HOW TO INTEGRATE MITRE ATT&CK INTO OFFICIAL SECURITY DOCUMENTATIONS

DESIREE SACHER-BOLDEWIN

ABOUT ME

Desiree Sacher-Boldewin

- Security Architect @ Finanz Informatik
- 10 years finance industry experience as IT Security Engineer & Security Analyst

Finanz Informatik

- German IT service provider for the German Savings Banks Finance Group
- 32k servers / 324k devices, incl. ATMs

finanz **informatik**

Disclaimer
The opinions and views expressed here are my own and do not represent the opinions of my employer

GOAL & WHY

Sustainable security

by building **intelligent processes**,

and **efficient workflows**

and detection capabilities

Intelligent processes – why?

- **guide employees to think the right way to learn to ask the right questions**

Efficient workflows – why?

- **prevent bore out and blunting of employees**
- **optimal use of internal resources**

  → save time and money

Efficient detection capabilities – why?

- **optimal use of vendor capabilities**

  → save time and money

How?
By enabling all employees to fulfill the responsibility that is expected of them and giving the SOC the chance to do the job they are actually here for..

CONCEPT OF «SECURITY DOCUMENTATION»

- Often used in regulated environments
  - Verified with ISO27001:2013 A.14.1
  - BSI IT Grundschutz Standard 100-2 –Chapter 4
- Documents security requirements by analysing
  - Application description
  - Systems used and «object of protection»
  - Analysis of threats, probability of occurence, effects
  - Security measures to decrease likelihood of risk occuring
  - Remaining or residual risk → «accepted the risk»

Subcategory
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
PR.DS-2: Data-in-transit is protected
PR.DS-5: Protections against data leaks are implemented
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
PR.IP-2: A System Development Life Cycle to manage systems is implemented
PR.PT-4: Communications and control networks are protected

Source: NIST Cybersecurity Framework - https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx

CHALLENGE WITH TRADITIONAL «THREAT CATALOGUE»

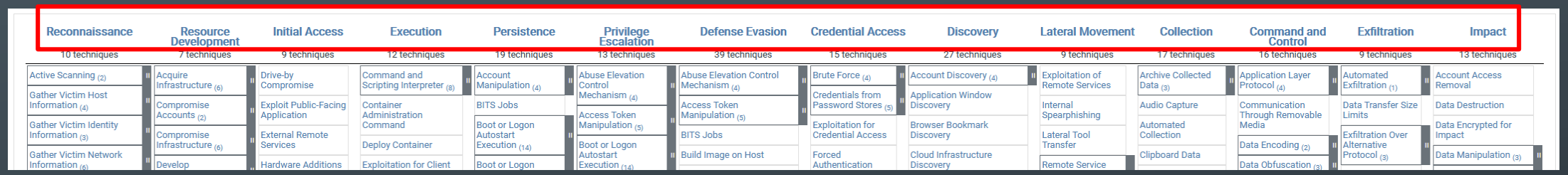
...AND WHY WE NEED A BRIDGE

- Traditional threats of «earth, wind and fire»..
  - Physical attack (deliberate /intentional)
  - Unintentional damange /loss of information or IT assets
  - Disaster (natural, environmental)
  - Failures/Malfunction
  - Outages
  - Eavesdropping /Interception /Hijacking
  - Nefarious Activity /Abuse
  - Legal

- Auditors look for a reasonable derivation why what protection or detection method was selected
- SOCs want to use MITRE ATT&CK Techniques
- Shift responsibility from SOC to technical engineering teams to support creation and prioritizing of rules

Source: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

BUILDING BRIDGES..



Source: https://attack.mitre.org/matrices/enterprise/

- Techniques are too specific for «normal people»
- Tactics are not as dynamic as techniques
- Current threat catalogue should not be completely thrown over…

APPLICATION GROUPS

- ...based on general threat landscape

A Internet facing Applications/Systems

B All (general) applications

C User/Admin devices

- Frontend applications & data gateways face different threats than internal only applications
- Focus DLP capabilities on relevant applications

MAPPING THE THREATS

- A Internet facing Applications/Systems
- B All (general) applications
- C User/Admin devices

MITRE ATT&CK Tactic		Related Threat	Threat analysis depth level
Reconnaissance	A	The adversary is trying to gather information they can use to plan future operations.	Internet facing Applications/Systems
Resource Development	B	The adversary is trying to establish resources they can use to support operations by manipulating a trust dependency.	All applications tactic relevance
Initial Access	A C	The adversary is trying to get into your network.	User/Admin devices, Internet facing Applications/Systems
Execution	B	The adversary is trying to run malicious code.	All applications tactic relevance
Persistence	B	The adversary is trying to maintain their foothold.	All applications tactic relevance
Privilege Escalation	B	The adversary is trying to gain higher-level permissions.	All applications tactic relevance
Defense Evasion	B	The adversary is trying to avoid being detected.	All applications tactic relevance
Credential Access	B	The adversary is trying to steal account names and passwords.	All applications tactic relevance

MAPPING THE THREATS

- A Internet facing Applications/Systems
- B All (general) applications
- C User/Admin devices

MITRE ATT&CK Tactic		Related Threat	Threat analysis depth level
Discovery	B	The adversary is trying to figure out your environment.	All applications tactic relevance
Lateral Movement	B	The adversary is trying to move through your environment.	All applications tactic relevance
Collection	B	The adversary is trying to gather data of interest to their goal.	All applications tactic relevance
Command and Control	B	The adversary is trying to communicate with compromised systems to control them.	All applications tactic relevance
Exfiltration	A C	The adversary is trying to steal data.	User/Admin devices, Internet facing Applications/Systems, All applications tactic relevance
Impact	B	The adversary is trying to manipulate, interrupt, or destroy your systems and data.	All applications techniques relevance

MAPPING THE THREATS

A Internet facing Applications/Systems
B All (general) applications
C User/Admin devices

MITRE ATT&CK Tactic	Related Threat
Impact B	The adversary is trying to manipulate, interrupt, or destroy your systems and data.
- Account Access Removal (T1531)	Account access/permissions are removed
- Data Destruction (T1485)	Data is destroyed by overwriting the file system
- Data Encrypted for Impact (T1486)	Encryption of data by attacked
- Data Manipulation (T1565)	Manipluation is possible
- Stored Data Manipulation	... For stored data
- Transmitted Data Manipulation	... For data in transmission
- Runtime Data Manipulation	... For data at runtime
- Defacement (T1491)	The application is defaced
- Disk Wipe (T1561)	Data is wiped from disks
- Endpoint Denial of Service (T1499)	Customer service access can be denied
- Firmware Corruption (T1495)	Firmware is being corrupted
- Inhibit System Recovery (T1490)	Standard recovery procedure is inhibited
- Network Denial of Service (T1498)	Network ressources are denied of service
- Resource Hijacking (T1496)	Resources are hijacked by attacker
- Service Stop (T1489)	Services are stopped by the attackers in an uncontrolled matter
- System Shutdown/Reboot (T1529)	System is shutdown or rebooted by the attacker in an uncontrolled matter

MAPPING THE THREATS

- A Internet facing Applications/Systems
- B All (general) applications
- C User/Admin devices

MITRE ATT&CK Tactic	Related Threat
Initial Access A C	The adversary is trying to get into your network.
- Drive-by Compromise (T1189)	Malware is transmitted to system when surfing the web A C
- Exploit Public-Facing Application (T1190)	Public-facing application is exploited through vulnerability A
- External Remote Services (T1133)	External facing remote services like VPNs, Citrix, WinRM are misused A
- Hardware Additions (T1200)	Adversary enters the infrastructure by using malicious hardware C
- Phishing (T1566)	Malware is transmitted via phishing messages C
- Replication Through Removable Media (T1091)	Malware is distributed via removable media like USB sticks C
- Supply Chain Compromise (T1195)	Malware is transmitted via compromised supplier A
- Trusted Relationship (T1199)	A trusted party is exploited and used to tranfer malware C
- Valid Accounts (T1078)	Stolen valid credentials are used to access the infrastructure A

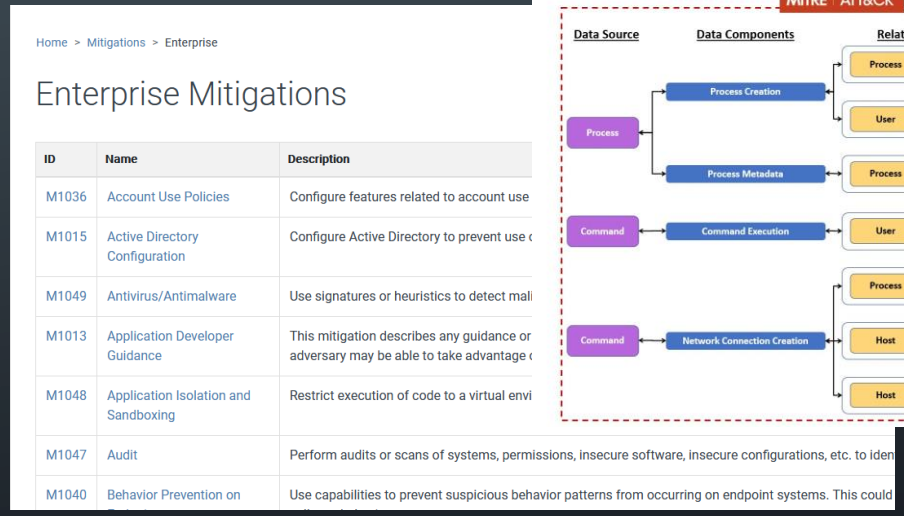
MAPPING THE THREATS

- A Internet facing Applications/Systems
- B All (general) applications
- C User/Admin devices

MITRE ATT&CK Tactic	Related Threat
Exfiltration A C	The adversary is trying to steal data.
- Automated Exfiltration (T1020)	Exfiltration is possible over automated procedures that are not monitored A C
- Data Transfer Size Limits (T1030)	Data can be exfiltrated in fixed size chunks A C
- Exfiltration Over Alternative Protocol (T1048)	Exfiltration is possible over additional unnoticed network connections A C
- Exfiltration Over C2 Channel (T1041)	Exfiltration is possible over directly executed malware A C
- Exfiltration Over Other Network Medium (T1011)	Exfiltration is possible over a different network medium like Bluetooth or LTS, etc A C
- Exfiltration Ove Physical Medium (T1052)	Exfiltration is possible over physical medium, like USB C
- Exfiltration Over Web Service (T1567)	Exfiltration is possible over web services like code repositories or cloud storage A C
- Scheduled Transfer (T1029)	Exfiltration is possible by using scheduled transfer times or intervals that are not monitored A C
- Transfer Data to Cloud Account (T1537)	Exfiltration is possible by using connections opened for access to cloud accounts A C

BENEFITS

- “Official” relevance assessment reasons usage of security tools on all infrastructure
- Easy way to build standardized technical catalogues for threats, mitigations and detection capabilities

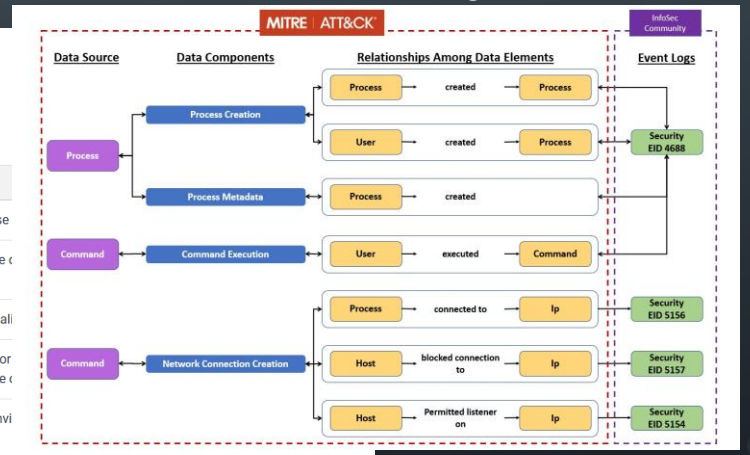


Home > Mitigations > Enterprise

Enterprise Mitigations

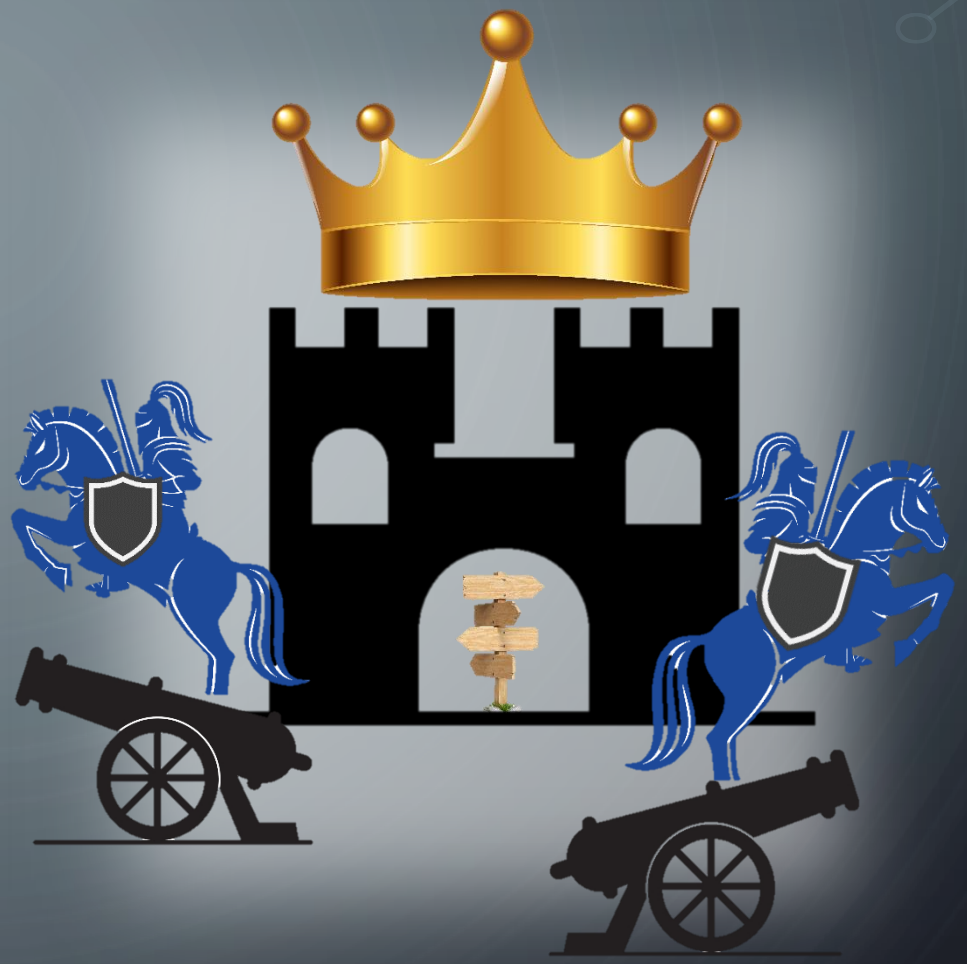
ID	Name	Description
M1036	Account Use Policies	Configure features related to account use
M1015	Active Directory Configuration	Configure Active Directory to prevent use
M1049	Antivirus/Antimalware	Use signatures or heuristics to detect mali
M1013	Application Developer Guidance	This mitigation describes any guidance or adversary may be able to take advantage
M1048	Application Isolation and Sandboxing	Restrict execution of code to a virtual envi
M1047	Audit	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to iden
M1040	Behavior Prevention on	Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could

Source: https://attack.mitre.org/mitigations/enterprise/



Source: https://github.com/mitre-attack/attack-datasources

QUESTIONS?



- Twitter: @d3sre
- More of my work can be found on https://github.com/d3sre/

ANNEX

MAPPING MITRE ATT&CK TACTICS TO ENISA THREAT TAXONOMY

ID	Name	Description	Nefarious Activity /Abuse
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.	Targeted attacks (APTs etc.)
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.	Generation and use of rogue certificates
TA0001	Initial Access	The adversary is trying to get into your network.	Receive of unsolicited E-mail; Social Engineering;
TA0002	Execution	The adversary is trying to run malicious code.	Malicious code/ software/ activity
TA0003	Persistence	The adversary is trying to maintain their foothold.	Unauthorized installation of software;
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.	Unauthorized activities
TA0005	Defense Evasion	The adversary is trying to avoid being detected.	Misuse of audit tools;
TA0006	Credential Access	The adversary is trying to steal account names and passwords.	Identity theft (Identity Fraud/ Account); Brute force
TA0007	Discovery	The adversary is trying to figure out your environment.	
TA0008	Lateral Movement	The adversary is trying to move through your environment.	
TA0009	Collection	The adversary is trying to gather data of interest to their goal.	Abuse of authorizations
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.	Remote activity (execution)
TA0010	Exfiltration	The adversary is trying to steal data.	Abuse of Information Leakage; Compromising confidential information (data breaches)
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.	Denial of service; Manipulation of hardware and software; Manipulation of information; Failed of business process; Misuse of information/ information systems (including mobile apps)