# Øvelse 49 – (Eftermiddagsgruppeøvelse) MITRE ATT&CK: Taktikker, Teknikker, Mitigering og Detektering

## Formål

Formålet med denne øvelse er at opnå forståelse for, hvordan MITRE ATT&CK kan anvendes som et analytisk rammeværk til at strukturere og analysere angriberes adfærd.

Øvelsen har fokus på:

- Grundlæggende forståelse af begreber anvendt i MITRE ATT&CK
- Forståelse af rammeværkets struktur (taktik, teknik, procedure)
- Anvendelse af TTP'er til analyse og prioritering

Målet er, at I bliver i stand til selvstændigt at navigere i MITRE ATT&CK og anvende rammeværket som kilde og reference i analysearbejde.

Øvelsen danner fundament for senere arbejde med:

- Observerbarhed
- Detektion
- SIEM og IDS
- Design af detekteringsregler

MITRE ATT&CK er ikke en liste over værktøjer, men en struktureringsmodel for observeret angriberadfærd.

Øvelsen ligger primært på et videns- og forståelsesniveau og har til formål at opbygge et begrebsmæssigt fundament.

De teknikker og begreber, der introduceres her, vil senere blive anvendt i praksis, når vi arbejder med loganalyse og detektion i Wazuh.

---

## Baggrund

MITRE ATT&CK er en struktureret og empirisk baseret model over observeret angriberadfærd dokumenteret i virkelige sikkerhedshændelser.

ATT&CK er ikke en liste over exploits eller konkrete værktøjer.
Det er en systematiseret strukturering af adfærdsmønstre, der er observeret og dokumenteret gennem cyber threat intelligence.

Rammeværket organiserer denne adfærd i tre centrale niveauer:

- Taktikker (angriberens mål)
- Teknikker (metoder til at opnå målet)
- Procedurer (konkrete implementeringer af teknikker)

Formålet er at skabe et fælles sprog og en analytisk struktur til at beskrive, kategorisere og analysere angriberadfærd.

---

## ATT&CK som analytisk model

MITRE ATT&CK kan anvendes som en analytisk struktur til at fortolke og kategorisere observerbar adfærd i systemer.

Rammeværket indeholder ikke heuristikker i sig selv, men kan bruges heuristisk – som en struktureret reference, der hjælper med at genkende mønstre i adfærd.

En heuristik er en analytisk tommelfingerregel – en måde at identificere mønstre på uden at kende hele konteksten.

Hvis man eksempelvis observerer:

- Ændringer i privilegier
- Uautoriseret brug af administrative mekanismer

kan disse handlinger indikere bestemte teknikker i ATT&CK.

ATT&CK giver dermed en fælles struktur til at:

- Genkende mønstre i observeret adfærd
- Kategorisere hændelser
- Analysere risiko
- Prioritere forsvar ved at koble taktikker, teknikker og procedurer til kendte trusselsaktører

ATT&CK anvendes blandt andet i:

- Detection engineering
- Threat hunting
- Incident response
- Trusselsmodellering

- Strategisk sikkerhedsarbejde

---

## Empirisk grundlag og kobling til CTI

MITRE ATT&CK er baseret på dokumenteret cyber threat intelligence (CTI).
Teknikker og taktikker oprettes og vedligeholdes på baggrund af analyser af virkelige angreb, herunder:

- Offentlige trusselsrapporter
- Incident response-undersøgelser
- Malware-analyser
- Samarbejde med industri og myndigheder

Hver teknik refererer til konkrete kilder, der dokumenterer observeret anvendelse.

ATT&CK er dermed ikke en teoretisk model, men en systematisering af dokumenteret angriberadfærd.
Rammeværket opdateres løbende i takt med nye observationer.

Teknikker er knyttet til konkrete trusselsaktører og kampagner, hvilket gør det muligt at se:

- Hvilke grupper der anvender en given teknik
- I hvilke kontekster den er observeret

Ved at sammenholde:

- Observeret adfærd (TTP'er)
- Dokumentation (CTI)
- Kendte trusselsaktører

kan vi danne et kvalificeret billede af vores eget trusselslandskab.

ATT&CK fungerer dermed som bindeled mellem konkret observerbar adfærd og strategisk prioritering af forsvar.

---

## TTP'er som abstraktionsniveauer

TTP'er (Taktik, Teknik og Procedure) kan forstås som tre forskellige abstraktionsniveauer, der strukturerer angriberadfærd.

```
Taktik   →   Teknik   →   Procedure
(mål)        (metode)      (konkret handling)
```

Disse niveauer gør det muligt at bevæge sig mellem det konkrete og det overordnede:

- Proceduren er det observerbare spor i systemet
- Teknikken beskriver metoden bag handlingen
- Taktikken repræsenterer angriberens overordnede mål

Analyse i systemsikkerhed starter typisk med det konkrete (procedure) og bevæger sig opad mod teknik og taktik.

---

## Taktik – Målet

TA0004 – Privilege Escalation er en taktik i MITRE ATT&CK, der beskriver angriberens mål om at opnå højere rettigheder på et system.

Formålet med privilege escalation er at:

- Omgå sikkerhedsrestriktioner
- Udvide kontrol over systemet
- Få adgang til beskyttede ressourcer
- Understøtte videre bevægelse eller persistens

Det er vigtigt at forstå, at en teknik kan understøtte flere taktikker.
Der er ikke nødvendigvis et 1:1-forhold mellem teknik og taktik.

---

## Teknik – Metoden

Et eksempel på en teknik i MITRE ATT&CK er
*T1548 – Abuse Elevation Control Mechanism*.

Teknikken beskriver misbrug af legitime mekanismer, der normalt anvendes til kontrol af privilegier og adgang.

Eksempler kan være:

- `sudo` (Linux/macOS)
- `setuid` / `setgid`
- User Account Control (UAC) i Windows
- Andre privilegie- og adgangskontrolmekanismer

Det centrale er, at disse mekanismer i sig selv er legitime administrative funktioner.

Teknikken beskriver ikke deres eksistens, men misbrug eller manipulation af dem med henblik på at opnå uautoriserede rettigheder.

---

### Procedure – Den konkrete handling

En **procedure** er den konkrete, observerbare handling, der kan identificeres i et system.

Det er på dette niveau, vi finder faktiske spor – i logs, filsystemer eller proceslister.
Proceduren er ikke angriberens intention, men den handling vi konkret kan observere.

---

### Eksempel

```
sudo chmod u+s /bin/bash
```

Denne kommando sætter setuid-bitten på `/bin/bash`.

Hvis den udføres med tilstrækkelige rettigheder, kan `bash` efterfølgende køres med root-rettigheder.

Et tilsvarende spor i loggen kan se således ud:

```
Feb 13 14:21:02 ubuntu sudo: student : USER=root ; COMMAND=/bin/chmod u+s
/bin/bash
```

Her kan vi observere:

- Brug af `sudo`
- Ændring af filrettigheder
- Manipulation af en sikkerhedskritisk systemfil (`/bin/bash`)

Det er denne observerbare aktivitet, der udgør **proceduren**.

Analysen starter med proceduren og bevæger sig derfra mod teknik og taktik.

## MITRE ATT&CK som analytisk ramme

Efter gennemgangen af TTP-strukturen kan vi nu se, hvordan rammeværket anvendes i praksis.

Analyse med MITRE bevæger sig typisk gennem tre niveauer:

### Operationelt niveau

Vi starter med det observerbare – proceduren.
Det kan være en kommando, en ændring i filrettigheder eller en loghændelse.

### Taktisk niveau

Herefter kategoriseres handlingen:

- Hvilken teknik beskriver adfærden?
- Hvilken taktik understøtter den?

### Strategisk niveau

Til sidst vurderes den bredere betydning:

- Hvilke trusselsaktører anvender teknikken?
- Hvor relevant er den i vores kontekst?
- Skal vi prioritere mitigering, detektion eller begge?

## Instruktioner

I skal nu anvende rammeværket ved at udforske MITRE ATT&CK database gennem en række undersøgelser.

1. Undersøg TA0004 – Privilege Escalation
   - Hvad beskriver denne taktik?
   - Hvilket overordnet mål har angriberen?
   - Hvor i et angrebsforløb kan den forekomme?
2. Undersøg T1548 – Abuse Elevation Control Mechanism
   - Hvad beskriver teknikken?
   - Hvilke underteknikker findes?
   - Hvilke systemmekanismer kan misbruges?
3. Undersøg M1026 – Privilege Separation
   - Hvad er formålet med denne mitigering?
   - Hvordan relaterer den sig til T1548?
4. Undersøg relationen mellem ATT&CK og CTI
   - Hvad kan man finde om grupper i ATT&CK?
   - Hvad betyder APT?
   - Hvordan relaterer grupper sig til teknikker?

---

## Præsentation (5 minutter)

Gruppen skal lave en kort præsentation af:

- Hvad Privilege Escalation dækker over
- Hvad T1548 beskriver
- Hvad M1026 repræsenterer i rammeværket
- Hvordan disse elementer hænger sammen i MITRE ATT&CK

Fokus er på begrebsforståelse og sammenhæng – ikke på design af konkrete løsninger.

Præsentationen skal bruges næste undervisningsgang til opsamlingen.

---

## Refleksionsspørgsmål

- Hvad er forskellen på taktik, teknik og procedure?
- Hvorfor er det nyttigt at strukturere angriberadfærd?
- Hvordan kan MITRE ATT&CK hjælpe med at skabe overblik?
- Hvordan hænger ATT&CK og CTI sammen?

## Nyttige links

- Mitre ATT&CK

---

Last update: 2026-03-20 13:58:28