Mitre

TryHackMe: Mitre

Opgaveinformation

Opgavens formål er at give en forståelse for Mitre.

Opgave + løsning

Opgave 2 - ATT&CK Framework

What Tactic does the Hide Artifacts technique belong to in the ATT&CK Matrix?

- https://attack.mitre.org/techniques/T1628/
- Defense Evasion

Which ID is associated with the Create Account technique?

- https://attack.mitre.org/detectionstrategies/DET0583/
- T1136

Opgave 3 - ATT&CK in Operation

Rolle	Mål / funktion	Eksempel på hvordan de bruger ATT&CK
Cyber Threat Intelligence (CTI) Teams	Indsamle og analysere trusselinformation for at forbedre organisationens sikkerhedsberedskab	Mapper observeret trusselsaktør-adfærd til ATT&CK TTP'er for at skabe handlingsorienterede profiler på tværs af industrien
SOC Analysts	Undersøge og triagere sikkerhedsalarmer	Knyt aktivitet til taktikker og teknikker for at give detaljeret kontekst til alarmer og prioritere hændelser

Rolle	Mål / funktion	Eksempel på hvordan de bruger ATT&CK
Detection Engineers	Designe og forbedre detektionssystemer	Mapper SIEM/EDR-regler og andre overvågningsregler til ATT&CK for at sikre bedre detektion
Incident Responders	Reagere på og undersøge sikkerhedshændelser	Mapper hændelses-tidslinjer til MITRE taktikker og teknikker for bedre visualisering af angrebet
Red & Purple Teams	Emulere modstanderadfærd for at teste og forbedre forsvar	Bygger emuleringsplaner og øvelser baseret på teknikker og kendte gruppers operationer

In which country is Mustang Panda based?

- https://attack.mitre.org/groups/G0129/
- China

Which ATT&CK technique ID maps to Mustang Panda's Reconnaissance tactics?

- T1598

Which software is Mustang Panda known to use for Access Token Manipulation?

- https://attack.mitre.org/groups/G0129/
- Søg efter "Access Token Manipulation"
- Svar: Cobalt Strike

Opgave 4 - ATT&CK for Threat Intelligence

Which APT group has targeted the aviation sector and has been active since at least 2013?

- https://attack.mitre.org/groups/
- Søg efter "2013"
- Svar: APT33

Which ATT&CK sub-technique used by this group is a key area of concern for companies using Office 365?

- https://attack.mitre.org/groups/G0064/
- Søg efter "Office"

- Svar: Cloud Accounts

According to ATT&CK, what tool is linked to the APT group and the sub-technique you identified?

- https://attack.mitre.org/groups/G0064/
- Søg efter "Office" og kig efter værktøjet.
- Svar: Ruler

Which mitigation strategy advises removing inactive or unused accounts to reduce exposure to this sub-technique?

- https://attack.mitre.org/techniques/T1078/004/
- Gå ned til Mitigations og undersøg
- Svar: User Account Management

What Detection Strategy ID would you implement to detect abused or compromised cloud accounts?

- https://attack.mitre.org/techniques/T1078/004/
- Gå til "Detection Strategy"
- Svar: DET0546

Opgave 5 - Cyber Analytics Repository (CAR)

MITRE defines the Cyber Analytics Repository (CAR) as "a knowledge base of analytics developed by MITRE based on the MITRE ATT&CK adversary model. CAR defines a data model that is leveraged in its pseudocode representations, but also includes implementations directly targeted at specific tools (e.g., Splunk, EQL) in its analytics. With respect to coverage, CAR is focused on providing a set of validated and well-explained analytics, in particular with regard to their operating theory and rationale."

CAR is a collection of ready-made detection analytics built around ATT&CK. Each analytic describes how to detect an adversary's behavior. This is key because it allows you to identify the patterns you should look for as a defender. CAR also provides example queries for common industry tools such as Splunk, so you, as a defender, can translate ATT&CK TTPs into real detections.

Which ATT&CK Tactic is associated with CAR-2019-07-001?

- https://car.mitre.org/analytics/CAR-2019-07-001/
- Kig under "ATT&CK Detections"
- Svar: Defense Evasion

What is the Analytic Type for Access Permission Modification?

- https://car.mitre.org/analytics/CAR-2019-07-001/
- Kig efter "Analytic Type"
- Svar: Situational Awareness

Opgave 6 - MITRE D3FEND Framework

D3FEND (Detection, Denial, and Disruption Framework Empowering Network Defense) is a structured framework that maps out defensive techniques and establishes a common language for describing how security controls work. D3FEND comes with its own matrix, which is broken down into seven tactics, each with its associated techniques and IDs.

De 7 taktikker er: Model, Harden, Detect, Isolate, Deceive, Evict & Restore

Which sub-technique of User Behavior Analysis would you use to analyze the geolocation data of user logon attempts?

- https://d3fend.mitre.org/technique/d3f:UserBehaviorAnalysis/
- Gå til "Technique Subclasses"
- Svar: User Geolocation Logon Pattern Analysis

Which digital artifact does this sub-technique rely on analyzing?

- https://d3fend.mitre.org/technique/d3f:UserDataTransferAnalysis/
- Kig under "How it works"
- Svar: Network Traffic

Opgave 7 - Other MITRE Projects

Beyond the frameworks and tools we have discussed previously, MITRE offers several other projects designed to help cyber security professionals strengthen their skills, test their defenses, and outsmart attackers. In this task, we will briefly explore these tools and how they can support your growth in the field.

Caldera

- *Caldera is an automated adversary emulation tool designed to help security teams test and enhance their defenses. It provides the ability to simulate real-world attacker behavior utilizing the ATT&CK framework. This allows defenders to evaluate detection methods and practice incident response in a controlled environment. Caldera supports offensive and defensive operations, making it a powerful tool for red and blue team exercises.*

New and Emerging Frameworks

- **AADAPT (Adversarial Actions in Digital Asset Payment Technologies)**
  - *is a newly released knowledge base that includes its own matrix, covering adversary tactics and techniques related to digital asset management systems. AADAPT follows a*

similar structure to the ATT&CK Framework we covered previously and aims to help defenders understand and mitigate threats targeting blockchain networks, smart contracts, digital wallets, and other digital asset technologies.

- **ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems)**
  - *is a knowledge base and framework that includes a matrix, focusing on threats targeting artificial intelligence and machine learning systems. It documents real-world attack techniques, vulnerabilities, and mitigations specific to AI technology.*

What technique ID is associated with Scrape Blockchain Data in the AADAPT framework?

- https://aadapt.mitre.org/techniques/ADT3025/
- Kig efter "ID"
- Svar: ADT3025

Which tactic does LLM Prompt Obfuscation belong to in the ATLAS framework?

- https://atlas.mitre.org/techniques/AML.T0068
- Kig efter "Tactic"
- Svar: Defense Evasion

2026-02-20 13:33:05