Proof of Concept (POC): Threat Intelligence

Name: Harshali Kasurde
Intern ID: 299

1. Introduction to Threat Intelligence

Threat Intelligence is the process of gathering, analysing, and utilizing information about current and potential cyber threats to prevent, detect, and respond to cyberattacks effectively. It provides context about attackers, their tools, techniques, tactics, procedures (TTPs), and motivations. This enables security teams to make informed decisions to protect their systems, networks, and data.

- Tactic: *Why* the attacker is taking an action (objective)
- Technique: *How* the attacker is accomplishing it (method)
- Sub-technique: More granular "how"
- Procedure: Real example of a technique in operation

2. Key Elements of Threat Intelligence

- Indicators of Compromise (IOCs): Technical artifacts observed in an attack (e.g., IPs, file hashes, URLs)
- Tactics, Techniques, and Procedures (TTPs): Patterns of behavior used by attackers (basis for MITRE ATT&CK)
- Threat Actors: Information about the individuals or groups behind attacks
- Motivations: Reasons behind targeting specific organizations (e.g., financial gain, espionage, political disruption)

3. Importance of Threat Intelligence

3.1 Proactive Defense

- Identify threats before they occur
- Block malicious IOCs (IPs, domains, files) in real time
- Recognize attack patterns and prepare countermeasures in advance

3.2 Better Threat Detection

- Provides contextual data to detect suspicious activity quickly and accurately
- Reduces false positives
- Enables threat hunting via clear TTPs

3.3 Faster Incident Response

- Identifies attack type and attacker's goal
- Provides response playbooks and case studies
- Speeds up decision-making to contain and eradicate threats

3.4 Improved Security Controls

- Updates security controls with new IOCs
- Refines policies (access, segmentation, data protection)
- Tailors security awareness training

3.5 Targeted and Informed Defenses

- Focuses resources on relevant threats
- Risk prioritization

3.6 Understanding Adversaries

No	Matrix Name	Domain/Environment	Key Focus
1	Enterprise	IT (Windows, macOS, Linux, Cloud)	Attacks on traditional/cloud IT infrastructure (14 tactics)
2	Mobile	Android, iOS	Threats to smartphones/tablets (14 tactics)
3	ICS	Industrial (SCADA, PLC, HMI)	OT threats (12 tactics)
4	MITRE ATLAS	AI/ML Systems	ML-specific attacks
5	Automotive Threat	Connected Vehicles	Car hacking (CAN, ECU, telematics)
6	Cloud Matrix	AWS, Azure, GCP, SaaS	IAM abuse/misconfigurations
7	Container/Kubernetes	Docker, Kubernetes	Container escape, image poisoning

No	Matrix Name	Domain/Environment	Key Focus
8	DevOps Threat	CI/CD, GitHub, Azure DevOps	Attack paths in pipelines/secrets
9	Cloud Storage	S3, Azure Blob, GCP Buckets	Public exposure, data theft
10	PRE-ATT&CK (Retired)	Pre-Compromise	OSINT, profiling (now merged to Enterprise)

- Identifies who attackers are and their methods/motives
- Builds stronger, more resilient security strategies

3.7 Collaboration and Sharing

- Enables intelligence sharing
- Promotes collective defences

5. Tactics and Techniques Explained

5.1 What is a Tactic?

- Tactics are the attacker's high-level strategic objectives, representing each stage of the attack lifecycle (e.g., gaining access, executing code, stealing credentials, exfiltrating data).

5.2 Main ATT&CK Tactic Categories

(A) Enterprise Tactics

ID	Name	Description
TA0043	Reconnaissance	Gathering information on target
TA0042	Resource Development	Establishing resources for later use
TA0001	Initial Access	First entry into the environment
TA0002	Execution	Running malicious code

ID	Name	Description
TA0003	Persistence	Maintaining access after reboot, logout, etc.
TA0004	Privilege Escalation	Gaining higher permissions
TA0005	defence Evasion	Avoiding detection or blocking
TA0006	Credential Access	Stealing account credentials
TA0007	Discovery	Learning about environment
TA0008	Lateral Movement	Moving to other network systems
TA0009	Collection	Gathering target data
TA0011	Command and Control	Communication with compromised systems
TA0010	Exfiltration	Stealing data out of the network
TA0040	Impact	Disrupt/Destroy/Alter systems or data

(B) Mobile Tactics

Similar to enterprise with two extra tactics for network/service-based attacks on mobile devices:

- Network Effects
- Remote Service Effects

(C) ICS Tactics

Similar layout but unique for industrial systems:

- Inhibit Response Function
- Impair Process Control

5.3 Techniques, Sub-Techniques, Procedures

- Technique: The how of the attack (e.g., brute force credential guessing).

- Sub-Technique: More detailed variant (e.g., password spraying).
- Procedure: Actual method an attacker uses (e.g., “APT28 used Hydra for brute-forcing RDP”).

6. Proof of Concept Examples: Core Techniques

Below are concise, lab-suitable steps for each ATT&CK tactic, demonstrating applications of threat intelligence.

6.1 Reconnaissance

Identifying targets using open-source methods

Technique: Scanning IP Blocks (T1595.001)

1. Define IP range (e.g., 192.168.1.0/24)
2. Run:

text

nmap -sn 192.168.1.0/24

nmap -sS -p1-65535 192.168.1.0/24

3. Record live hosts and open ports.

Technique: DNS Enumeration (T1590.002)

- dig target.com ANY
- dnsrecon -d target.com -t brt

Technique: Email Discovery (T1589.002)

- theHarvester -d target.com -b google
- Or: Google for site:target.com "@target.com"

6.2 Resource Development

Preparing infrastructure for attacks

Technique: Registering Domains (T1583.001)

- Use a registrar to buy e.g., login-secure.com
- Add DNS A record to attacker server

Technique: Malware Development (T1587.001)

- Create reverse shell in Python
- Convert to .exe using PyInstaller

6.3 Initial Access

Gaining entry into the environment

Technique: Spearphishing Attachment (T1566.001)

- Create macro-enabled Word document with msfvenom payload
- Deliver via phishing email in a test lab

Technique: Exploit Public Web App (T1190)

- Use exploit for known CVE, e.g.,
  python exploit.py --rhost victim --payload revshell

Technique: Valid Accounts (T1078)

- ssh user@target-ip using stolen credentials

6.4 Execution

Running malicious payloads

Technique: Command & Scripting Interpreter (T1059)

- powershell.exe -ExecutionPolicy Bypass -File payload.ps1

Technique: User Execution of Malicious File (T1204.002)

- User opens a document, triggers PowerShell

6.5 Persistence

Maintaining long-term access

Technique: Registry Run Keys (T1547.001)

- reg add HKCU\...\Run /v updater /t REG_SZ /d "C:\\Tools\\payload.exe"

Technique: Scheduled Task (T1053.005)

- schtasks /create /tn updater ...

Technique: Create Local Account (T1136.001)

- net user stealthadmin Pass123! /add

6.6 Privilege Escalation

Gaining higher permissions

Technique: Exploiting Vulnerability (T1068)

- Use public exploit to escalate privileges

6.7 Defense Evasion

Avoiding detection

Technique: Disable Security Tools (T1562.001)

- sc stop WinDefend

Technique: Obfuscate Scripts (T1027)

- Encode PowerShell script as Base64

6.8 Credential Access

Stealing passwords or tokens

Technique: Dumping LSASS Memory (T1003.001)

- Use Mimikatz (sekurlsa::logonpasswords)

Technique: Keylogging (T1056.001)

- Linux: sudo logkeys --start --output /tmp/keys.log

6.9 Discovery

Exploring target's environment

Technique: System Info Discovery (T1082)

- Windows: systeminfo
- Linux: uname -a

6.10 Lateral Movement

Moving across the network

Technique: SMB Admin Shares (T1021.002)

- net use \\target\C$ /user:admin password

6.11 Collection

Gathering data of interest

Technique: Local Data (T1005)

- find / -name "*.docx"

Technique: Email Collection (T1114.001)

- Extract PST/OST files

6.12 Command & Control (C2)

Remotely controlling compromised systems

Technique: Web Protocols (T1071.001)

- Use HTTP/S for beaconing

Technique: Encrypted Channel (T1573.001)

- Use HTTPS listeners in C2 frameworks

6.13 Exfiltration

Exfiltrating data out of network

Technique: Exfiltration over HTTPS (T1048.002)

- curl or rclone copy data to cloud storage

6.14 Impact

Disrupting operations or destroying data

Technique: Data Destruction (T1485)

- Remove-Item -Path "...Documents*" -Recurse -Force

Technique: Data Encryption (T1486)

- Use (simulated) ransomware encryption for impact