
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.

Reminder: the TAXII 2.0 server retired on December 18. Please switch to the TAXII 2.1 server to ensure uninterrupted service. MITRE ATT&CK®

Initial Access 7 techniques	Execution 4 techniques	Persistence 7 techniques	Privilege Escalation 3 techniques	Defense Evasion 16 techniques	Credential Access 5 techniques	Discovery 8 techniques	Lateral Movement 2 techniques	Collection 13 techniques	Command and Control 9 techniques	Exfiltration 2 techniques	Impact 10 techniques
Application Versioning	Command and Scripting Interpreter (0/1)	Boot or Logon Initialization Scripts	Abuse Elevation Control Mechanism (0/1)	Application Versioning	Access Notifications	File and Directory Discovery	Exploitation of Remote Services	Access Notifications	Application Layer Protocol (0/1)	Exfiltration Over Alternative Protocol (0/1)	Account Access Removal
Drive-By Compromise	Exploitation for Client Execution	Compromise Application Executable	Exploitation for Privilege Escalation	Download New Code at Runtime	Clipboard Data	Location Tracking (0/2)	Replication Through Removable Media	Adversary-in-the-Middle	Call Control	Exfiltration Over C2 Channel	Call Control
Exploitation for Initial Access	Native API	Compromise Client Software Binary	Process Injection (0/1)	Execution Guardrails (0/1)	Credentials from Password Store (0/1)	Network Service Scanning	Process Discovery	Archive Collected Data	Dynamic Resolution (0/1)		Data Destruction
Lockscreen Bypass	Scheduled Task/Job			Foreground Persistence	Input Capture (0/2)			Audio Capture	Encrypted Channel (0/3)		Data Encrypted for Impact
Phishing		Event Triggered Execution (0/1)		Hide Artifacts (0/2)	Steal Application Access Token (0/1)	Software Discovery (0/1)		Call Control	Ingress Tool Transfer		Data Manipulation (0/1)
Replication Through Removable Media		Foreground Persistence		Hooking		System Information Discovery		Clipboard Data	Non-Standard Port		Endpoint Denial of Service
Supply Chain Compromise (0/3)		Hijack Execution Flow (0/1)		Indicator Removal on Host (0/2)		System Network Configuration Discovery (0/2)		Data from Local System	Out of Band Data		Generate Traffic from Victim
		Scheduled Task/Job		Input Injection		System Network Connections Discovery		Input Capture (0/2)	Remote Access Software		Input Injection
				Masquerading (0/1)				Location Tracking (0/2)	Web Service (0/3)		Network Denial of Service
				Native API				Protected User Data (0/4)			SMS Control
				Obfuscated Files or Information (0/2)				Screen Capture			
				Process Injection (0/1)				Stored Application Data			
				Proxy Through Victim							

legend

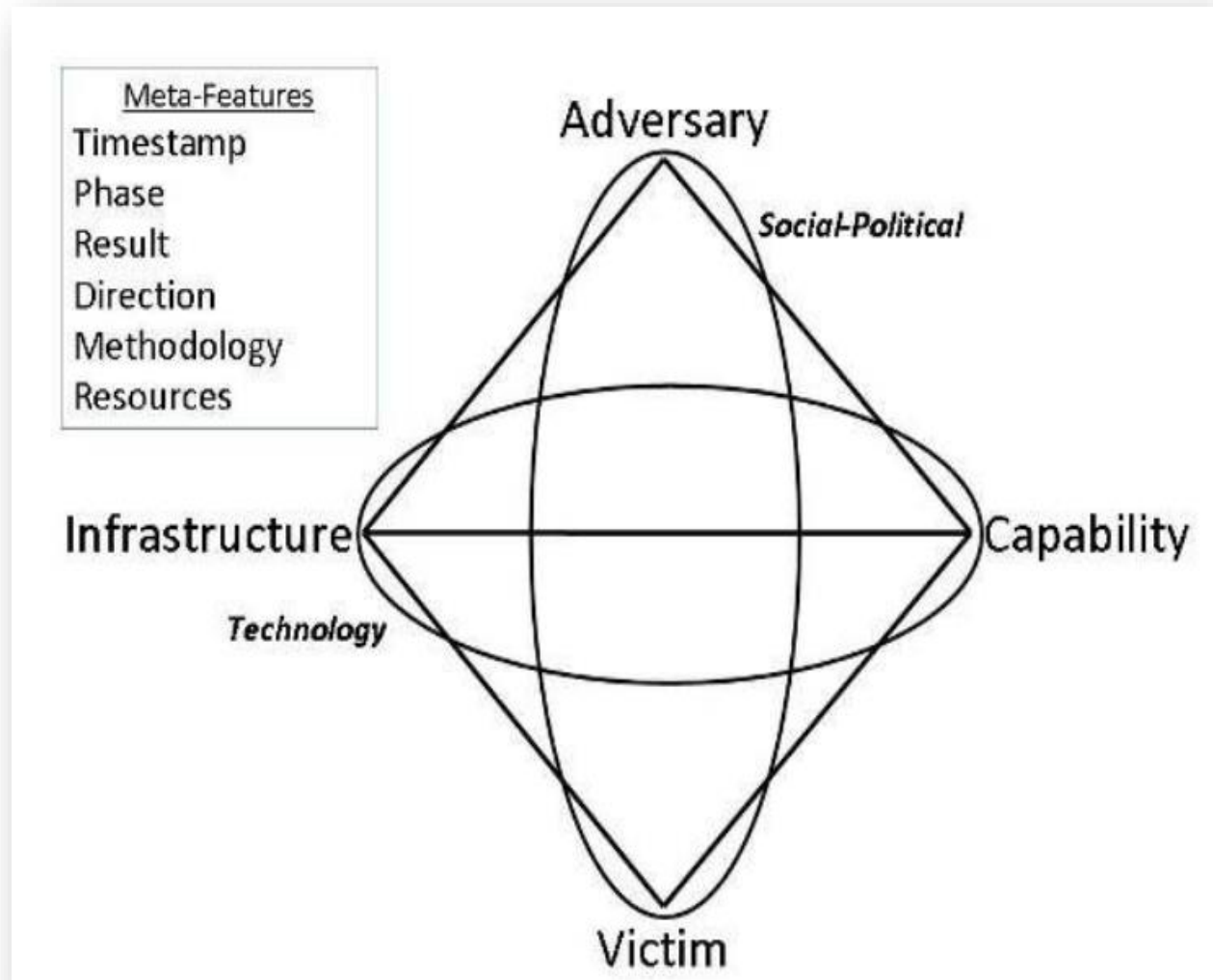
2. LOCKHEED MARTIN CYBER KILL CHAIN:

- Mainly Used in United States.



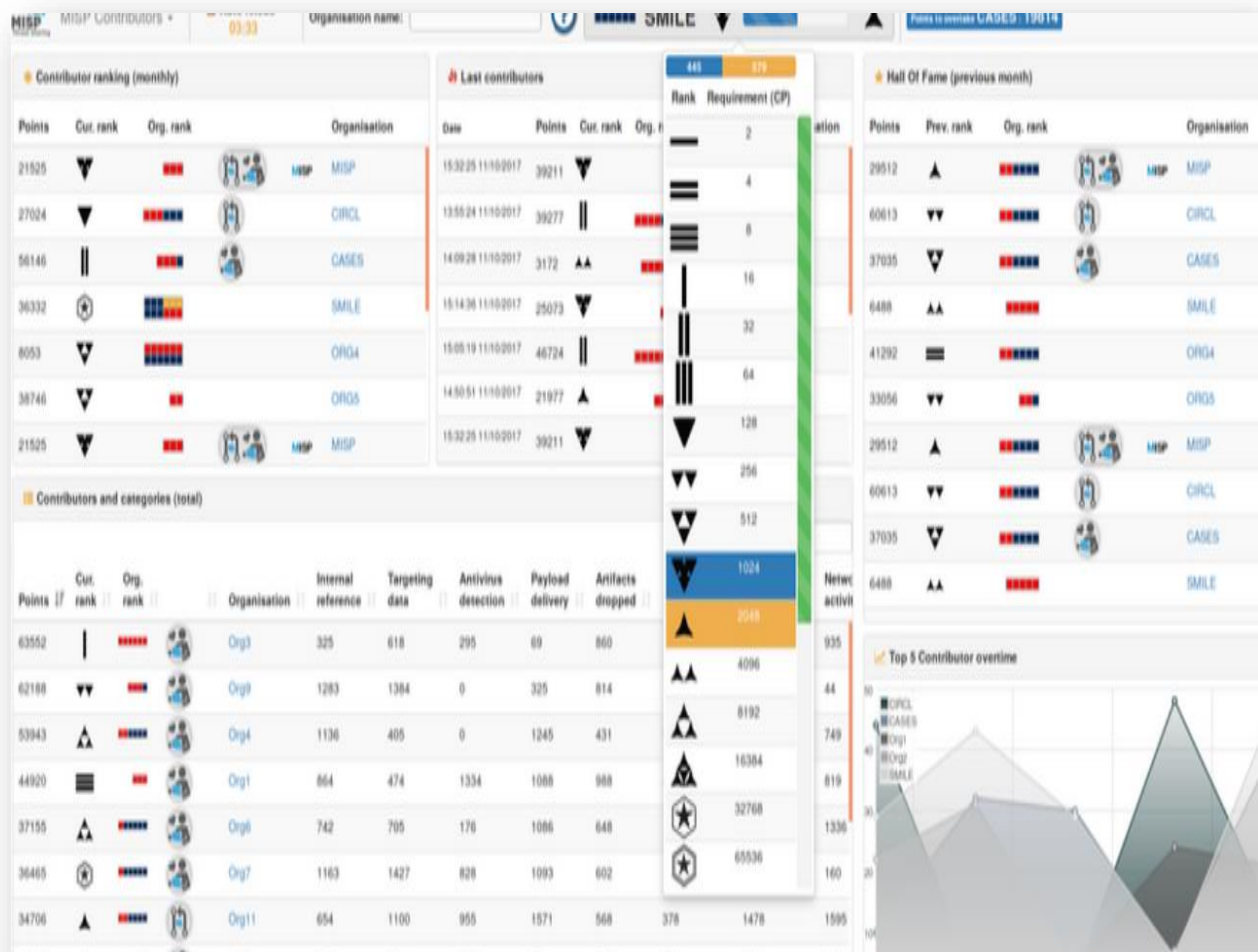
3. DIAMOND MODEL OF INTRUSION ANALYSIS:

- Mainly used in United State.

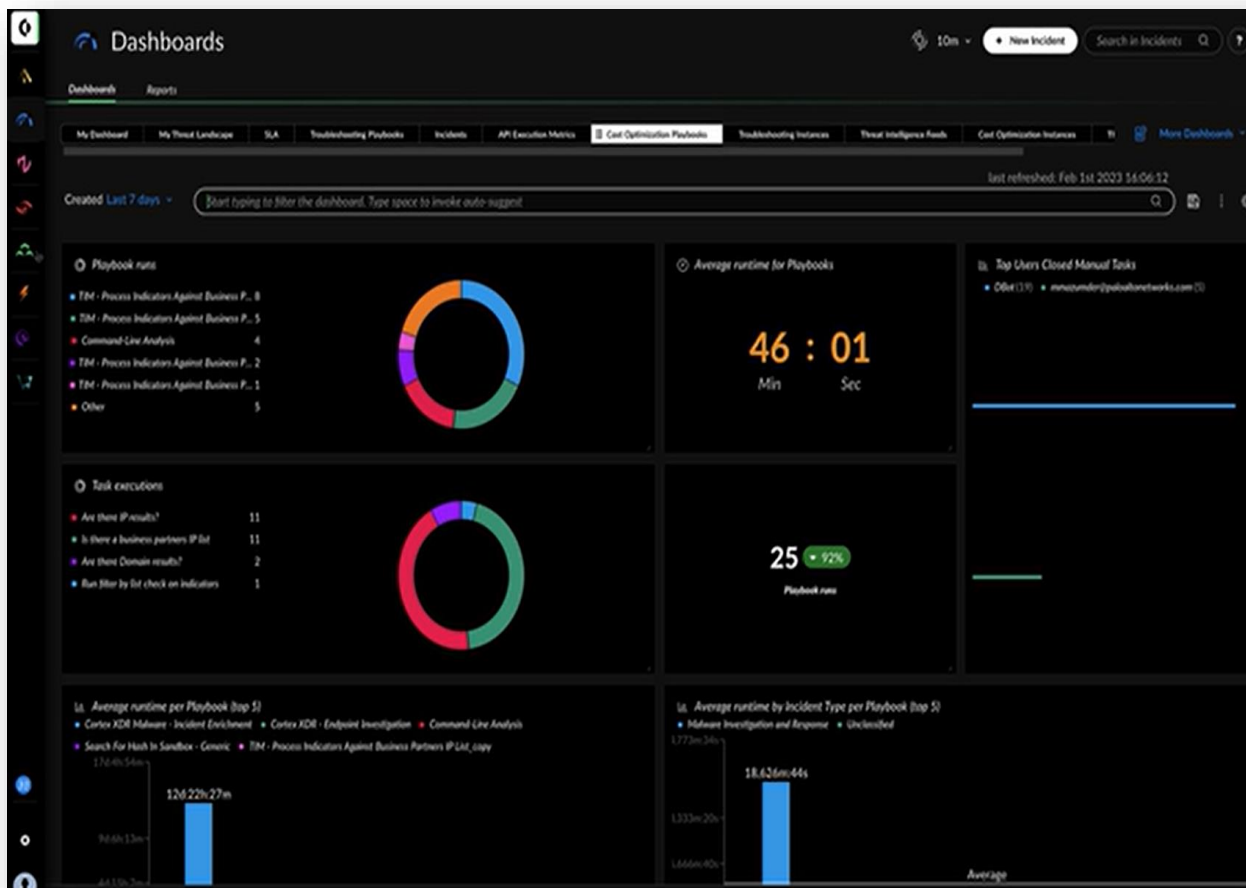


CTI TOOLS:

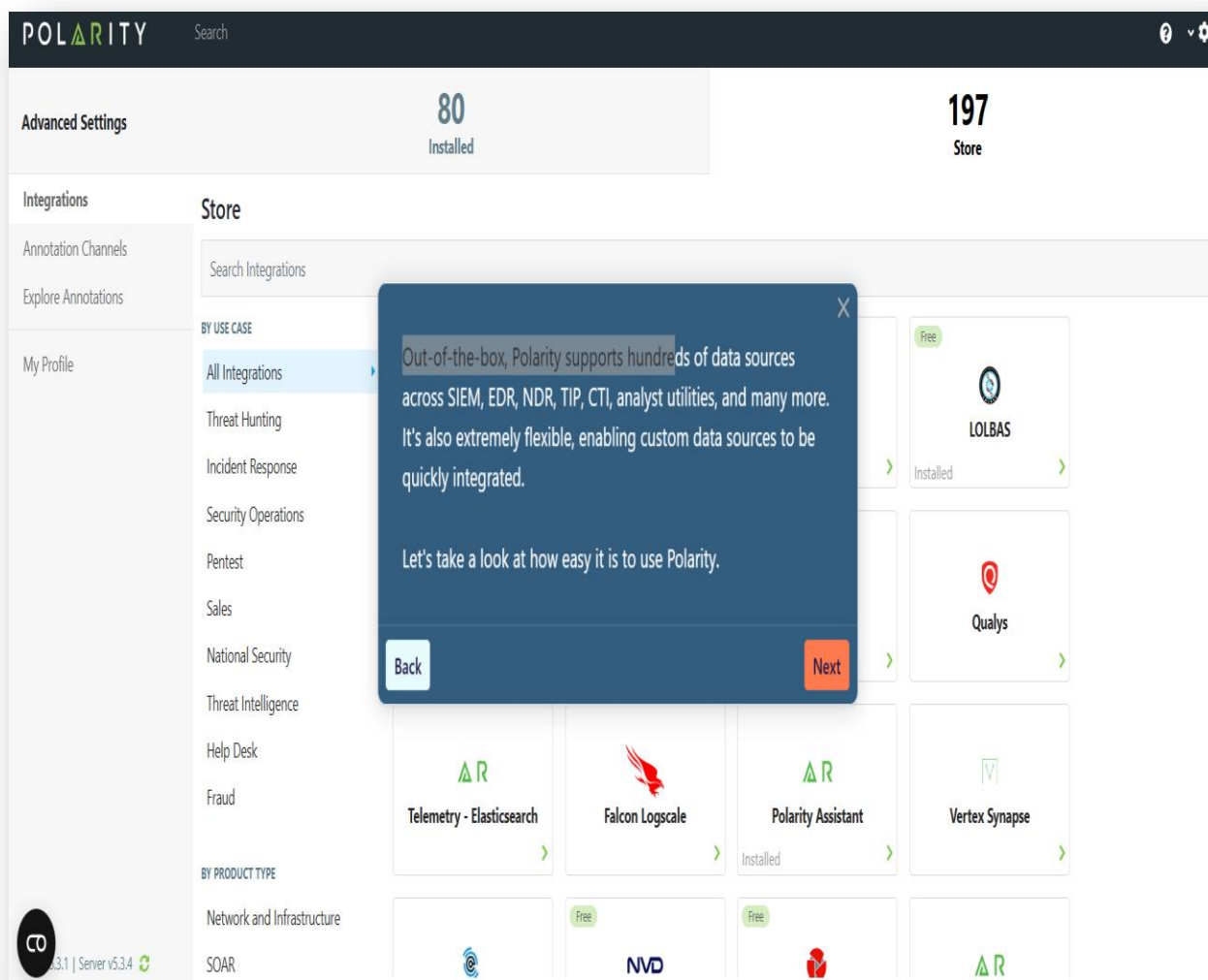
1. Malware Information Sharing Platform (MISP):



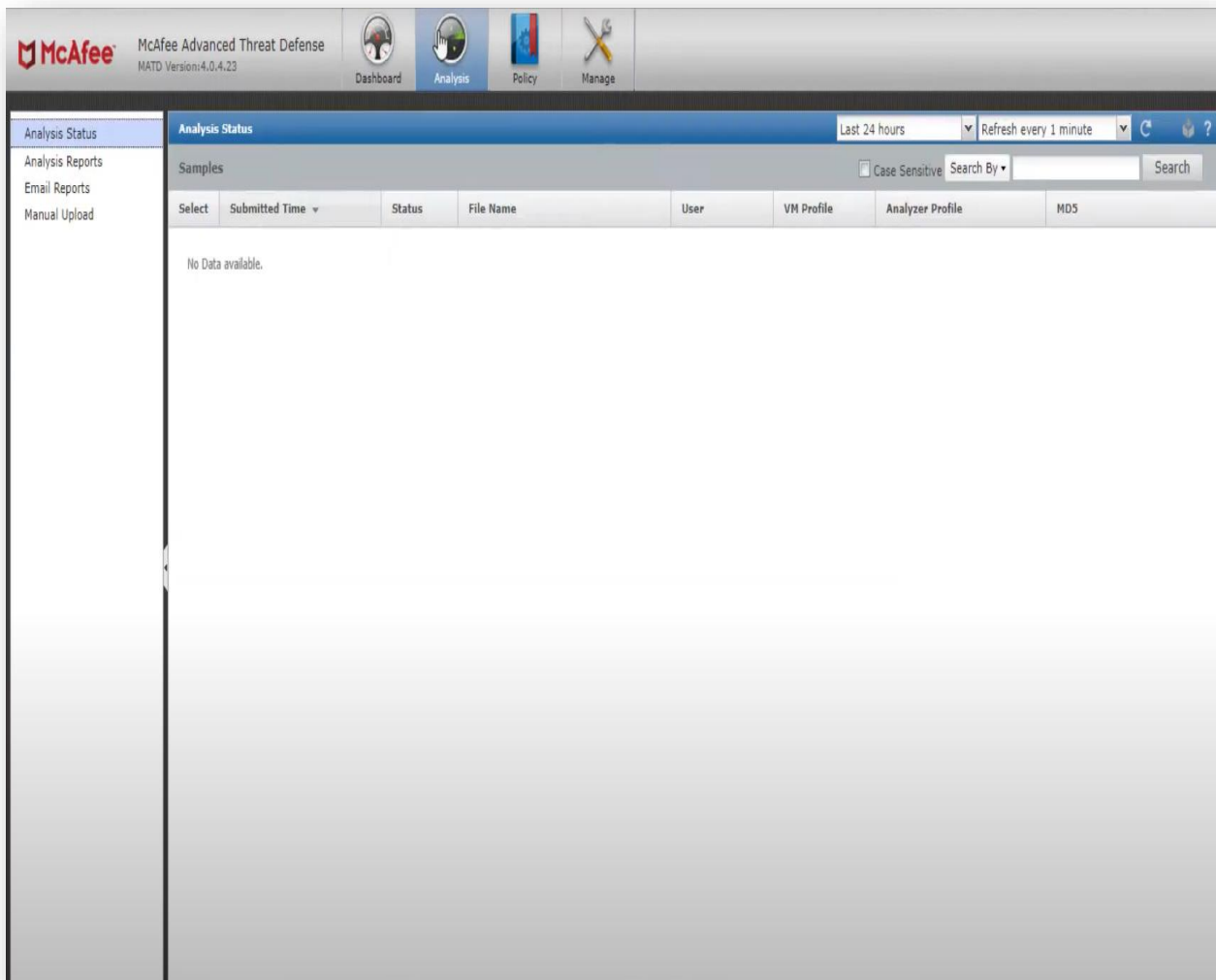
2. Cortex XSOAR:



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