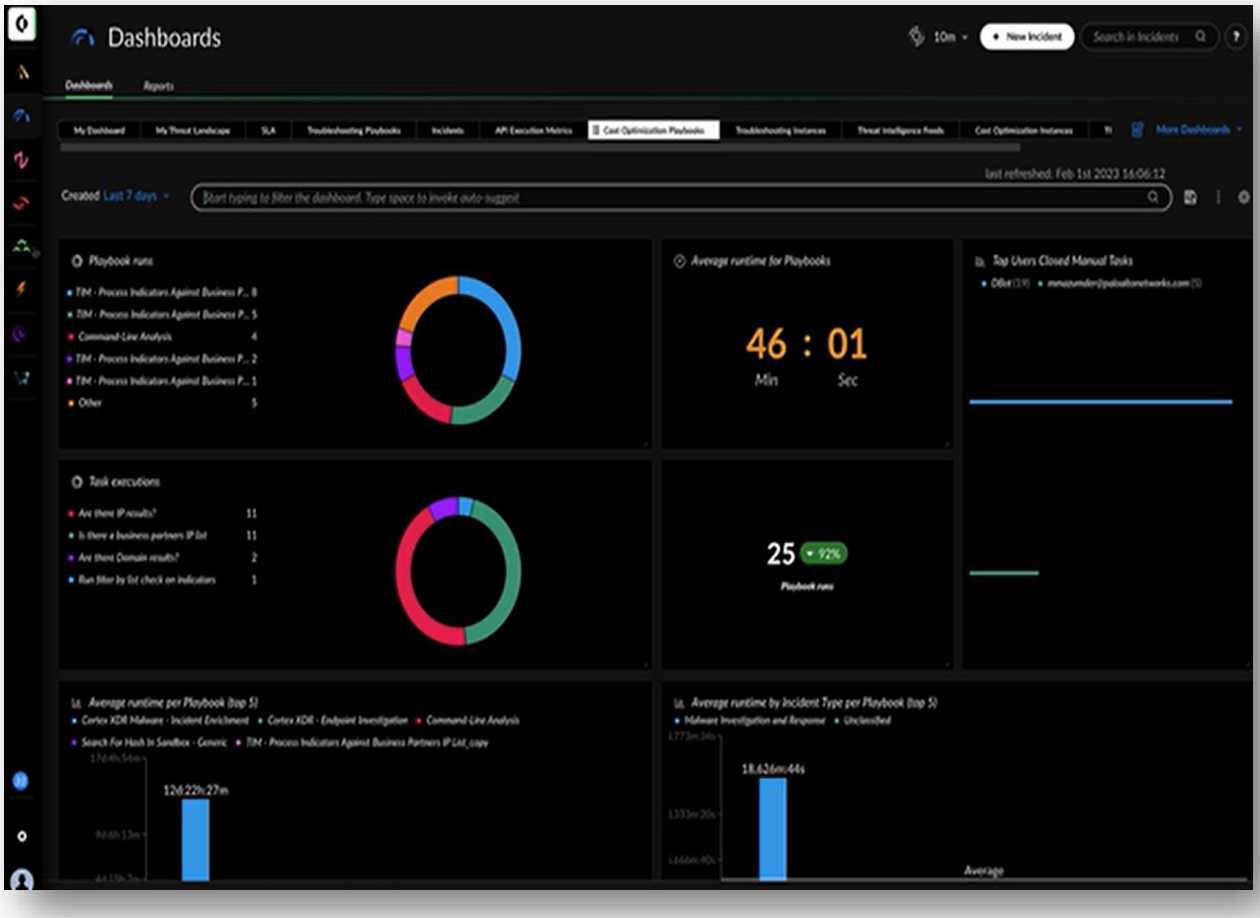


## CTI TOOLS:

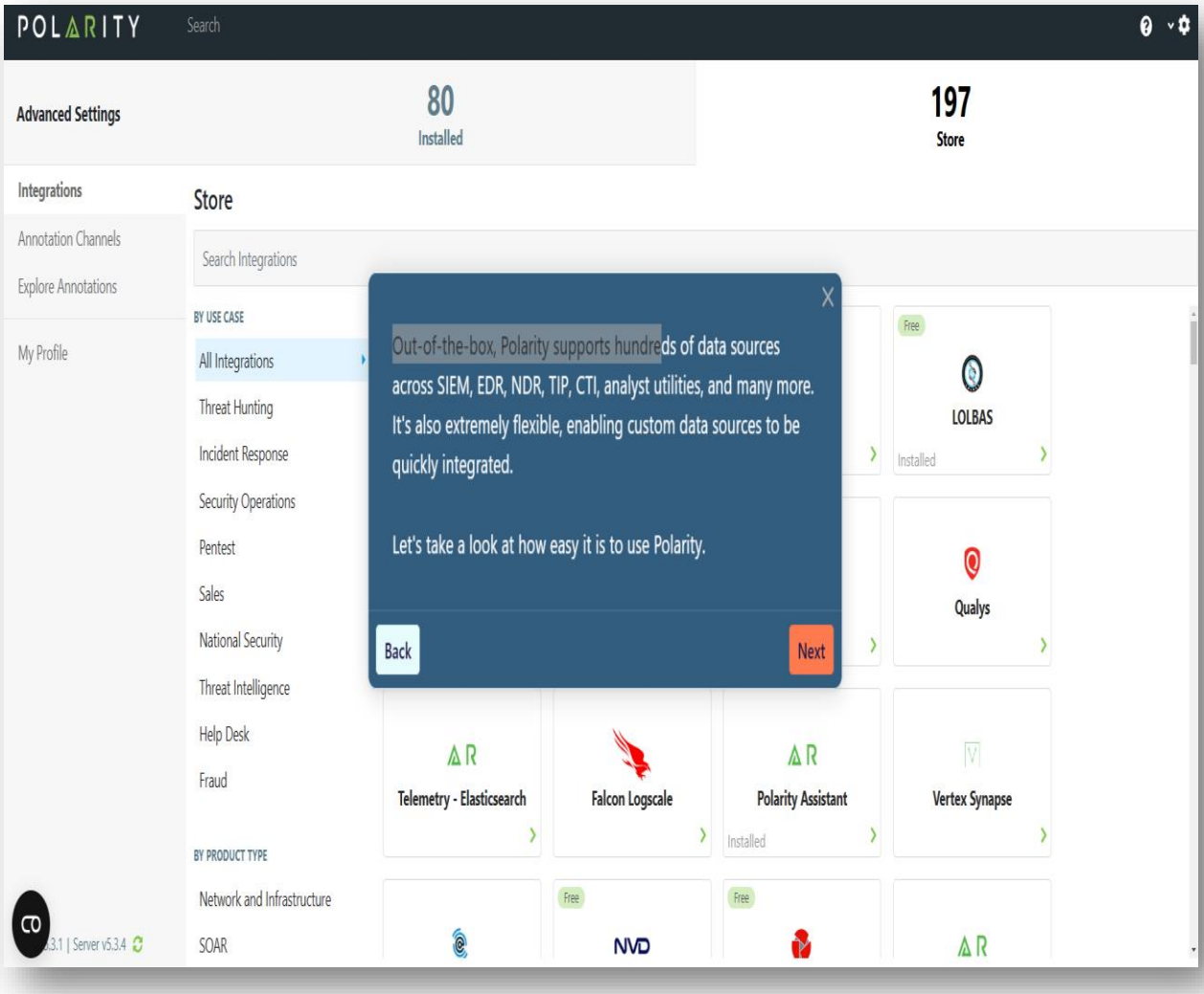
### 1. Malware Information Sharing Platform (MISP):



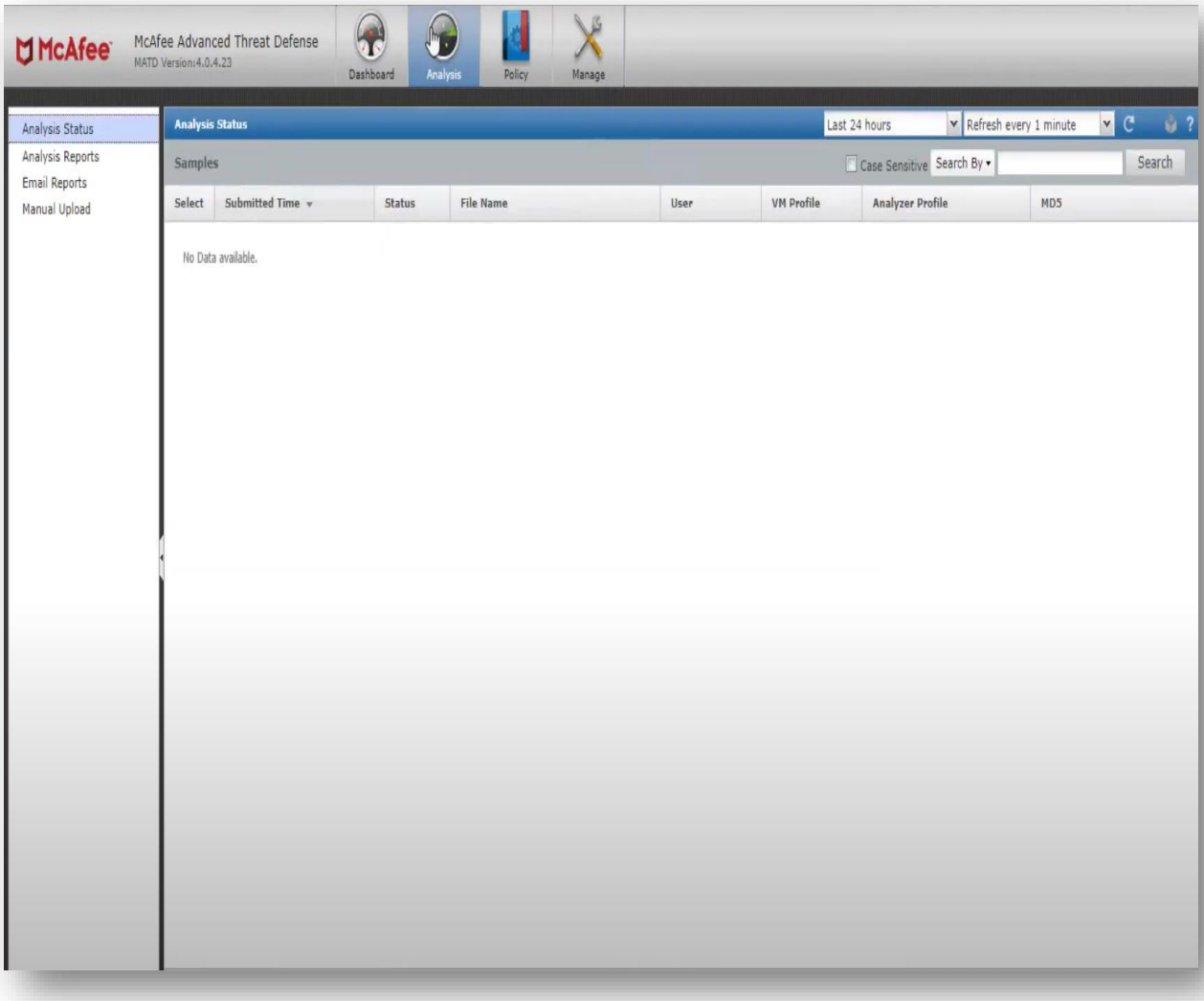
## 2. Cortex XSOAR:



## 3. POLARITY BY THREAT CONNECT:



## 4. OPENDXL BY McAfee:



## 5. VIRUS TOTAL:

## TECHNIQUES OF CTI:

1. Indicator of Compromise (IOC) Analysis
2. Tactics, Techniques, and Procedures (TTP) Analysis
3. Threat Hunting
4. Phishing Campaign Analysis
5. Attribution Analysis