MITRE ATT&CK, THREAT HUNTING Project Overview

Purpose

This project serves as a comprehensive guide for threat hunting, detection engineering, and adversary emulation using industry-standard frameworks and tools.

Objectives

- Understand and implement MITRE ATT&CK framework
- Develop threat hunting methodologies
- Build effective detection rules
- Analyze adversary tactics, techniques, and procedures (TTPs)
- Map security controls to compliance frameworks

Target Audience

- SOC Analysts
- Threat Hunters
- Detection Engineers
- Security Researchers
- Incident Responders

Threat Hunting Fundamentals

Definition

Threat hunting is the proactive and iterative search through networks and datasets to detect and isolate advanced threats that evade existing security solutions.

Types of Threat Hunting

1. Hypothesis-Driven Hunting

Based on threat intelligence or understanding of attacker behavior.

2. Intelligence-Driven Hunting

Driven by external threat intelligence reports.

3. Situational Awareness Hunting

Triggered by specific events or alerts.

Threat Hunting Process

```
┌─────────────────┐
│ 1. Hypothesis │
│  Development  │
└────────┬────────┘
    │
    ▼
┌─────────────────┐
│  2. Data     │
│  Collection   │
└────────┬────────┘
    │
    ▼
┌─────────────────┐
│ 3. Analysis & │
│  Investigation │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ 4. Response &   │
│  Resolution     │
└────────┬────────┘
         │
         ▼
┌─────────────────┐
│ 5. Documentation│
│  & Improvement  │
└─────────────────┘
```

Threat Hunting Events

Key Events to Hunt:

1. **Authentication Events**
   - Multiple failed logins
   - Login from unusual locations
   - Off-hours authentication
2. **Process Execution Events**
   - Suspicious process creation
   - PowerShell execution
   - Command-line anomalies

3. **Network Events**
    - Unusual outbound connections
    - DNS queries to suspicious domains
    - Large data transfers
4. **File System Events**
    - File creation in suspicious locations
    - Modification of system files
    - Executable downloads

Advantages

- ✅ Proactive threat detection
- ✅ Reduces dwell time
- ✅ Discovers unknown threats
- ✅ Improves security posture
- ✅ Enhances analyst skills

Disadvantages

- ❌ Resource intensive
- ❌ Requires skilled personnel
- ❌ Can generate false positives
- ❌ Time-consuming process

- Threat hunting workflow diagram
- Sample hypothesis document
- Investigation timeline

Log Analysis & Event Codes

Definition

Log analysis is the process of examining log files to identify security incidents, troubleshoot issues, and ensure compliance.

Critical Windows Event IDs

Authentication & Account Events

Event ID	Description	Importance
4624	Successful logon	Track user access
4625	Failed logon	Detect brute force
4634	Logoff	Session tracking
4648	Logon with explicit credentials	Lateral movement
4672	Special privileges assigned	Privilege escalation
4720	User account created	Persistence
4722	User account enabled	Suspicious reactivation
4724	Password reset attempt	Account takeover
4728	Member added to global group	Privilege escalation
4732	Member added to local group	Local admin changes

4756	Member added to universal group	Domain-level changes

Process & Service Events

Event ID	Description	Importance
4688	Process creation	Malware execution
4689	Process termination	Investigation timeline
7045	Service installed	Persistence mechanism
7040	Service state changed	Service manipulation

Object Access Events

Event ID	Description	Importance
4663	Object access attempt	File access monitoring
4656	Handle to object requested	Sensitive file access
5140	Network share accessed	Lateral movement
5145	Network share checked	SMB enumeration

Policy & System Events

Event ID	Description	Importance
4719	System audit policy changed	Defense evasion
1102	Security log cleared	Anti-forensics
4657	Registry value modified	Persistence
4698	Scheduled task created	Persistence

Threat Intelligence

Definition

Threat intelligence is evidence-based knowledge about existing or emerging threats that can be used to inform decisions about responding to those threats.

Types of Threat Intelligence

1. Strategic Threat Intelligence

- High-level information for executives
- Long-term trends and risks
- Business impact analysis

2. Tactical Threat Intelligence

- TTPs of threat actors
- Campaign information
- Attack vectors

3. Operational Threat Intelligence

- Specific information about attacks
- Nature, motive, timing, and method
- Real-time threat data

4. Technical Threat Intelligence

- Indicators of Compromise (IOCs)
- IP addresses, domains, hashes
- Specific technical details

Threat Intelligence Sources

Open Source (OSINT):

- AlienVault OTX (https://otx.alienvault.com/)

- Abuse.ch (https://abuse.ch/)

- VirusTotal (https://www.virustotal.com/)

- MISP (Malware Information Sharing Platform)

- Threat Crowd (https://threatcrowd.org/)

- Shodan (https://www.shodan.io/)

- GreyNoise (https://www.greynoise.io/)

- URLhaus (https://urlhaus.abuse.ch/)

- Feodo Tracker (https://feodotracker.abuse.ch/)

Commercial Sources:

- Recorded Future

- Anomali ThreatStream

- CrowdStrike Falcon Intelligence

- Mandiant Threat Intelligence

- IBM X-Force Exchange

Government Sources:

- US-CERT

- CISA Alerts

- NCSC (National Cyber Security Centre)

- ENISA Threat Landscape

Threat Intelligence Lifecycle

```
┌─────────────┐
│ Planning &  │
│ Direction   │
└──────┬──────┘
   │
   ▼
┌─────────────┐
│ Collection  │
└──────┬──────┘
   │
   ▼
┌─────────────┐
│ Processing  │
└──────┬──────┘
   │
   ▼
┌─────────────┐
│  Analysis   │
└──────┬──────┘
   │
   ▼
┌─────────────┐
│Dissemination │
└──────┬──────┘
   │
   ▼
┌──────────┐
│ Feedback │
└──────────┘
```

Indicators of Compromise (IOCs)

Common IOC Types:

1. **File-based IOCs**

- MD5/SHA1/SHA256 hashes
- File names
- File sizes
- File paths

2. **Network-based IOCs**

- IP addresses
- Domain names
- URLs
- Email addresses
- SSL certificate hashes

3. **Registry Keys**

- Persistence mechanisms
- Configuration data
- Malware artifacts

4. **Behavioral IOCs**

- Unusual network traffic patterns
- Abnormal process execution
- Suspicious user behavior

Adversary TTP Analysis

Definition

TTP Analysis involves studying the Tactics, Techniques, and Procedures used by threat actors to understand their behavior, predict future actions, and develop effective defenses.

Components of TTP Analysis

Tactics - The "Why"

Strategic goals of the adversary.

Techniques - The "How"

Methods used to achieve tactical goals.

Procedures - The "What"

Specific implementations in real attacks.

TTP Analysis Process

Step-by-Step Methodology:

1. **Collect Incident Data**

Sources:

- Incident response reports
- Threat intelligence feeds
- SIEM alerts
- EDR telemetry

- Network packet captures
- Memory forensics

2. **Identify Observable Artifacts**

- File hashes (MD5, SHA1, SHA256)
- IP addresses and domains
- Registry keys
- File paths
- Process names
- Network protocols
- User accounts

3. **Map to MITRE ATT&CK Example Mapping:**

Observed Behavior	**MITRE Technique**	**Tactic**
Spearphishing email with malicious attachment	T1566.001	Initial Access
PowerShell downloads payload	T1059.001	Execution
Registry Run key modification	T1547.001	Persistence
Mimikatz execution	T1003.001	Credential Access
RDP connection to other host	T1021.001	Lateral Movement

4. **Analyze TTP Patterns**

Questions to Answer:

- What is the attacker's preferred initial access method?

- Which persistence mechanisms are used?

- What tools are in their arsenal?

- How do they move laterally?

- What is their end goal (ransomware, espionage, destruction)?

APT Groups Analysis

Definition

Advanced Persistent Threat (APT) groups are sophisticated, organized threat actors typically backed by nation-states or well-funded organizations that conduct long-term targeted cyber espionage or sabotage campaigns.

Major APT Groups

APT28 (Fancy Bear)

Profile:

- **Origin:** Russia (GRU)
- **Active Since:** 2007
- **Motivation:** Espionage, influence operations
- **Targets:** Government, military, security organizations, media

Common TTPs:

Tactic	**Technique ID**	**Technique Name**	**Description**
Initial Access	T1566.001	Spearphishing Attachment	Malicious Office documents
Initial Access	T1189	Drive-by Compromise	Watering hole attacks
Execution	T1059.001	PowerShell	PowerShell-based malware
Persistence	T1053.005	Scheduled Task	Persistence via scheduled tasks
Defense Evasion	T1070.004	File Deletion	Anti-forensics
Credential Access	T1003.001	LSASS Memory	Mimikatz and variants
Lateral Movement	T1021.001	RDP	Remote Desktop Protocol
Exfiltration	T1041	C2 Channel	Data exfiltration over C2

Known Tools:

- X-Agent
- X-Tunnel
- Sofacy
- LoJax (UEFI rootkit)

APT Group Comparison Matrix

APT Group	Origin	Primary Motivation	Sophistication	Preferred Initial Access	Notable Campaign
APT28	Russia (GRU)	Espionage	High	Spearphishing	DNC hack (2016)
APT29	Russia (SVR)	Intelligence	Very High	Supply Chain	SolarWinds (2020)
APT41	China	Dual (Espionage/Financial)	High	Web Exploits	Healthcare breaches
Lazarus	North Korea	Financial/Sabotage	High	Spearphishing	WannaCry (2017)
APT32	Vietnam	Espionage	Medium-High	Spearphishing	Manufacturing sector
APT38	North Korea	Financial	High	Compromise	SWIFT attacks

APT Hunting Methodology

Step-by-Step APT Hunt:

1. **Select Target APT Group**

Research: APT29 (Cozy Bear)

Focus: Recent campaigns and TTPs

2. **Gather TTPs from MITRE ATT&CK**

Visit: https://attack.mitre.org/groups/G0016/

Extract: All associated techniques

3. **Identify Data Sources**

- Windows Event Logs
- Sysmon
- Network logs (DNS, Firewall, Proxy)
- EDR telemetry

4. **Build Hunt Hypothesis**

Hypothesis: "APT29 has established persistence via WMI event subscriptions and is using PowerShell for execution."

5. **Create Hunt Queries**

spl

```
 # Hunt for WMI Persistence
  index=windows EventCode=5861
  | table _time, Computer, User, Operation, Consumer, Filter

  # Hunt for Suspicious PowerShell
  index=windows EventCode=4104
  | rex field=ScriptBlockText "(?<ioc>Invoke-Expression|IEX|DownloadString)"
  | where isnotnull(ioc)
  | table _time, Computer, User, ScriptBlockText
```

6. **Analyze Results**

- Correlate findings across multiple data sources
- Build timeline of activities
- Identify patient zero
- Map to kill chain

7. **Document Findings**

markdown

```
 ## APT Hunt Report: APT29 Indicators


  **Date:** 2024-01-15
  **Hunter:** [Your Name]
  **Hypothesis:** APT29 WMI persistence


  ### Findings:
  - Discovered 3 WMI event subscriptions on servers
  - PowerShell execution with encoded commands
  - Network connections to known APT29 infrastructure


  ### IOCs:
  - IP: 192.0.2.100 (C2 server)
  - Hash: a1b2c3d4e5f6... (PowerShell script)
  - WMI Consumer: "SystemPerformanceMonitor"
```

Recommendations:

- Isolate affected systems

- Reset credentials

- Deploy detection rules

- MITRE ATT&CK APT29 group page
- APT TTP comparison matrix
- Hunt query results
- APT timeline visualization

Tools & Platforms

SOC Radar

What is SOC Radar?

SOC Radar is a threat intelligence and attack surface management platform that provides continuous monitoring, threat detection, and vulnerability assessment.

How to Use SOC Radar

Step-by-Step Process:

1. **Account Setup**

1. Visit: https://socradar.io

2. Create account / Sign in

3. Complete organization profile

4. Configure notification preferences

2. **Dashboard Overview**
    - **Threat Intelligence Feed:** Real-time threats
    - **Attack Surface:** Exposed assets
    - **Vulnerabilities:** CVE tracking

- **Dark Web Monitoring:** Leaked credentials
- **Brand Protection:** Phishing domains

3. **Configure Monitoring**

Settings → Add Assets:

- Domain names
- IP ranges
- Brand keywords
- Email domains
- Social media accounts

4. **Set Up Alerts**

Alerts → Create New Alert:

- Alert type (vulnerability, threat intel, dark web)
- Severity threshold
- Notification channels (email, Slack, Teams)

5. **Threat Intelligence Integration**

Integrations → SIEM:

- Get API key
- Configure endpoints
- Map fields
- Test connection

6. **Incident Investigation**

Threats → Select Incident:

- Review threat details
- Check MITRE ATT&CK mapping

- Download IOCs

- Export report

Key Features:

- ✅ Real-time threat intelligence
- ✅ Attack surface monitoring
- ✅ Dark web monitoring
- ✅ Vulnerability management
- ✅ MITRE ATT&CK mapping
- ✅ API integration

- SOC Radar dashboard
- Threat intelligence feed
- Alert configuration page
- IOC export interface

MITRE ATT&CK Framework

Definition

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Components

1. Tactics (The "Why")

The adversary's tactical goal - the reason for performing an action.

14 Enterprise Tactics:

1. Reconnaissance

2. Resource Development
3. Initial Access
4. Execution
5. Persistence
6. Privilege Escalation
7. Defense Evasion
8. Credential Access
9. Discovery
10. Lateral Movement
11. Collection
12. Command and Control
13. Exfiltration
14. Impact

2. Techniques (The "How")

How an adversary achieves a tactical goal.

3. Sub-Techniques

More specific descriptions of adversarial behavior.

4. Procedures

Specific implementations observed in the wild.

Importance

Advantages:

- ✅ Common language for cybersecurity professionals
- ✅ Threat-informed defense strategy
- ✅ Gap analysis capabilities

- ✅ Prioritization of security investments
- ✅ APT behavior modeling
- ✅ Detection coverage mapping

Disadvantages:

- ❌ Can be overwhelming for beginners
- ❌ Requires continuous updates
- ❌ May not cover all emerging threats immediately
- ❌ Implementation complexity

How to Use MITRE ATT&CK

Step-by-Step Process:

1. **Access the Framework**

URL: https://attack.mitre.org/

2. **Navigate the Matrix**
   - Select your domain (Enterprise, Mobile, ICS)
   - Browse tactics (columns)
   - Explore techniques (cells)

3. **Search for Specific Techniques**

Example: T1566 - Phishing

Sub-technique: T1566.001 - Spearphishing Attachment

- **Review Technique Details**
  - Description
  - Detection methods
  - Mitigations
  - Real-world examples

- MITRE ATT&CK homepage
- Enterprise Matrix view
- Specific technique page (e.g., T1059 - Command and Scripting Interpreter)
- Group profile page

MITRE ATT&CK Navigator

What is ATT&CK Navigator?

A web-based tool for annotating and exploring ATT&CK matrices, visualizing defensive coverage, planning red team operations, and comparing threat intelligence.

How to Use ATT&CK Navigator

Step-by-Step Process:

1. **Access the Navigator**

URL: https://mitre-attack.github.io/attack-navigator/

Or run locally:

```
git clone https://github.com/mitre-attack/attack-navigator.git

cd attack-navigator

npm install

npm start
```

2. **Create a New Layer**

1. Click "Create New Layer"

2. Select domain (Enterprise, Mobile, ICS)

3. Choose matrix version

3. **Annotate Techniques**

For each technique:

- Click on technique cell

- Set color (coverage level)

- Add score (1-100)

- Add comment (detection rule ID, notes)

- Set state (enabled/disabled)

4. **Color Coding Strategy**

Red (#ff6666): No coverage

Orange (#ffb366): Low coverage

Yellow (#ffff66): Medium coverage

Green (#66ff66): High coverage

Blue (#6666ff): Full coverage with validation

6. **Compare Layers**

1. Create multiple layers (e.g., APT28 TTPs, Your Defenses)
2. Click "+" to create selection
3. Select layers to compare
4. View differences highlighted

7. **Export Layer**

File → Export:

- Excel (.xlsx)
- JSON (.json)
- SVG image (.svg)

8. **Use Cases A. Detection Coverage Analysis:**

1. Create layer for current detections
2. Score each technique (0-100) based on coverage
3. Identify gaps (red/orange cells)
4. Prioritize detection development

B. APT Campaign Mapping:

1. Create layer for specific APT group
2. Highlight techniques used by APT
3. Compare with detection coverage

4. Identify blind spots

C. Red Team Planning:

1. Create attack scenario layer
2. Select techniques for operation
3. Identify heavily monitored areas
4. Plan evasion strategies

Navigator Features:

- Layer management
- Technique annotation
- Scoring system
- Comment/metadata
- Multi-layer comparison
- Export capabilities
- Search and filter
- Tactic filtering

- Navigator homepage
- Technique selection and annotation
- Layer comparison view
- Exported coverage heatmap

Security Frameworks Mapping

NIST Cybersecurity Framework (CSF)

5 Core Functions:

1. **Identify (ID)**
2. **Protect (PR)**
3. **Detect (DE)**
4. **Respond (RS)**
5. **Recover (RC)**

Mapping Threat Hunting to NIST CSF:

NIST Function	Category	Threat Hunting Activity	MITRE ATT&CK Alignment
Identify	Asset Management (ID.AM)	Inventory all systems and data sources	All tactics
Identify	Risk Assessment (ID.RA)	Identify critical assets and threat scenarios	Reconnaissance, Resource Development
Protect	Access Control (PR.AC)	Monitor authentication events	Credential Access, Initial Access
Protect	Data Security (PR.DS)	Monitor data access and transfers	Collection, Exfiltration
Detect	Anomalies and Events (DE.AE)	Hunt for suspicious behaviors	All techniques

Detect	Security Monitoring (DE.CM)	Continuous monitoring of logs and network	All techniques
Respond	Response Planning (RS.RP)	Incident response procedures	All tactics
Respond	Analysis (RS.AN)	Investigate and analyze incidents	All techniques
Recover	Recovery Planning (RC.RP)	Document lessons learned	Impact

ISO/IEC 27001:2022 Annex A Controls

Mapping to Threat Hunting Topics:

Annex A Control	**Control Name**	**Threat Hunting Relevance**	**Implementation**
A.5.1	Policies for information security	Define threat hunting policies	Document hunting procedures
A.5.7	Threat intelligence	Integrate TI into hunting	Use MISP, OTX, commercial feeds
A.8.8	Management of technical vulnerabilities	Hunt for exploitation attempts	Monitor CVE exploitation
A.8.10	Information deletion	Monitor for data destruction	Detect anti-forensics (T1070)
A.8.11	Data masking	Protect sensitive data in logs	Implement log sanitization
A.8.12	Data leakage prevention	Hunt for exfiltration	Monitor T1041, T1048

A.8.15	Logging	Ensure comprehensive logging	Enable Sysmon, audit policies
A.8.16	Monitoring activities	Continuous monitoring	SIEM, EDR deployment
A.8.19	Installation of software	Monitor unauthorized software	Detect T1204, T1072
A.8.23	Web filtering	Monitor web-based threats	Analyze proxy logs
A.8.25	Secure development lifecycle	Security in SDLC	Code review, SAST/DAST

Control Framework Mapping Matrix

Control Framework	**Control ID**	**Control Name**	**Threat Hunting Activity**	**Detection Rule**	**MITRE Technique**
NIST CSF	DE.AE-2	Detected events are analyzed	Analyze authentication anomalies	Multiple failed logins detection	T1110
ISO 27001	A.8.16	Monitoring activities	Monitor process execution	Suspicious PowerShell detection	T1059.001

CIS Controls	8.5	Collect logs	Centralize log collection	SIEM ingestion rules	All
NIST CSF	DE.CM-1	Network monitored	Monitor network traffic	Detect C2 beaconing	