Heidelberg Materials

# Defensive Security

25.10.2025

# Wiederholung – 10 min

25.10.2025

Heidelberg Materials

# Ausgangssitia-tion

25.10.2025

Heidelberg Materials

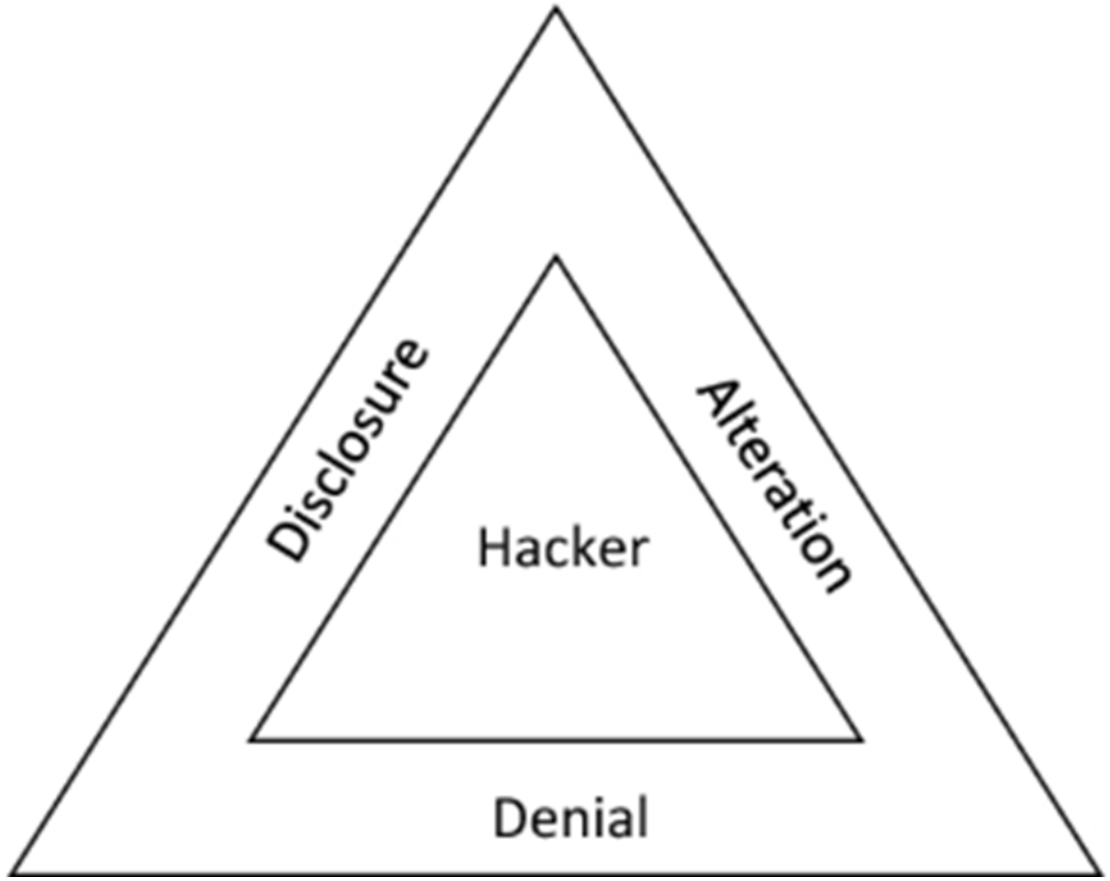
# Ausgangssituation GlobalTechIndustries

**GlobalTech Industries** ist ein **weltweit tätiger Produktionskonzern** mit Hauptsitz in Deutschland und Standorten in Europa, Asien und Nordamerika. Das Unternehmen produziert hochspezialisierte Komponenten für die **Luftfahrtindustrie** und betreibt ein komplexes Netzwerk aus Produktionsanlagen und Logistiksystemen.

Am frühen Montagmorgen meldet das Werk in Mexiko einen **Ausfall** des Produktionssystems. Gleichzeitig registriert das **Security Operations Center (SOC)** in Deutschland **verdächtigen Datenverkehr** zu einem unbekannten Server in Osteuropa. Innerhalb weniger Stunden breitet sich die Störung auf weitere Standorte aus – Maschinen lassen sich nicht mehr steuern, Lieferketten sind unterbrochen und interne Kommunikationssysteme sind gestört.

Eine erste Analyse zeigt: Ein gezielter **Angriff auf die industrielle Steuerungstechnik (ICS)** und das ERP-System ist im Gange. Es besteht der Verdacht auf einen **Advanced Persistent Threat (APT)** mit möglicher Beteiligung eines staatlich unterstützten Akteurs.

# Welche Ziele sind für GlobalTech Industries gefärdet?

# Einführung

25.10.2025

Heidelberg Materials

# Glossar - Wie hätte GlobalTech Industries sich vorbereiten können?

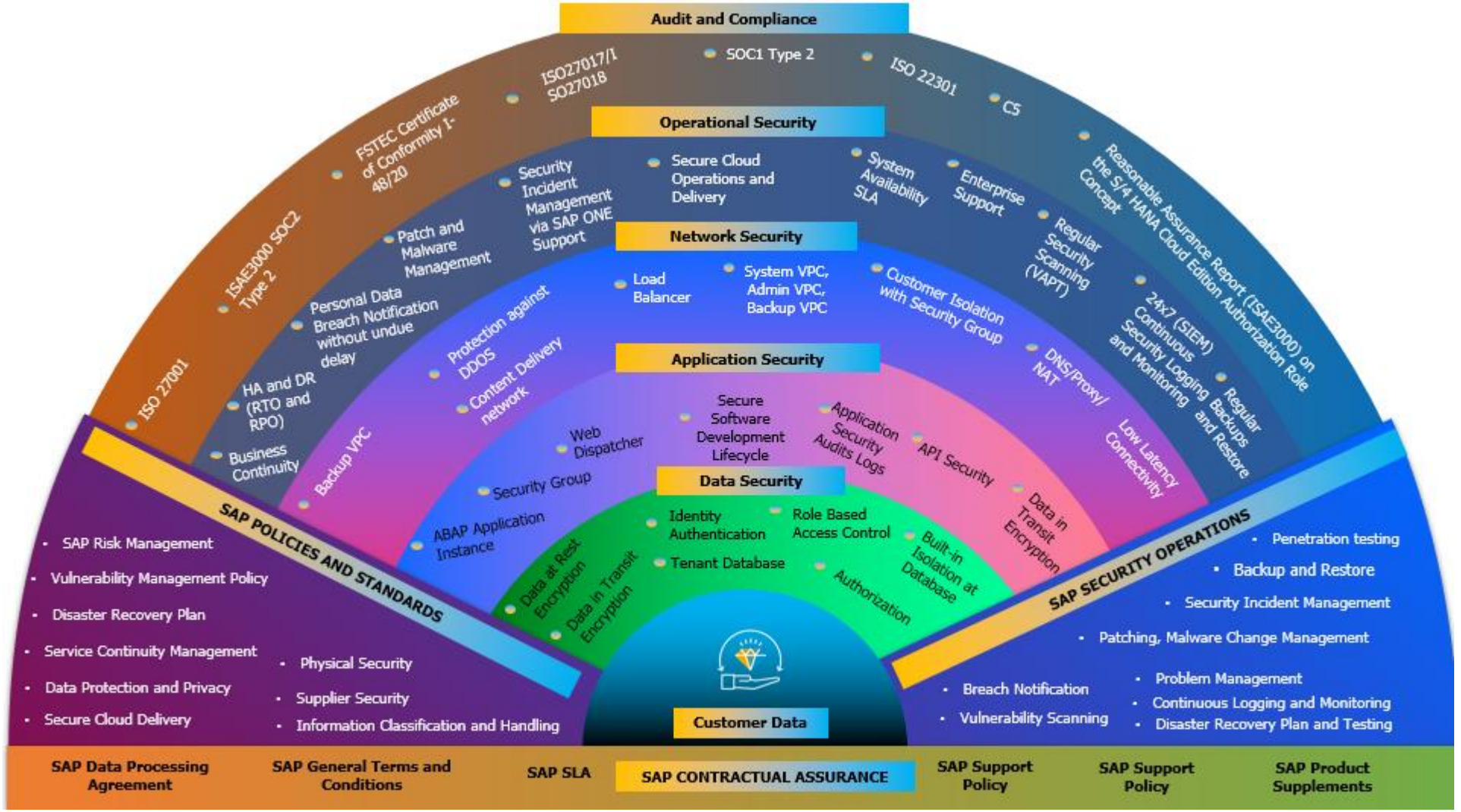
| Gruppe 1 – Security Operations | Gruppe 2 – Data Security | Gruppe 3 – Application Security | Gruppe 4 – Endpoint Security | Gruppe 5 – Network Security | Gruppe 6 – Perimeter Security |
|---|---|---|---|---|---|
| Security Operation Center (SOC) | Data Loss Prevention (DLP) | Least Privilege Principle & Need to Know | Patch Management | NIDS & NIPS | DMZ |
| SIEM & SOAR | Identity & Access Management (IAM) incl. MFA | Web Application Firewall (WAF) | EDR (Endpoint Detection & Response) vs. Antivirus vs. XDR | Firewalls | VPN |
| Playbooks & Incident Response Plan | Encryption | Secure Coding Practices (e.g. SBOM) | HIDS, HIPS | NAC | Security Gateways |
| Threat Intelligence | Data Classification, Masking & Tokenization | OWASP Top 10 | Disk Encryption (z. B. BitLocker) | Wireless Security | (Reverse) Proxy |
| Penetration Testing | Key Management (e.g. HSM) | Vulnerability Management | UEBA | Segmentation / VLANs | Zero Trust |
| Digital Forensics | Backup & Recovery | | | | Physical Security Measures (e.g. CCTV) |

Erklären Sie die Grundbegriffe, nennen Sie ggf. bekannte Tools und beantworten Sie folgende Fragen:

**Verhindert** (prevent), **erkennt** (detect) und/oder **reagiert** (respond) diese Maßnahme auf Cybersicherheitsvorfälle?
Handelt es sich um eine **administrative, technische** und/oder **physische** Maßnahme?

RISE with SAP: ‘Defense in Depth’ Security Archite... - SAP Community

# Defense-in-Depth / Layered Security – Beispiel ERP SAP S/4 HANA

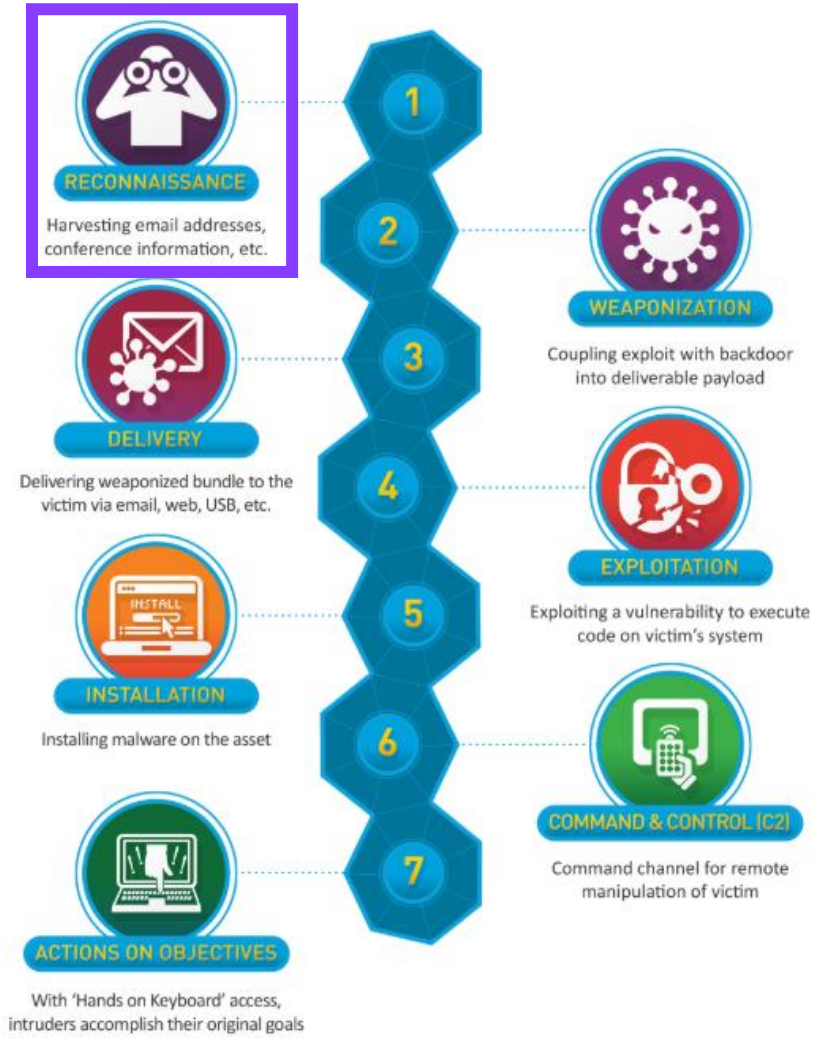


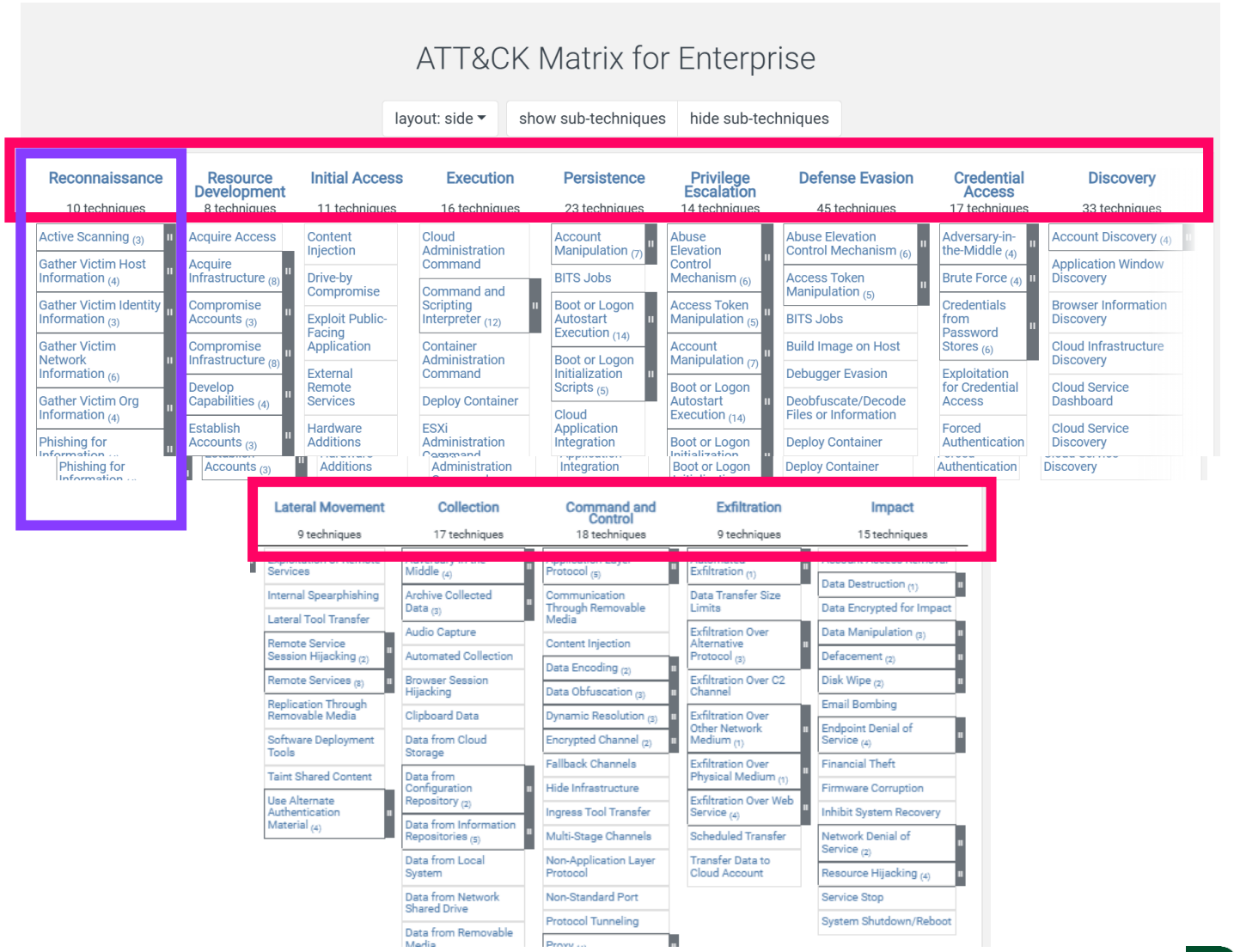
# MITRE ATT&CK vs. D3FEND

25.10.2025

Heidelberg Materials

# Cyber Kill Chain vs. MITRE ATT&CK Framework



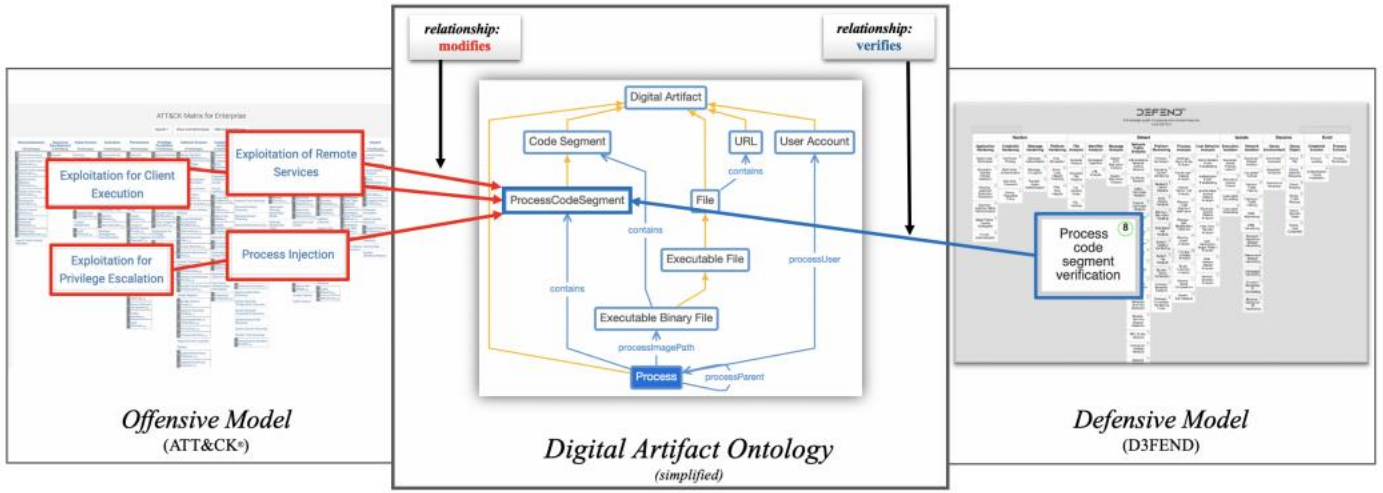



# MITRE ATT&CK & D3FEND

Was sind die **Unterschiede und Gemeinsamkeiten** zwischen dem Cyber Kill Chain und MITRE ATT&CK?

Was sind **Tactics**, **Techniques** & **Defenses/Mitigations**?

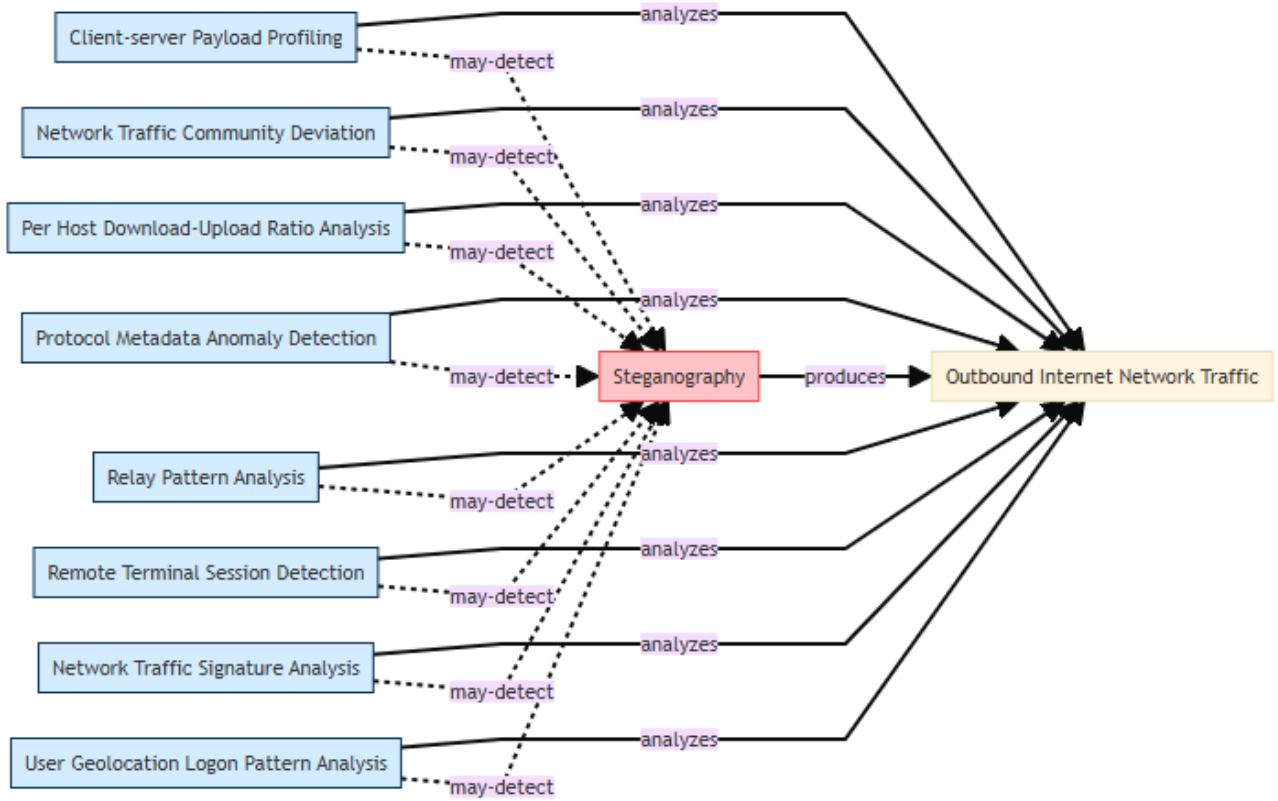
Schauen Sie sich das **MITRE D3FEND Model** an. Modellieren und diskutieren Sie die *Technique T1566* über "ATT&CK Lookup". Suchen Sie sich zwei weitere Techniques selbst aus.



# Beispiel Steganography - T1001.002

## Definition

Adversaries may **use steganographic** techniques **to hide command and control (C2) traffic** to make detection efforts more difficult. Steganographic techniques can be used to **hide data in digital messages** that are transferred between systems. This hidden information can be used for command and control of compromised systems. In some cases, the passing of files embedded using steganography, such as image or document files, can be used for command and control.



# SOC & SIEM

25.10.2025

Heidelberg Materials

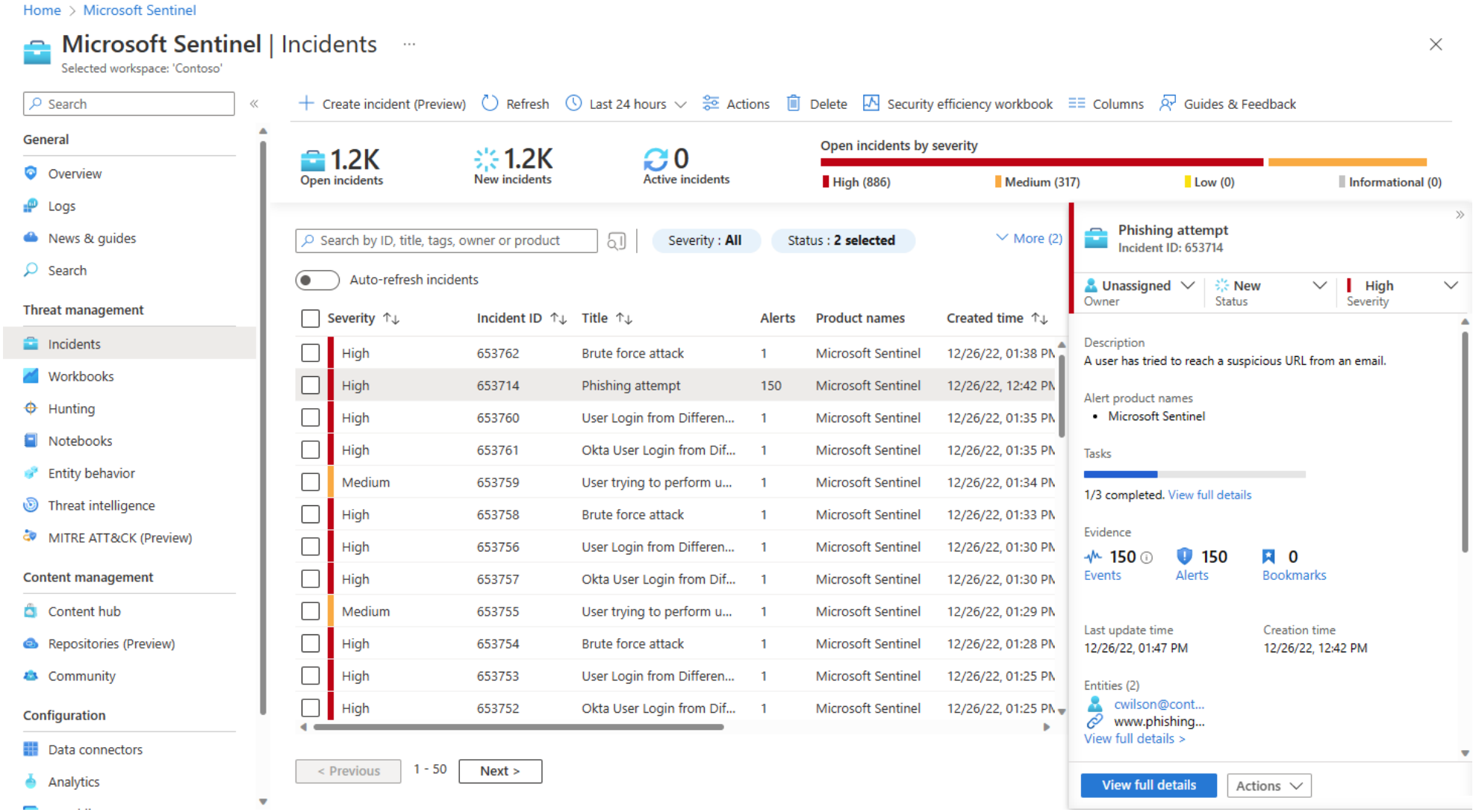
# Security Information & Event Management System (SIEM)

1. **Zentrale Log-Sammlung und –Analyse**: SIEM-Systeme sammeln und korrelieren Logdaten aus verschiedenen Quellen (Firewalls, Servern, Endpoints, etc.), um Sicherheitsvorfälle zu erkennen.
2. **Echtzeit-Erkennung von Bedrohungen**: Durch definierte Regeln und KI-gestützte Analysen erkennt ein SIEM verdächtige Aktivitäten und kann automatisch Alarme auslösen.
3. **Incident Response & Forensik**: Es ermöglicht eine schnelle Reaktion auf Sicherheitsvorfälle und unterstützt bei der Ursachenanalyse durch detaillierte Event-Historien.

**Figure 1: Magic Quadrant for Security Information and Event Management**

Was ist Microsoft Sentinel SIEM? | Microsoft Learn

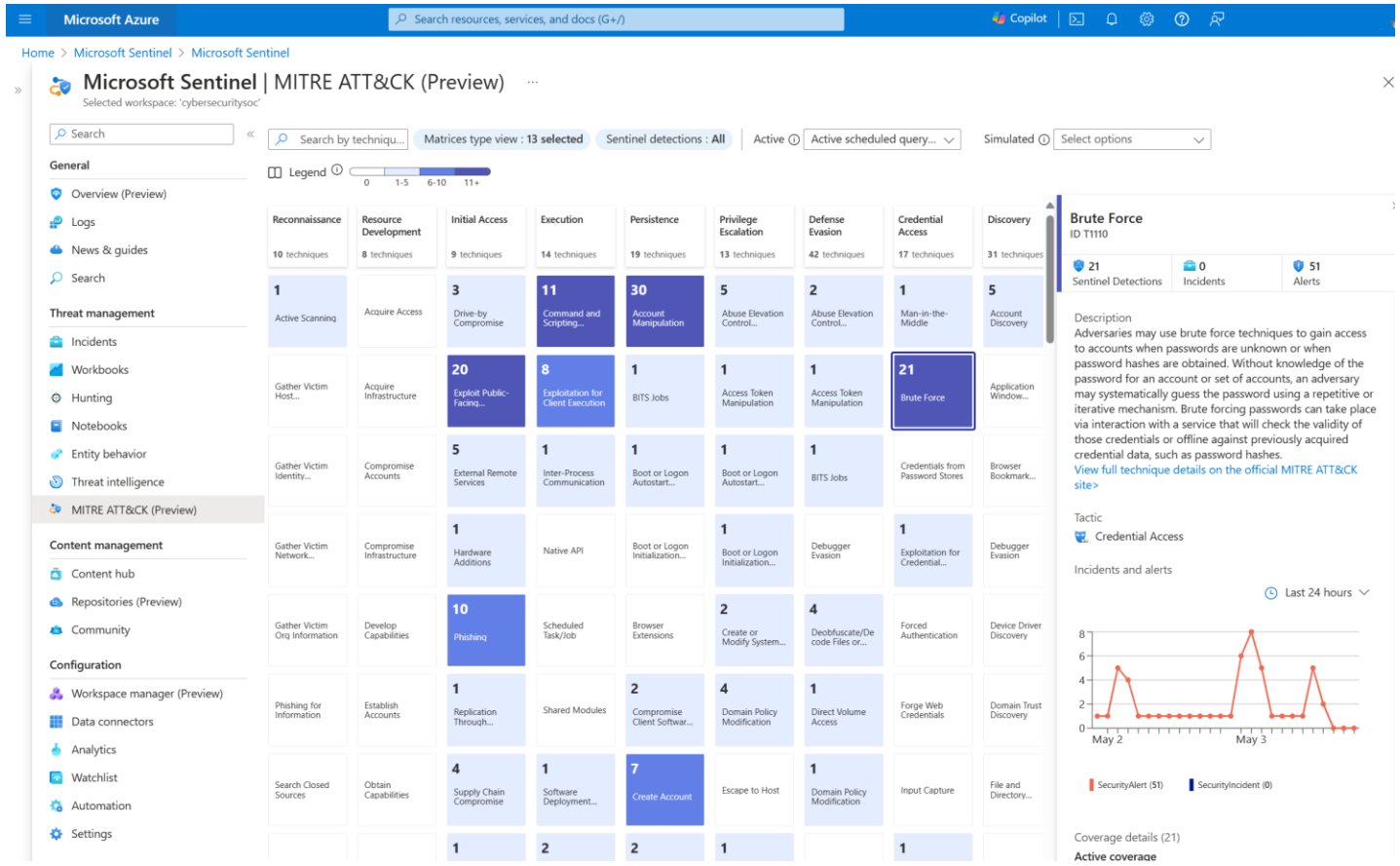
# MS Sentinel (SIEM Solution)



Was ist Microsoft Sentinel SIEM? | Microsoft Learn

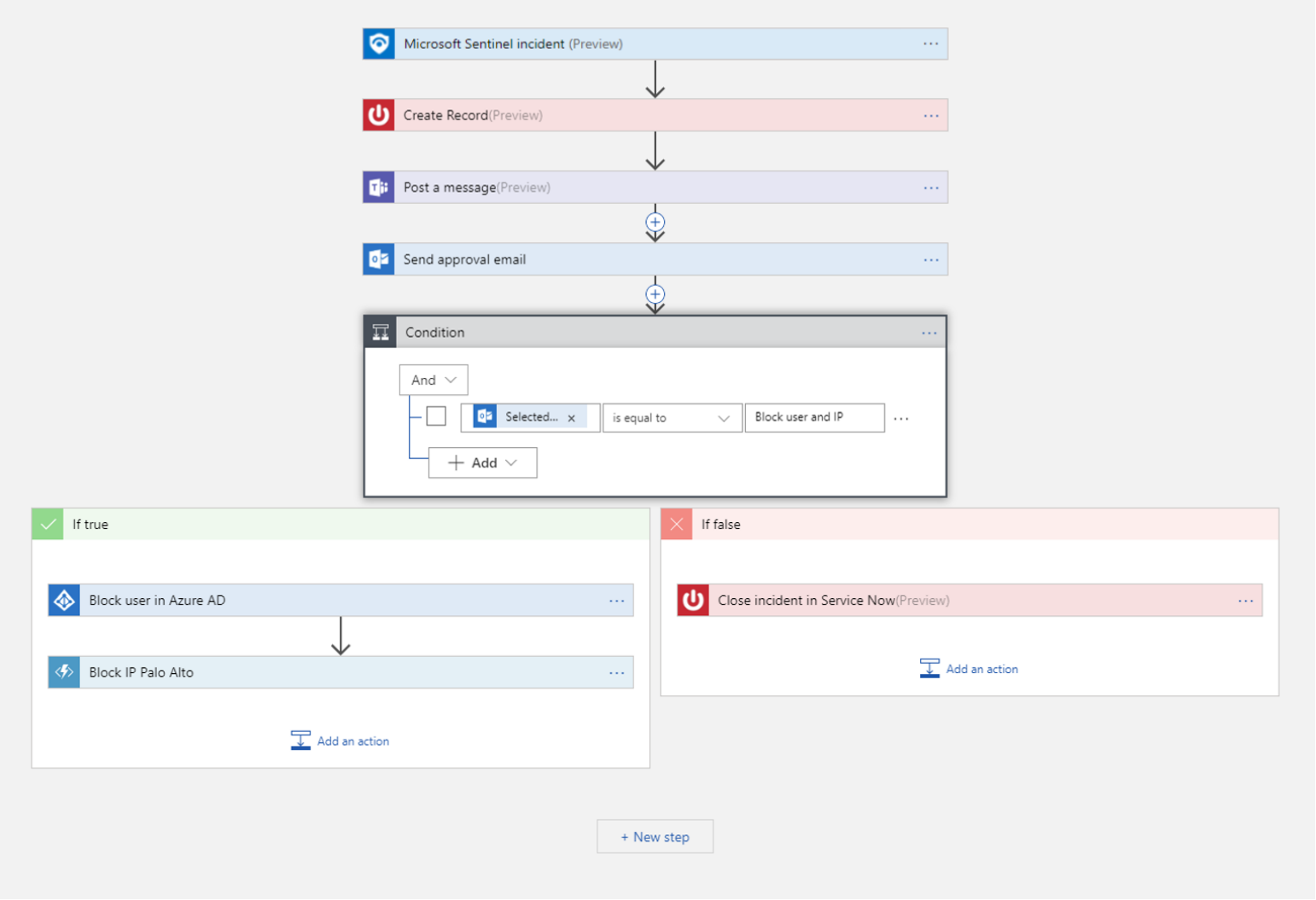
# MS Sentinel & MITRE ATT&CK

- SIEMs können Logdaten und **Alerts** bestimmten MITRE **ATT&CK-Techniken zuordnen** (Phase des Angriffs)
- SIEM-**Regeln** und **Use Cases** werden oft auf Basis von ATT&CK-Techniken erstellt.
- SIEMs bieten Dashboards, die zeigen, welche ATT&CK-Taktiken in der Umgebung beobachtet wurden (Statistik).
- In Kombination mit SOAR-Systemen können SIEMs **automatisiert auf erkannte ATT&CK-Techniken reagieren**, z. B. durch Isolierung eines Hosts bei „Command & Control“-Aktivitäten.



Was ist Microsoft Sentinel SIEM? | Microsoft Learn

# MS Sentinel: Automatisiert auf Incidents reagieren auf Basis von Workflows



# Security Operation Center (SOC)

Ein SOC überwacht, erkennt, analysiert und reagiert auf Sicherheitsvorfälle in Echtzeit: **24/7 an 365 Tagen**

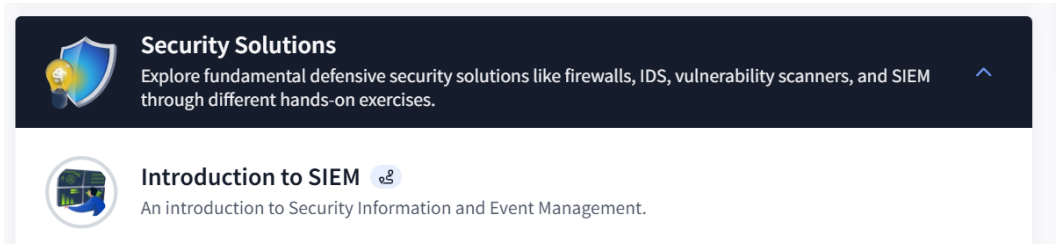
- Unternehmen können:
  - eigenes SOC ganzjährig betreiben (follow-the-sun)
  - hybrid arbeiten mit einem Partner (z.B. on-call)
  - ihr SOC vollständig outsourcen
- Wichtige Kennzahlen:
  - Mean Time to Detect (MTTD)
  - Mean Time to Respond (MTTR)
  - False Positive Rate
- Wichtige Rollen:
  - **Analysten** (Alert Monitoring & Incident Response)
  - Threat Hunter (Proaktive Suche)
  - Threat Intelligence Analyst

# Defense Security - SIEM

1. Erstellen Sie einen kostenlosen Account bei TryHackMe (THM)

2. Schreiben Sie sich für Cyber Security 101 ein

3. Absolvieren Sie das Modul **“Introduction to SIEM”**


https://tryhackme.com

# Gruppenarbeit: Backdoors & Breaches – 30 min

25.10.2025

Heidelberg Materials

# Aufgabe

Ihre Gruppe übernimmt die Rolle eines **SOC-Teams** bei GlobalTech Industries und nutzt das Spiel *Backdoors & Breaches*, um den Angriff zu analysieren, einzudämmen und geeignete Gegenmaßnahmen zu ergreifen.

1. Nutzen Sie die Karten, um ein mögliches Angriffsszenario zu rekonstruieren (Initial Compromise, Pivot & Escalate, C2 & Exfil, Persistence).
2. Diskutieren Sie die genutzen Taktiken & Techniques (auch auf Basis von MITRE ATT&CK).
3. Entwickeln Sie eine Incident-Response-Strategie (auch auf Basis von MITRE D3FEND):
    - Wie wird der Angriff im Szenario vom SOC erkannt (detect)?
    - Welche Maßnahmen werden sofort ergriffen?
    - Was sind die Lessons Learned für GlobalTech Industries? Wie kann man sich zukünftig schützen?
4. Präsentieren Sie Ihr Szenario.

*Hinweis: Wählen Sie einen Moderator in Ihrer Gruppe. Dieser trifft (realistische) Annahmen auf Basis der Ausgangssituation.*

# Gruppenarbeit Hacker-paragraph - 20 min

25.10.2025

Heidelberg Materials

# Der “Hackerparagraph” – 202c Strafgesetzbuch (StGB)

**§ 202 Verletzung des Briefgeheimnisses**

(1) Wer unbefugt

1. einen verschlossenen Brief oder ein anderes verschlossenes Schriftstück, die nicht zu seiner Kenntnis bestimmt sind, öffnet oder

2. sich vom Inhalt eines solchen Schriftstücks ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in § 206 mit Strafe bedroht ist.

(2) Ebenso wird bestraft, wer sich unbefugt vom Inhalt eines Schriftstücks, das nicht zu seiner Kenntnis bestimmt und durch ein verschlossenes Behältnis gegen Kenntnisnahme besonders gesichert ist, Kenntnis verschafft, nachdem er dazu das Behältnis geöffnet hat.

(3) Einem Schriftstück im Sinne der Absätze 1 und 2 steht eine Abbildung gleich.

**§ 202a Ausspähen von Daten**

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

# Der “Hackerparagraph” – 202c Strafgesetzbuch (StGB)

**§ 202b Abfangen von Daten**

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

**§ 202c Vorbereiten des Ausspähens und Abfangens von Daten**

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

# Der “Hackerparagraph” – 202c Strafgesetzbuch (StGB)

**§ 202d Datenhehlerei**

(1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der **Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten** dienen. Dazu gehören insbesondere

1. solche Handlungen von **Amtsträgern oder deren Beauftragten**, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie

2. solche **beruflichen Handlungen** der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.

# Gruppenarbeit 3: Bekannte Urteile zum “Hackerparagraphen”

Geben Sie den Studierenden eine Zusammenfassung folgender Urteile:

Gruppe 1: **BVerfG, Beschluss vom 18.05.2009 - 2 BvR 2233/07**

Gruppe 2: **AG Berlin-Tiergarten, 16.01.2017 - 327 Ds 44/16**

Gruppe 3: **Modern-Solution-Prozess / Hendrik Heinle (2023-2025)**

Gruppe 4: **Fall der Sicherheitsforscherin Lillith Wittmann (2021)**

Gruppe 5: **BGH, 13.05.2020 - 5 StR 614/19**

Gruppe 6: **BGH, Urteil vom 21.07.2015 – 1 StR 16/15**

# Themen und Hinweise

25.10.2025

Heidelberg Materials

# Cybercrime-as-a-Service: Wie Spezialisierung und Outsourcing die digitale Kriminalität verändern

1. Analysieren Sie das Geschäftsmodell „Cybercrime-as-a-Service“ und untersuchen Sie, wie Spezialisierung und Outsourcing die digitale Kriminalität verändern. Beschreiben Sie zunächst die Struktur der Underground Economy und die Rolle der neun Säulen des Cybercrime.
2. Erläutern Sie, wie Arbeitsteilung und Dienstleistungsangebote technisch weniger versierten Tätern den Zugang zu komplexen Straftaten ermöglichen.
3. Diskutieren Sie die ökonomischen und organisatorischen Vorteile für Täter sowie die Risiken für Unternehmen und Strafverfolgungsbehörden.
4. Verwenden Sie wissenschaftliche Quellen und Praxisbeispiele, um die Entwicklung und Professionalität dieser kriminellen Märkte zu belegen.
5. Bewerten Sie abschließend, welche Herausforderungen sich für Prävention, Detektion und internationale Strafverfolgung ergeben und geben Sie Handlungsempfehlungen für Unternehmen und Sicherheitsbehörden.

**Links:**

https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2021/Code2.html

# Modellierung und Bewertung eines Cybervorfalls im Unternehmenskontext unter Anwendung von Backdoors & Breaches

1. Modellieren Sie für Ihr Unternehmen einen möglichen Sicherheitsvorfall auf Grundlage der Spielmechanik von Backdoors & Breaches (Initial Access, Persistence, C2 & Exfil, Pivot & Escalate).
2. Erläutern Sie das mögliche Vorgehen der Angreifer detailliert. Verwenden Sie dazu wissenschaftliche Quellen und Praxisbeispiele.
3. Erstellen Sie den dazugehörigen fiktiven Incident Report (inkl. Grafische Timeline & Ablaufdiagramm) für einen Vorfall dieser Art.
4. Geben Sie Handlungsempfehlungen für eine zukünftige Sicherheitsstrategie.

**Links:**

https://www.blackhillsinfosec.com/tools/backdoorsandbreaches/

https://play.backdoorsandbreaches.com/play.backdoorsandbreaches.com-Engine-V1/App/

# Taktiken, Techniken und Gegenmaßnahmen: Modellierung eines Vorfalls mit MITRE ATT&CK und D3FEND

1. Modellieren Sie für Ihr Unternehmen einen möglichen Sicherheitsvorfall auf Grundlage von MITRE ATT&CK.
2. Erläutern Sie die eingesetzten Tactics & Techniques. Verwenden Sie dazu wissenschaftliche Quellen und Praxisbeispiele.
3. Wählen Sie für jede eingesetzte ATT&CK Technique die geeigneten D3FEND Technique aus. Begründen Sie, warum diese wirksam sind.
4. Visualisieren Sie das Szenario im D3FEND CAD Tool. Ziel ist eine grafische Darstellung der Defense-in-Depth-Verteidigungsarchitektur.

**Links:**

https://attack.mitre.org/

https://d3fend.mitre.org/

# Ethisches Hacken mit Kali Linux: Tools und Methoden im Überblick

1. Erläutern Sie, was ethisches Hacken bedeutet und wie es sich von illegalem Hacking abgrenzt. Gehen Sie dabei sowohl auf technische als auch auf die rechtlichen Unterschiede in Deutschland ein (inkl. Analyse bekannter Urteile).
2. Stellen Sie Kali Linux und die zentralen Tools vor, die typischerweise im Rahmen von Penetration Tests eingesetzt werden. Analysieren Sie deren Funktionsweise, Einsatzszenarien und Grenzen anhand konkreter Beispiele.
3. Vergleichen Sie Kali Linux mit alternativen Distributionen.

**Links:**

https://www.gesetze-im-internet.de/stgb/__202c.html

https://www.kali.org/

# OWASP Top 10 in der Praxis: Pentesting einer Webanwendung mit Kali Linux und OWASP ZAP

1. Im Rahmen dieser praktischen Arbeit führt der Studierende einen vollständigen Penetration Test auf die Webanwendung **OWASP Juice Shop** durch (eine absichtlich unsichere Anwendung, die speziell für Trainingszwecke entwickelt wurde).
2. Ziel ist es, typische Schwachstellen gemäß den **OWASP Top 10** zu identifizieren, zu analysieren und geeignete Gegenmaßnahmen zu entwickeln.
3. Der Studierende nutzen **OWASP ZAP** als zentrales Werkzeug zur Durchführung automatisierter und manueller Tests.
4. Die Arbeit umfasst die technische Dokumentation der einzelnen Schritte (von der Informationsbeschaffung über die Schwachstellenanalyse bis zur Risikobewertung).
5. Zusätzlich wird die Rolle von Pentesting im modernen Softwareentwicklungsprozessen reflektiert.

**Links:**

https://owasp.org/www-project-juice-shop/

https://owasp.org/www-project-top-ten/

https://www.zaproxy.org/

# Angriffssimulation mit Metasploit: Schwachstellenanalyse und Exploitation eines verwundbaren Systems

1. Im Rahmen dieser praktischen Arbeit führt der Studierende eine kontrollierte Angriffssimulation auf ein absichtlich verwundbares System durch: **Metasploitable 2**. Ziel ist es, mithilfe des Frameworks **Metasploit** eine Schwachstelle zu identifizieren, einen passenden Exploit auszuwählen und erfolgreich auszuführen.
2. Der Studierende soll dabei einen vollständigen Ablauf eines Penetration Tests nachvollziehen:
    - Einsatz von Kali Linux als Angreifer VM
    - Einsatz von Metasploitable 2 als Zielsystem in einer isolierten virtuellen Umgebung
    - Nutzung von Nmap zur Port- und Dienst-Erkennung
    - Durchführung eines Exploits mit Metasploit
    - Dokumentation des Angriffsverlaufs inkl. Screenshots und Logs
    - Analyse der Schwachstelle und Bewertung nach CVSS
    - Vorschläge zur Absicherung und ethische sowie rechtliche Reflexion

**Links:**

https://www.kali.org/

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

https://www.gesetze-im-internet.de/stgb/__202c.html

# Worauf sollte ich besonders achten?

## Hinweise zur Form

1. Halten Sie sich an die Vorlage und Vorgaben der DHBW
2. Zitieren Sie korrekt und konsequent (inkl. aller notwendigen Angaben)
3. Verwenden Sie qualitative hochwertige wissenschaftliche und praxisnahe Quellen
4. Lesen Sie auch Ihr Literaturverzeichnis vor der Abgabe nochmal Korrektur

Punkte für Form sind einfach erreicht und ebenso einfach verschenkt.

## Hinweise zum Inhalt

1. Erzählen Sie eine Geschichte / Halten Sie sich an Ihren roten Faden
2. Grenzen Sie das Thema zu Beginn ein und setzen Sie das Ziel der Arbeit fest
3. Schreiben Sie für ein informatiknahes Fachpublikum / Überlegen Sie sich, ob die Arbeit für Ihre Mitstudierenden verständlich ist und erläutern Sie relevante Fachbegriffe
4. Nutzen Sie Visualisierungen, um komplexe Inhalte verständlich darzustellen