

How to Use MITRE ATT&CK in SOC

Using MITRE ATT&CK in a Security Operations Center (SOC) can greatly enhance threat detection and response capabilities. Here are the steps to effectively utilize MITRE ATT&CK framework in a SOC:

▼ Familiarize Yourself with MITRE ATT&CK

- Understand the purpose and structure of the MITRE ATT&CK framework.
- Explore the ATT&CK website (https://attack.mitre.org/) and review the ATT&CK matrix, techniques, tactics, and sub-techniques.

▼ Map ATT&CK to Your Environment

- Identify the relevant MITRE ATT&CK techniques and tactics that align with your organization's infrastructure, applications, and data.
- Map the MITRE ATT&CK techniques to your existing security controls, such as firewalls, intrusion detection systems, and endpoint protection solutions.

▼ Create Detection Rules

- Develop detection rules and use cases based on specific MITRE ATT&CK techniques and tactics.
- Leverage your security information and event management (SIEM) system or threat intelligence platforms to create rules that trigger alerts when suspicious activities related to specific ATT&CK techniques are detected.

▼ Implement Threat Hunting

• Utilize MITRE ATT&CK as a guide for proactive threat hunting exercises.

 Search for indicators of compromise (IOCs) associated with known ATT&CK techniques and use them to identify potential threats within your environment.

▼ Enhance Incident Response

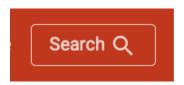
- Incorporate MITRE ATT&CK into your incident response procedures
- Develop playbooks and response plans that align with specific ATT&CK techniques and tactics to effectively handle and mitigate threats.

▼ Collaborate with Threat Intelligence

- Leverage external threat intelligence sources that align with MITRE ATT&CK.
- Stay updated on the latest threat intelligence reports that reference ATT&CK techniques and tactics.



You can search things on MITRE ATT&CK website search box like tools or attack TTP



▼ How to use MITRE ATT&CK in action

- ▼ Step 1 : Find what you looking for
 - Find Tactics, technique, Sub-technique or ID
 - Example : Scheduled Task/Job: Scheduled Task
 - **ID**: T1053.005
 - Sub-technique of: <u>T1053</u>
 - Tactics: Execution, Persistence, Privilege Escalation

Scheduled Task/Job: Scheduled Task, Sub-technique T1053.005 - Enterprise | MITRE ATT&CK®

M https://attack.mitre.org/techniques/T1053/005/

▼ Step 2 : Learn about it

Understand ATT&CK

- Familiarize yourself with the overall structure of ATT&CK
- Find the behavior
 - Find parameters and tools attacker should use to implement the ATT&CK
- Research the behavior / tools
 - Search about the **technique** or **Sub-technique** on the other resources
- Read Procedure Examples section
 - Learn how Groups or tools use the technique or Sub-technique
- ▼ Step 3 : Defeat it 🗡
 - Mitigations section
 - Find the Mitigation
 - · Detection section
 - Find the **Detection**
- ▼ Step 4 : Convert TTP to SIEM rule / use case
 - Find Detection rule at MITRE CAR project
 - Example : <u>Scheduled Task Creation or Modification Containing Suspicious</u>
 <u>Scripts</u>

▼ Data Sources

You can identify **technique** or **Sub-technique** based on data source that you have like <u>Windows Registry</u> or <u>Network Traffic</u>

Data Sources | MITRE ATT&CK®

M https://attack.mitre.org/versions/v13/datasources/

Examples

- **▼** Process and process command line monitoring
 - Often collected by Sysmon, Windows Event Logs

Command, Data Source DS0017 | MITRE ATT&CK®

M https://attack.mitre.org/versions/v13/datasources/DS0017/

▼ Registry monitoring

· A Windows OS hierarchical database that stores much of the information and settings for software programs

Windows Registry, Data Source DS0024 | MITRE ATT&CK®

M https://attack.mitre.org/versions/v13/datasources/DS0024/

▼ Network Traffic

 such as capturing socket information with a source/destination IP and port(s) (ex: Windows EID 5156, Sysmon EID 3, or Zeek conn.log)

Network Traffic, Data Source DS0029 | MITRE ATT&CK®

M https://attack.mitre.org/versions/v13/datasources/DS0029/

▼ ATT&CK Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

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

Credit by Sina Mohebi & blog.sinamohebi.com