

Course: Real time Cyber Threat Detection and Mitigation

Project: Cyber **Security** 4 **ALL** (CS4ALL)



Chapter 6: Threat Intelligence



Index

6.1 Threat Intelligence Overview

6.2 Threat Intelligence Platforms

6.3 Threat Intelligence Frameworks

6.4 Critical Data Protection
Capabilities

6.5 Vulnerability Assessment Tools

6.6 Port Scanning

6.7 Application Security Threats and
Attacks

6.8 SIEM Deployment

6.9 AI and SIEM

6.10 SOC Cyber Threat Hunting



6.1 Threat Intelligence Overview

What is Threat intelligence?

Potential Damage or Danger
+
Actionable Insights & Knowledge
Application
=
Threat Intelligence



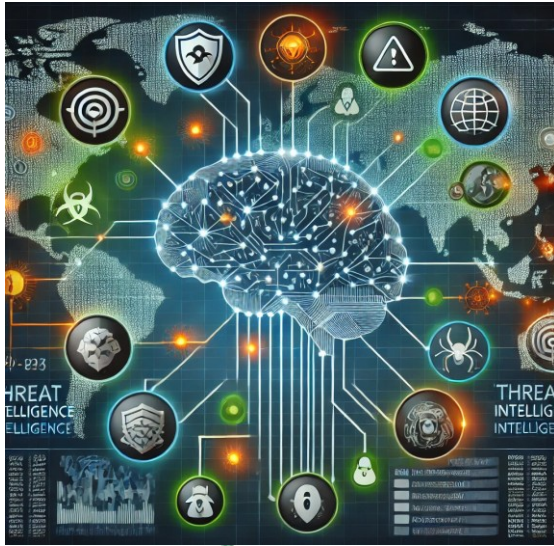
Threat Intelligence (TI)

- Refers to the information that organizations use to understand the threats targeting them
- Enabling proactive defense against cyberattacks, breaches, and other malicious activities
- Involves gathering, processing, and analyzing data related to potential or active threats to provide insights that help organizations improve their security posture.



Why Threat Intelligence is important?

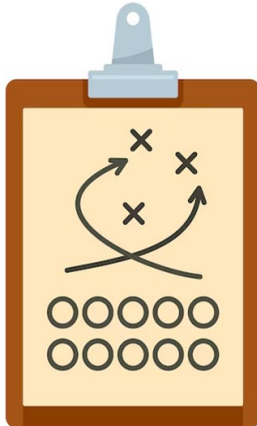
- To Identify Vulnerabilities
- Enhance Incident Response
- Inform Security Strategies



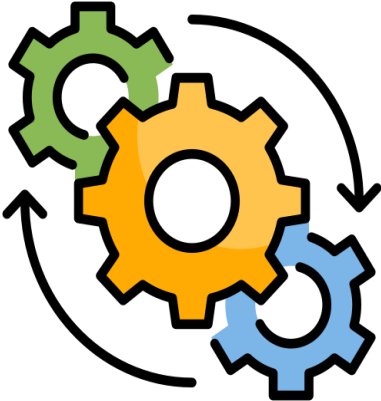
Types of Threat Intelligence



Strategic
Threat
Intelligence



Tactical
Threat
Intelligence



Operational
Threat
Intelligence



Types of Threat Intelligence

Strategic Intelligence:

- High-level information that provides insights into global trends, risks, and geopolitical threats.
- Helps senior leadership and decision-makers plan long-term security strategies.

Tactical Intelligence:

- Provides specific details about techniques, tactics, and procedures (TTPs) used by attackers.
- Helps security teams understand how attacks are carried out.

Operational Intelligence:

- Involves intelligence about specific events and incidents, such as ongoing attack campaigns and vulnerabilities being exploited.



6.2 Threat Intelligence Platforms

- Tools designed to collect, process, and organize threat intelligence data from multiple sources
- Enable organizations to centralize their threat intelligence efforts, providing a comprehensive view of potential threats.

Features of TIPs:

- Integration with Security Tools
- Automated Data Analysis
- Customizable Dashboards



6.3 Threat Intelligence Frameworks

Structured methods for gathering, analyzing, and using threat data, ensuring effective cyber threat management.

Components of Threat Intelligence Frameworks:

- Structured Approach
- Integration of Data
- Focus on Tactics, Techniques, and Procedures



The Most Commonly Used Frameworks for Threat Intelligence:

1. Cyber Kill Chain
2. Unified Cyber Kill Chain
3. The MITRE ATTACK Framework
4. Diamond Model of Intrusion Analysis



1. Cyber Kill Chain

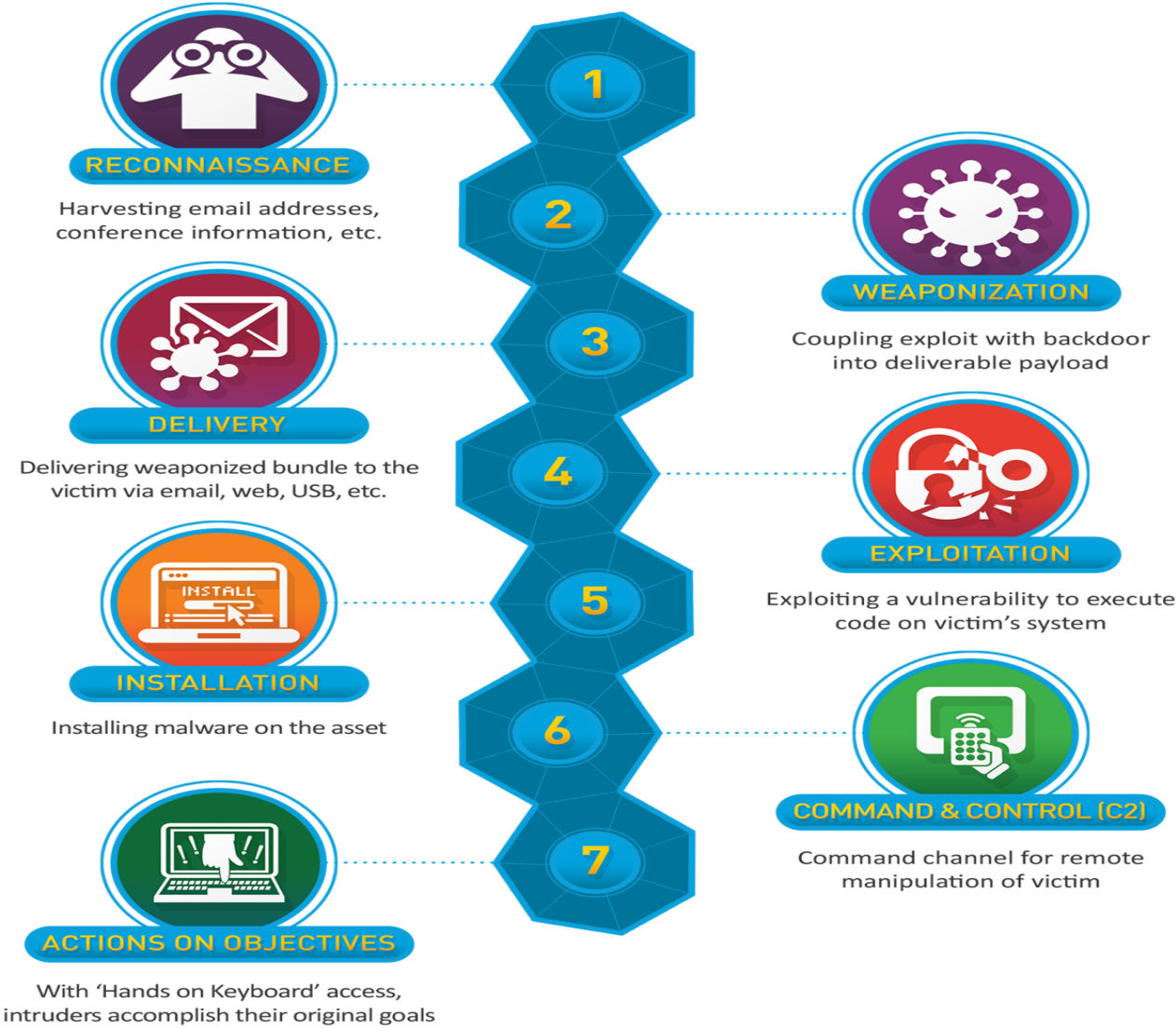
- Developed by Lockheed Martin, the Cyber Kill Chain framework, also known as the Cyber Attack Lifecycle, breaks down attacks into stages to identify and disrupt adversarial activities.



Co-funded by
the European Union



The Cyber Kill Chain illustrated by Lockheed Martin



Co-funded by the European Union



Cyber Kill Chain (cont..)

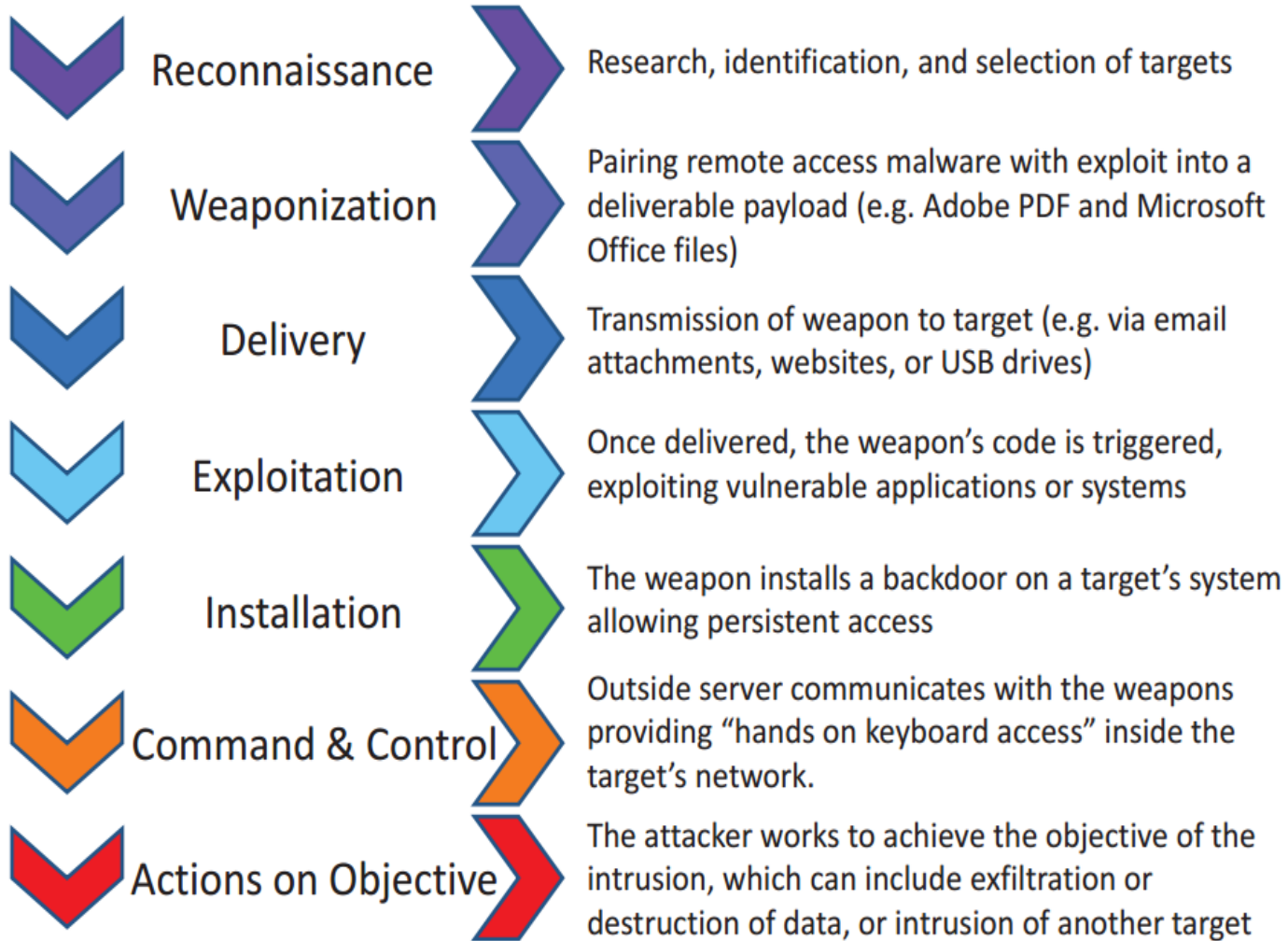
- has seven steps
- integrating threat intelligence with these steps helps organizations minimize the impact of cyber-attacks.



Co-funded by
the European Union



Phases of the Intrusion Kill Chain



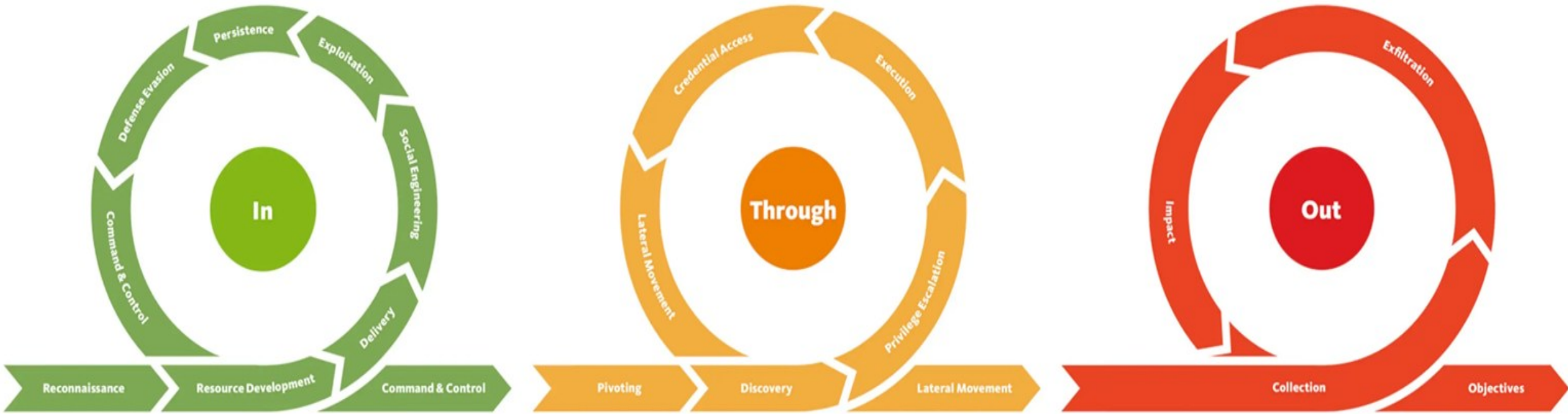
2. Unified Cyber Kill Chain

- In 2017, introduced by Paul Pols
- Augment and expand upon the Cyber Kill Chain. Incorporates elements from both the Lockheed Martin-Cyber Kill Chain and the MITRE ATTACK framework.

It distills the attack process into three high-level steps:

- Initial Foothold
- Network Propagation
- Action on Objectives.





The Unified Kill Chain includes 18 phases or tactics



Co-funded by
the European Union



The Unified Kill Chain 18 tactics in detail

The Unified Kill Chain

1	Reconnaissance	<i>Researching, identifying and selecting targets using active or passive reconnaissance.</i>
2	Weaponization	<i>Preparatory activities aimed at setting up the infrastructure required for the attack.</i>
3	Delivery	<i>Techniques resulting in the transmission of a weaponized object to the targeted environment.</i>
4	Social Engineering	<i>Techniques aimed at the manipulation of people to perform unsafe actions.</i>
5	Exploitation	<i>Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.</i>
6	Persistence	<i>Any access, action or change to a system that gives an attacker persistent presence on the system.</i>
7	Defense Evasion	<i>Techniques an attacker may specifically use for evading detection or avoiding other defenses.</i>
8	Command & Control	<i>Techniques that allow attackers to communicate with controlled systems within a target network.</i>
9	Pivoting	<i>Tunneling traffic through a controlled system to other systems that are not directly accessible.</i>
10	Discovery	<i>Techniques that allow an attacker to gain knowledge about a system and its network environment.</i>
11	Privilege Escalation	<i>The result of techniques that provide an attacker with higher permissions on a system or network.</i>
12	Execution	<i>Techniques that result in execution of attacker-controlled code on a local or remote system.</i>
13	Credential Access	<i>Techniques resulting in the access of, or control over, system, service or domain credentials.</i>
14	Lateral Movement	<i>Techniques that enable an adversary to horizontally access and control other remote systems.</i>
15	Collection	<i>Techniques used to identify and gather data from a target network prior to exfiltration.</i>
16	Exfiltration	<i>Techniques that result or aid in an attacker removing data from a target network.</i>
17	Impact	<i>Techniques aimed at manipulating, interrupting or destroying the target system or data.</i>
18	Objectives	<i>Socio-technical objectives of an attack that are intended to achieve a strategic goal.</i>



 Co-funded by
the European Union



3. The MITRE ATTACK Framework

- Widely recognized framework that offers a comprehensive, systematic, and actionable way to understand attacker behaviors
- Open-source cybersecurity framework
- Catalogs adversarial tactics, techniques, and procedures (TTPs)
- Provides comprehensive view of attacker behaviors



The MITRE ATTACK Framework (cont..)

- Serves as a universal dictionary for threat tactics
- Continuously updated by global security community
- Widely adopted for threat intelligence and defense strategies



ATTACK Matrix

Shows tactics as columns, and techniques as rows.

What are tactics, techniques, and procedures (TTPs)?

1. Tactics

- adversary's goals during an attack, representing the "why" of an attack.
- Examples of tactics:
- Initial Access
- Execution
- Persistence
- Privilege Escalation



ATTACK Matrix

- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Impact



ATTACK Matrix

Techniques

- describes "how" adversaries achieve their tactical goals.
- tactic includes multiple techniques, detailing specific methods adversaries use.

For instance:

- Phishing (under Initial Access)
- PowerShell (under Execution)
- Credential Dumping (under Credential Access)



ATTACK Matrix

Sub-Techniques

These provide more granular details on specific methods within a technique. For example:

- Phishing: Spear Phishing Attachment
- PowerShell: PowerShell Scripts



ATTACK Matrix

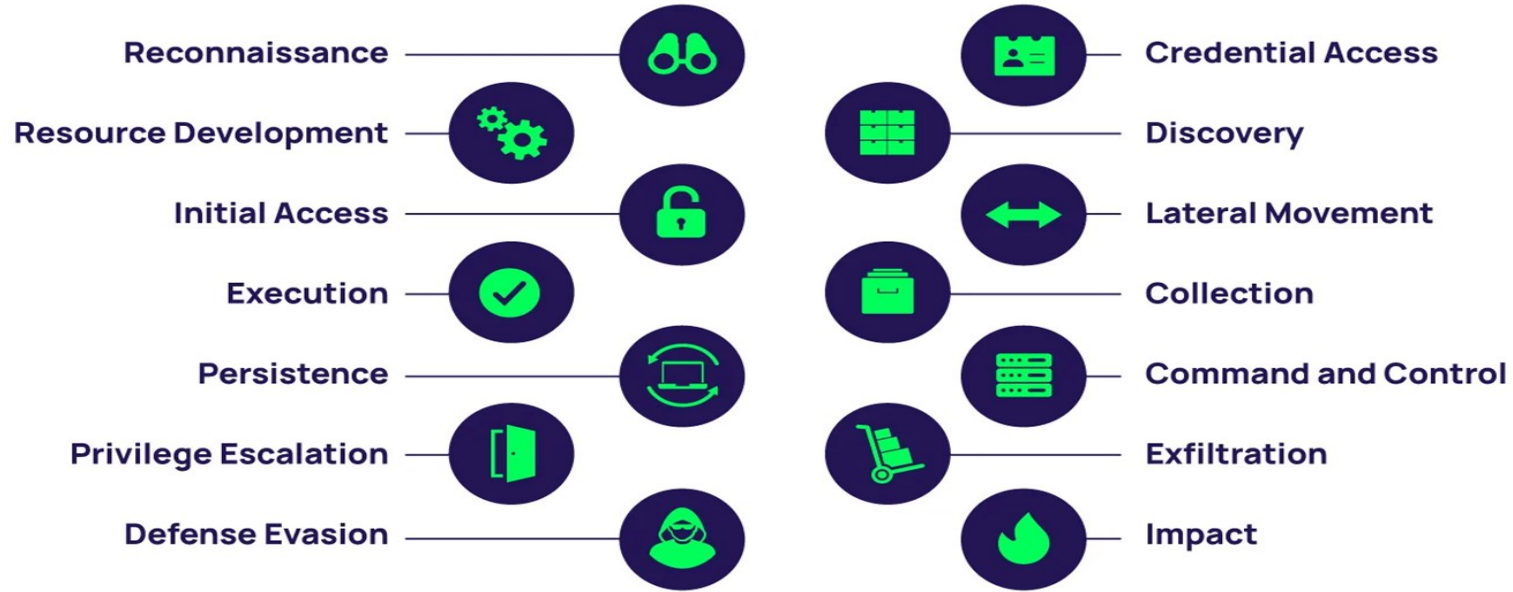
Procedures

- Specific implementations of techniques by adversaries.
- Offer practical examples of how particular techniques and sub-techniques are executed in real-world scenarios.
- Uses 14 different tactic categories to describe adversarial behaviours



MITRE ATTACK Matrix

MITRE ATT&CK Tactics in the Enterprise Matrix



 Co-funded by
the European Union



4. Diamond Model

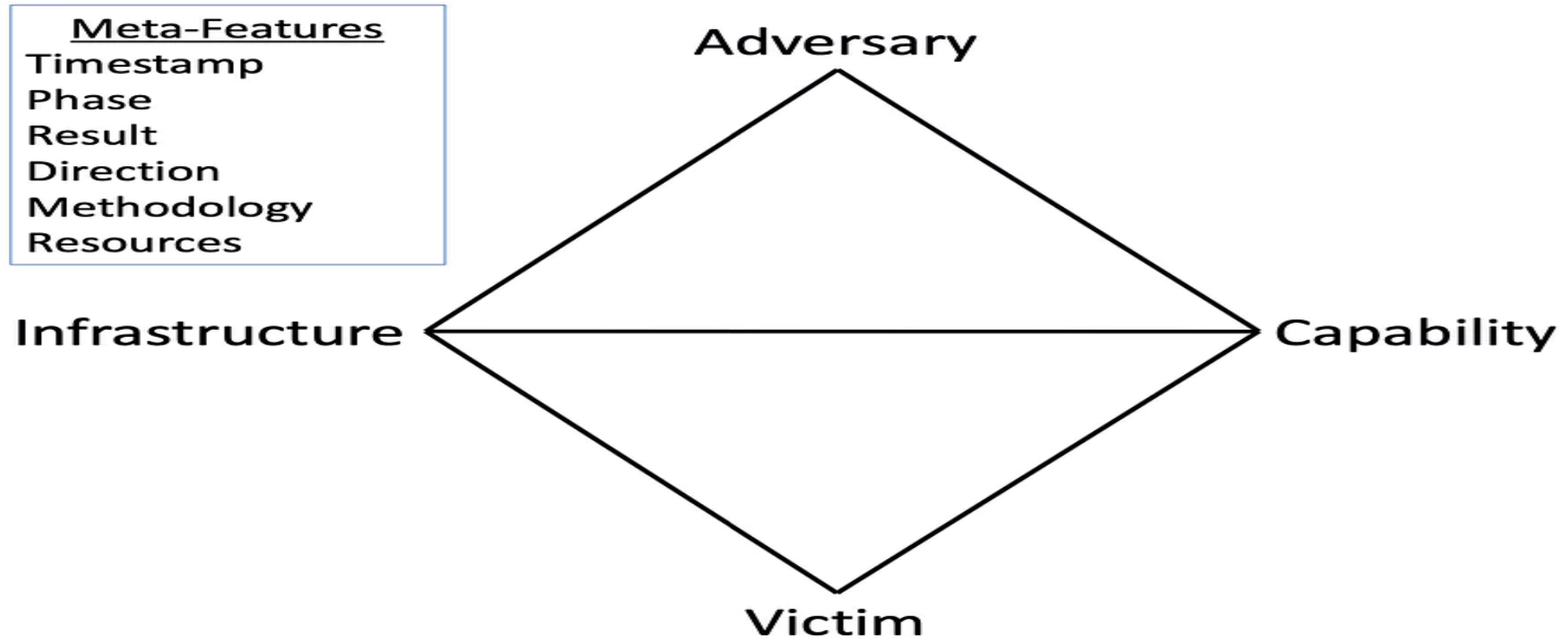
Threat modeling framework designed for intrusion analysis.

Four core components:

- Adversary
- Capability
- Infrastructure
- Victim (Target)



Diamond Model and Meta-Features



Meta-features of Diamond Model

The meta-properties and their descriptions:

- Timestamp
- Phase
- Result
- Direction
- Methodology
- Resources
- Social-political
- Technology



How to Use the Diamond Model for Threat Intelligence?

- Analyze Intrusions
- Develop Proactive Defenses
- Identify Intelligence Gaps
- Recognize Patterns
- Use in Conjunction with Other Models



Co-funded by
the European Union



6.4 Critical Data Protection Capabilities

Essential tools and practices that organizations use to safeguard their sensitive information.

Some key critical data protection capabilities:

- Data Encryption
- Access Control
- Data Backup and Recovery
- Data Masking
- Monitoring and Auditing
- Incident Response Plan
- Employee Training



6.5 Vulnerability Assessment Tools

- Software programs designed to scan IT infrastructure (computers, networks, applications) to find potential security weaknesses or vulnerabilities that hackers could exploit.

How Do They Work?

- Scanning
- Identification
- Analysis
- Reporting



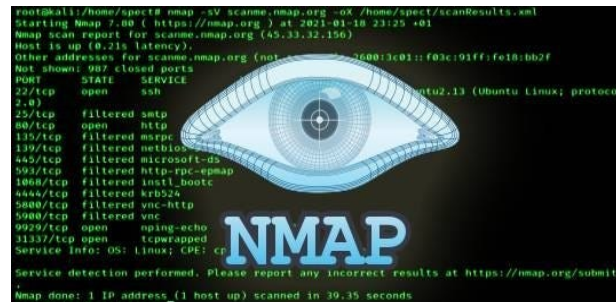
Types of Vulnerability Assessment Tools

- Network-based scanners
- Host-based scanners
- Wireless scanners
- Application scanners
- Database scanners



Popular Vulnerability Assessment Tools:

- Nessus
- OpenVAS
- Qualys
- Acunetix
- Nmap



6.6 Port Scanning

- Technique checks which ports on a network are open and can send or receive data
- Involves sending packets to ports and analyzing responses
- Requires initial host discovery through network scanning
- Helps map hosts to IP addresses
- **Goal:** Identify vulnerable servers and assess security levels



What are ports?

Central docking point for the flow of information from a program or the Internet, to a device or another computer in the network and vice versa.



Co-funded by
the European Union



What are port numbers?

- 16-bit unsigned integer that identifies a specific process or service on a device
- Ranges from 0 to 65535
- different numbers are used for different services.
 - Port 80 is used for HTTP (web traffic).
 - Port 21 is used for FTP (file transfer).
 - Port 25 is used for SMTP (email sending).



How Does a Port Scanner Operate?

A port scanner, such as nmap, works by sending traffic to a particular port and examining the results. It will respond in different ways to a port scan, including:

- Open
- Closed
- Filtered



Some of the common types of port scans include:

- Ping Scan
- SYN Scan
- TCP Connect Scan
- UDP Scan
- XMAS and FIN Scans
- FTP Bounce Scan



Legitimate Uses of Port Scanning:

- Identifies open ports and potential vulnerabilities in a network.
- Helps administrators monitor and manage network resources and configurations.
- Ensures that only required ports are open, adhering to security policies and standards.
- Troubleshooting



Illegitimate Uses of Port Scanning

- Used by attackers to find vulnerabilities and potential entry points for unauthorized access.
- Information Gathering
- Part of the initial phase of an attack to map out the network and identify targets.
- Scans for open ports to exploit unprotected services or software.



6.7 Application Security Threats and Attacks

Refer to vulnerabilities and malicious activities that target software applications, aiming to compromise their integrity, confidentiality, or availability.

Types of application security threats

- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Security Misconfiguration



Application security threats:

- Insufficient Logging and Monitoring
- Denial of Service (DoS) and Distributed Denial of Service (DDoS)
- Broken Authentication and Session Management
- Zero-Day Vulnerabilities
- Insecure Direct Object References
- Using Components with Known Vulnerabilities



6.8 SIEM Deployment

What is SIEM (Security Information and Event Management)?

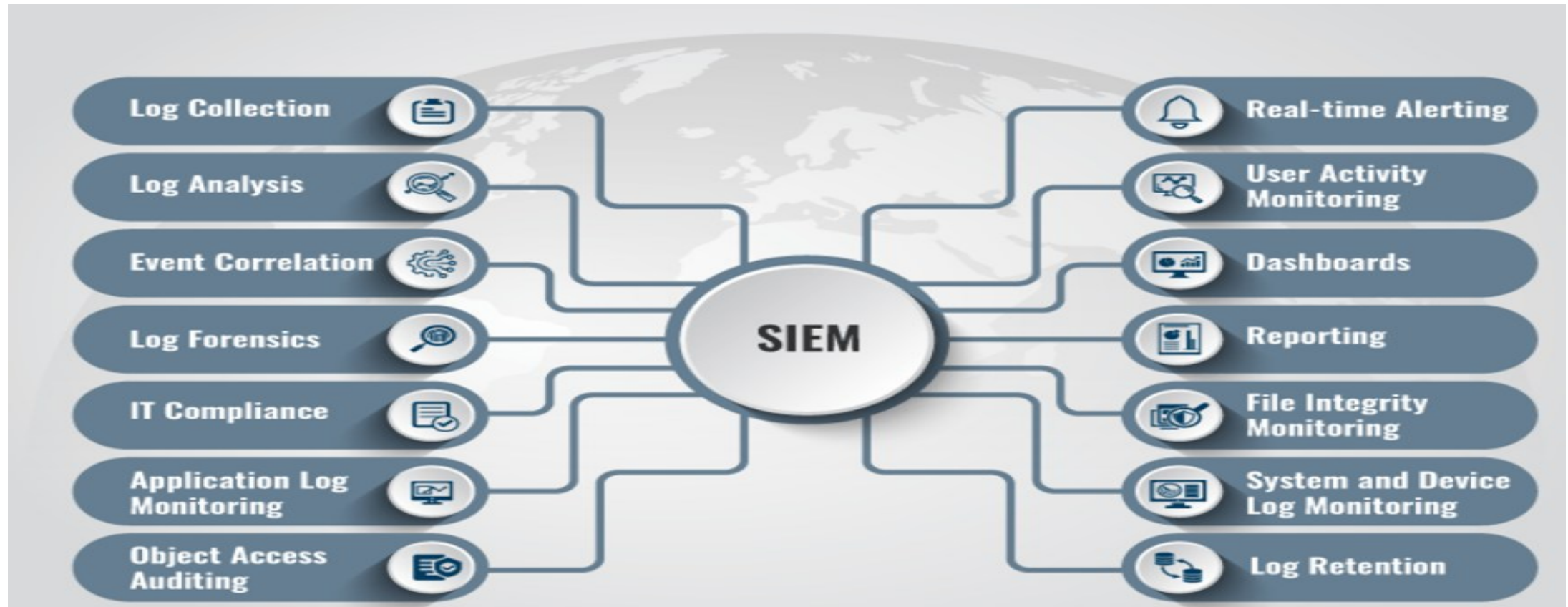
Security solution designed to help organizations detect, analyze, and respond to security threats and vulnerabilities in real-time.

It combines two key functions:

- Security Information Management (SIM)
- Security Event Management (SEM).



Components and Capabilities of SIEM



Co-funded by
the European Union



Why is SIEM important?

- Centralized security management
- Identifies potential security incidents that might otherwise go unnoticed
- Enables faster and more effective responses to security threats
- Allows reconstruction of attack timelines for better understanding of threats
- Real-time monitoring
- Correlation of events
- Automated response
- Operational efficiency



Steps in SIEM Deployment

- Planning and Scoping
- Installation
- Configuration
- Data Collection
- Testing and Validation
- Ongoing Monitoring and Maintenance
- Training and Support



SIEM tools and software

- Splunk
- IBM QRadar
- LogRhythm
- Exabeam
- NetWitness
- Datadog Cloud SIEM
- Log360
- SolarWinds Security
Event Manager



6.9 AI and SIEM

What is AI-Based SIEM?

- Traditional SIEM systems aggregate security data from various sources
- AI and Machine Learning (ML) are transforming SIEM by enhancing threat detection, improving incident response, and providing better insights



Components of AI-Driven SIEM:

- Data Aggregation
- Normalization
- Enrichment
- Machine Learning and Pattern Recognition
- Automated Incident Response
- Predictive Analytics



How AI and ML in SIEM are Revolutionizing Security Operations Centers?

- Enhanced Threat Detection
- Improved Incident Response Efficiency
- Reduced False Positives
- Improved Insight into Security Posture



6.10 SOC Cyber Threat Hunting

What is SOC?

Centralized unit responsible for monitoring, detecting, and responding to security incidents and threats within an organization's IT infrastructure

Key Functions of a SOC:

- Continuous Monitoring
- Incident Detection and Response
- Threat Intelligence Gathering
- Vulnerability Management





Co-funded by
the European Union

6.10 SOC Cyber Threat Hunting

What is Cyber Threat Hunting?

Proactive cybersecurity practice focused on identifying and mitigating threats that have already entered in an organization's network.



Threat Hunting Methodologies:

Operate under the assumption that adversaries are already present and investigate unusual behaviors that may signal malicious activity.

initiation of investigation typically falls into three main categories:

- Hypothesis-driven investigation
- Investigation based on known Indicators of Compromise or Indicators of Attack
- Advanced analytics and machine learning investigations



Threat Hunting Steps:

Step 1: Hypothesis (Trigger)

- Initiate threat hunting based on a specific event or hypothesis about a potential threat.
- Use known Tactics, Techniques, and Procedures (TTPs) and third-party data to outline clues.
- Formulate a hypothesis suggesting a named threat has compromised the network.

Step 2: Investigation

- In this phase, hunters actively search through data to uncover evidence supporting or refuting the hypothesis.



Threat Hunting Steps:

Step 3: Validation

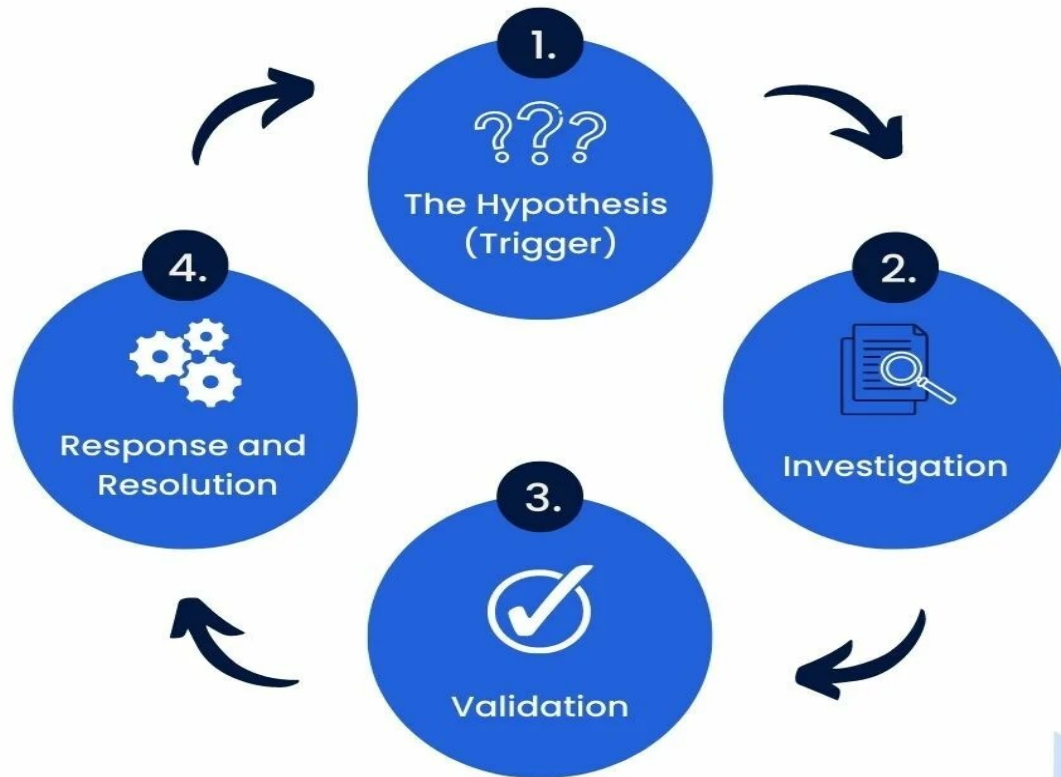
- This step involves confirming whether the findings from the investigation indicate a genuine threat or are false positives.

Step 4: Response/Resolution

- Once a threat is confirmed, this step focuses on mitigating its impact and restoring normal operations.



4 STEPS OF CYBER THREAT HUNTING



WWW.BITLYFT.COM/RESOURCES



Co-funded by
the European Union

6.10 SOC Cyber Threat Hunting

Types of threat hunting:

- Structured hunting
- Unstructured hunting
- Situational or entity-driven hunting



Different types of Threat Hunting

Structured threat hunting



Unstructured threat hunting



Situational threat hunting



Structured hunting

- Involves the systematic search for specific threats or IoCs based on predefined criteria or intelligence.
- Based on known attack techniques and frameworks (e.g., MITRE ATTACK).
- Follows a specific hypothesis about potential threats.
- Targets specific adversary behaviors or tactics.
- Efficient for detecting threats tied to known patterns.



Unstructured (Exploratory) hunting

- No specific hypothesis
- exploratory in nature.
- Analyzes a broad range of data for anomalies or unusual activities.
- Detects unknown or emerging threats.
- Flexible and useful for uncovering novel attack vectors.



Situational or Entity-Driven Hunting

- Triggered by specific alerts, events, or anomalies.
- Focuses on investigating specific assets, users, or events.
- Entity-driven hunting
- involves tracking users, devices, or applications for abnormal behavior.
- Effective for detecting insider threats, credential misuse, or active incidents.



6.10 SOC Cyber Threat Hunting

Threat hunting platforms:

Threat hunters use solutions and tools to find suspicious activities.

Three main categories:

- **Security monitoring tools**

Tools such as firewalls, antivirus, and endpoint security solutions collect security data and monitor the network.



6.10 SOC Cyber Threat Hunting

- **SIEM solutions**

Security information and event management (SIEM) solutions help manage the raw security data and provide real-time analysis of security threats.

- **Analytics tools**

Statistical and intelligence analysis software provides a visual report through interactive charts and graphs, making it easier to correlate entities and detect patterns.



Top 4 Effective Threat-Hunting Tools:




Managed Detection and Response (MDR)



SIEM



Security Analytics



Endpoint Detection and Response (EDR)



Learning Outcome

1. Students will learn the fundamentals of threat intelligence, including its types (strategic, tactical, operational) and its importance in cybersecurity.
2. Students will learn the key threat intelligence frameworks (e.g., Cyber Kill Chain, MITRE ATT&CK) and their applications.
3. Students will apply the knowledge of vulnerability assessment tools and port scanning to recognize potential security weaknesses in systems and networks.
4. Students will build the ability to conceptualize the deployment and operation of Security Information and Event Management (SIEM) systems, including the integration of Artificial Intelligence for enhanced threat detection and response.
5. Students will understand the role of Security Operations Centers (SOC) and the concept of cyber threat hunting in proactive cybersecurity.

Question no 01

What is threat intelligence?

- A) A type of cyber attack**
- B) A security framework**
- C) Information used to understand threats targeting an organization**
- D) A vulnerability assessment tool**



Question no 02

Which of the following is NOT a type of threat intelligence?

- A) Strategic
- B) Tactical
- C) Operational
- D) Functional



Question no 03

Which framework breaks down attacks into stages to identify and disrupt adversarial activities?

- A) MITRE ATT&CK**
- B) Cyber Kill Chain**
- C) Diamond Model**
- D) Unified Cyber Kill Chain**



Question no 04

How many phases or tactics does the Unified Kill Chain include?

- A) 7**
- B) 14**
- C) 18**
- D) 21**



Question no 05

What is the purpose of port scanning?

- A) To encrypt data**
- B) To check which ports on a network are open**
- C) To create backups**
- D) To install software**



Question no 06

Which of the following is NOT a common type of port scan?

- A) SYN Scan
- B) TCP Connect Scan
- C) UDP Scan
- D) HTTP Scan



Question no 07

What is the primary goal of cyber threat hunting?

- A) To patch vulnerabilities**
- B) To identify and mitigate threats already in the network**
- C) To develop new security software**
- D) To train new security personnel**



Question no 08

In which type of hunting is the investigation prompted by a specific alert or event?

- A. Structured hunting**
- B. Unstructured hunting**
- C. Situational hunting**
- D. Machine learning-based hunting**



Answers



1. C) Information used to understand threats targeting an organization
2. D) Functional
3. B) Cyber Kill Chain
4. C) 18
5. B) To check which ports on a network are open
6. D) HTTP Scan
7. B) To identify and mitigate threats already in the network
8. C) Situational hunting

Resources

- <https://www.bluevoyant.com/knowledge-center/threat-intelligence-complete-guide-to-process-and-technology>
- <https://www.ncsc.gov.uk/files/An-introduction-to-threat-intelligence.pdf>
- <https://socradar.io/main-analytical-frameworks-for-cyber-threat-intelligence/>
- <https://unifiedkillchain.com/>
- <https://attack.mitre.org/>
- <https://delinea.com/blog/what-is-the-mitre-attack-framework>
- <https://www.sangfor.com/glossary/cybersecurity/what-is-cyber-threat-hunting>
- <https://tryhackme.com/r/room/rpnessusredux>



Resources

- <https://play.google.com/store/apps/details?id=com.splunk.android.alerts&pli=1>
- <https://www.maltego.com/transform-hub/ibm-gradar>
- <https://www.bankinfosecurity.com/blogs/your-siem-ready-for-ai-era-essential-insights-preparations-p-3706>
- <https://www.exabeam.com/explainers/information-security/threat-hunting-tips-and-tools/>
- <https://www.bitlyft.com/resources/introduction-cyber-threat-hunting>
- <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/threat-hunting/>
- <https://www.fortinet.com/resources/cyberglossary/threat-hunting>



Reference Book

- **Intelligence-Driven Incident Response: Outwitting the Adversary 2nd Edition, Kindle Edition**



Co-funded by
the European Union