Abbildung und Simulation cyber-physischer Bedrohungen für kritische Infrastrukturen

Michael Mundt, Harald Baier

30. DFN-Konferenz „Sicherheit in vernetzten Systemen“

08.-10. Februar 2023, Grand Elysée Hotel Hamburg

Agenda

- Motivation
- Cyber Threat Intelligence
- Verortung cyber-physischer Objekte
- Verkettung der Informationsmodelle
- Use Case: SIEM Alarmierung

KRITIS…Kritische Infrastrukturen
CTI……Cyber Threat Intelligence
ICS……Industrial Control Systems
SIEM…..Security Information and Event Management

Agenda

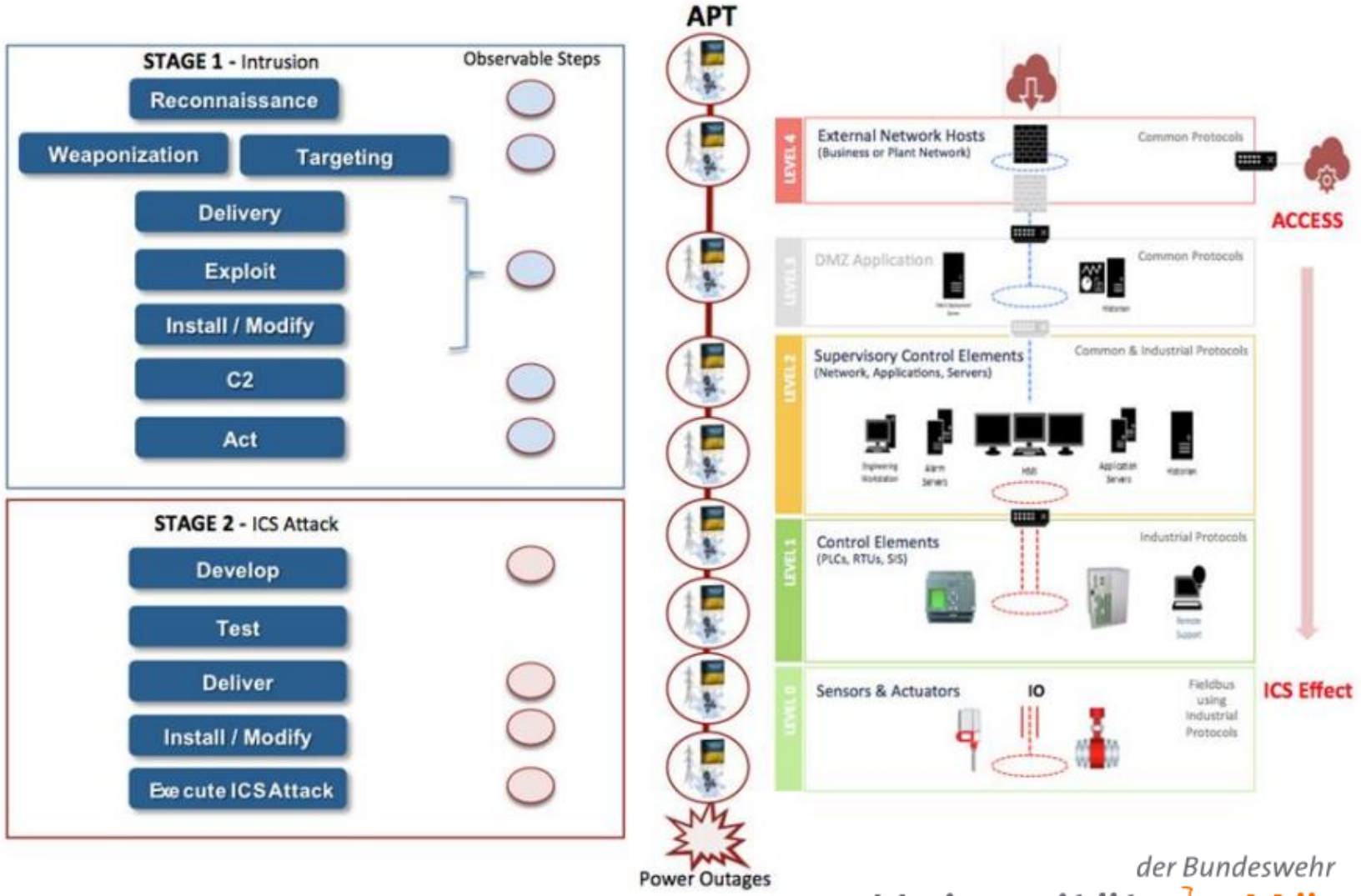
- **Motivation**
- Cyber Threat Intelligence
- Verortung cyber-physischer Objekte
- Verkettung der Informationsmodelle
- Use Case: SIEM Alarmierung

KRITIS…Kritische Infrastrukturen
CTI……Cyber Threat Intelligence
ICS……Industrial Control Systems
SIEM…..Security Information and Event Management

Analyse des Angriffs auf die Energieversorgung

Ukraine, 18. März 2016

Electricity – Information Sharing and Analysis Center



Quelle: Internet
https://scadahacker.com/library/Documents/Cyber_Events/E-ISAC%20-%20Analysis%20of%20the%20Cyber%20Attack%20on%20the%20Ukrainian%20Power%20Grid.pdf
Aufgerufen 29.01.2023

Analyse des Angriffs auf die Energieversorgung

Ukraine, 18. März 2016

- Langzeit-Aufklärung
  - Datenexfiltration, Vorbereitung und Tests

- Schwerpunkt des Angriffs
  - Ausführung von SCADA Funktionen zur Abschaltung der Versorgung
- Flankierende Angriffe
  - Löschen (KillDisk) von Arbeitsstationen, Servern und Fernzugriffsstationen
  - Einsatz maliziöser Firmware auf Serial-to-Ethernet Geräten in den verteilten Stationen
- Weitere Störungen und Ablenkungen
  - Planmäßige Trennungen von UPS
  - DoS gegen die Support-Hotline des Unternehmens

DoS…Denial of Service

UPS…Uninterruptable Power Supplies

Agenda

- Motivation
- **Cyber Threat Intelligence**
- Verortung cyber-physischer Objekte
- Verkettung der Informationsmodelle
- Use Case: SIEM Alarmierung

KRITIS…Kritische Infrastrukturen
CTI……Cyber Threat Intelligence
ICS……Industrial Control Systems
SIEM…..Security Information and Event Management

Standards About us News Taking part Store Search

ISO/IEC 27001:2022

Information security, cybersecurity and privacy manage

Control 5.7 - Threat Intelligence

A notable addition to the new standard is Control 5.7, which refers to Threat Intelligence. This covers the need for organizations to collect, analyze, and produce threat intelligence relating to information security threats. In today's environment of an ever-changing threat landscape, cyber threat intelligence allows firms to take preventative measures before an attack begins.

For maximum efficiency, ISO advises three aspects of intelligence.

Strategic	Operational	Tactical
•Information on Threat Landscape, security architecture, aligning with strategy, emerging threats, prioritized and tailored reporting	•Information on attacks, threat actors, mapping with frameworks, gap assessment, diverse sources	•Information on recent attacks and indicators of compromise, proative detection, real time insights

Abstract

This document specifie
maintaining and continu
system within the conte
requirements for the as
tailored to the needs of

MITRE ATT&CK Framework

Cyber Threat Intelligence

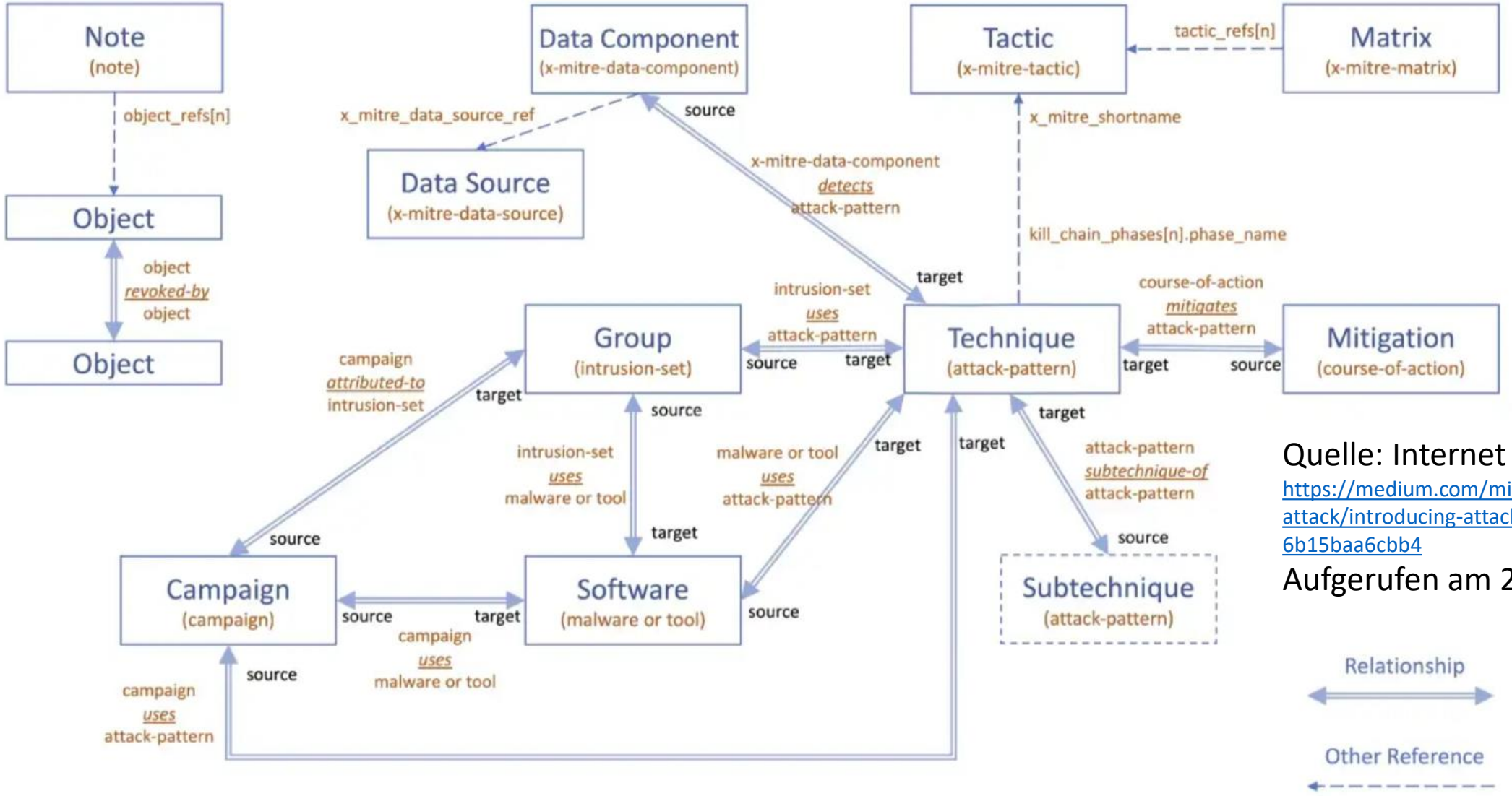
- Weltweit zugängliche Wissendatenbank
- Gegnerische Ziele und Techniken
- Ausgewertete Cyber-Analyseberichte
- Life Cycle Management durch die MITRE Corporation

Quelle: Internet
https://mitre-attack.github.io/attack-navigator/
Aufgerufen am 27.01.2023

ATT&CK…Adversarial Tactics, Techniques and Common Knowledge

MITRE ATT&CK Framework

Objektmodell



Quelle: Internet

https://medium.com/mitre-attack/introducing-attack-campaigns-6b15baa6cbb4

Aufgerufen am 21.01.2023

MITRE ATT&CK Framework

Eingehende Informationsquellen

- Threat Intelligence Berichte
- Konferenz-Präsentationen
- Webinare
- Social Media
- Blog-Einträge
- Open Source Code Repositories
- Malware Samples

Quelle: Internet
https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
Aufgerufen am 29.01.2023

MITRE ATT&CK Framework

Auswertung von Informationsquellen

- Aus Rohdaten

```
UPLOAD file (upload a file server->client)
DOWNLOAD file (download a
SHELL command (runs a command
PSHELL command (runs a command via power
EXEC path (executes a PE at the
```

Command and Control – Remote File Copy (T1105)

Execution - Command-Line Interface (T1059)

Execution - Powershell (T1086)

Execution - Execution through API (T1106)

- Aus finalisierten Berichten

The most interesting PDB string is the "`4113.pdb`," which appears to reference CVE-2014-4113. This CVE is a local kernel vulnerability that, with successful exploitation, would give any user SYSTEM access on the machine.

The malware component, `test.exe`, uses the Windows command "`cmd.exe" /C whoami`" to verify it is running with the elevated privileges of "System" and creates persistence by creating the following scheduled task:

```
schtasks /create /tn "mysc"  exe /sc ONLOGON
```

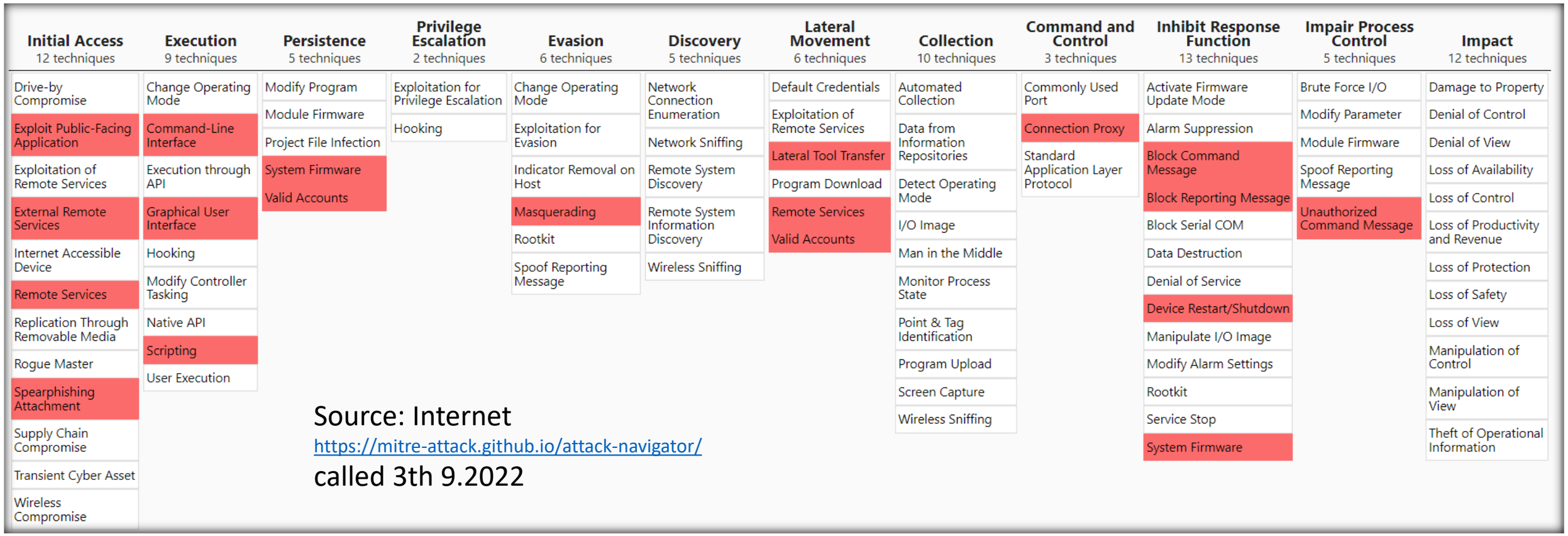
[Tactic] | 1. [Technique]

[Tactic] | 2. [Technique]

When executed, the malware first establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913. The malware sends the SOCKS5 connection request "`05 01 00`" and verifies the server response starts with "`05 00`".

Sandworm Advanced Persistent Threat

MITRE ATT&CK Framework – Enterprise, ICS, Mobile Matrizen



Initial Access 12 techniques	Execution 9 techniques	Persistence 5 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 6 techniques	Collection 10 techniques	Command and Control 3 techniques	Inhibit Response Function 13 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

Source: Internet

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

called 3th 9.2022

Agenda

- Motivation
- Cyber Threat Intelligence
- **Verortung cyber-physischer Objekte**
- Verkettung der Informationsmodelle
- Use Case: SIEM Alarmierung

KRITIS…Kritische Infrastrukturen
CTI……Cyber Threat Intelligence
ICS……Industrial Control Systems
SIEM…..Security Information and Event Management

Purdue Modell

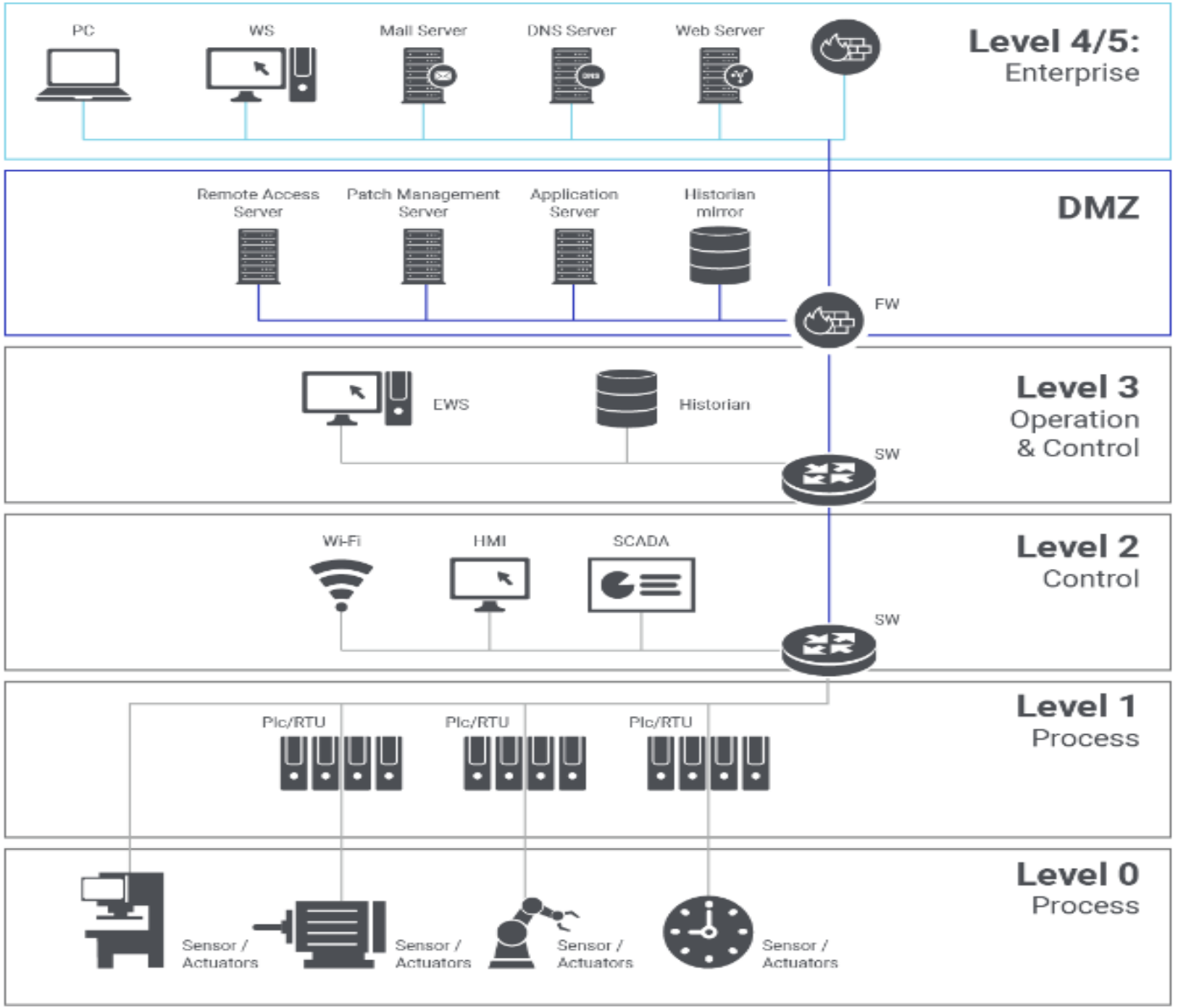
Enterprise Referenz-Architektur

Quelle: Internet
https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security
Aufgerufen am 29.01.2023

DMZ…Demilitarisierte Zone

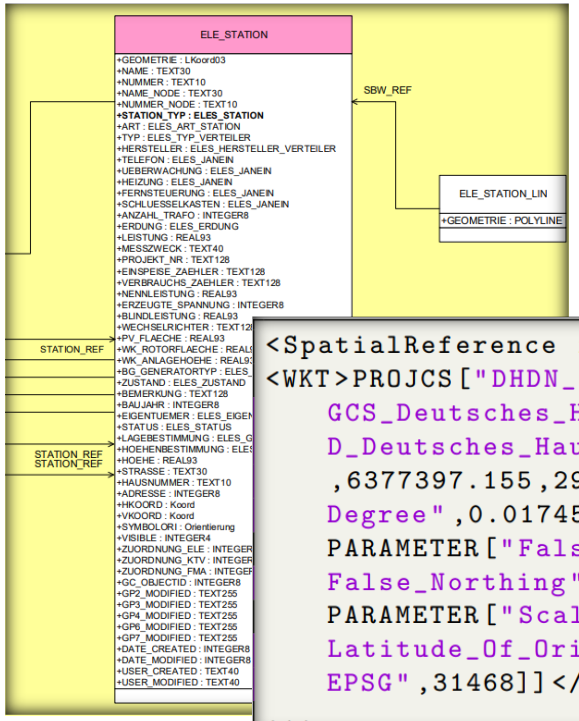
der Bundeswehr Universität München

esri Deutschland



GIS Objektmodell

Verortung von Assets

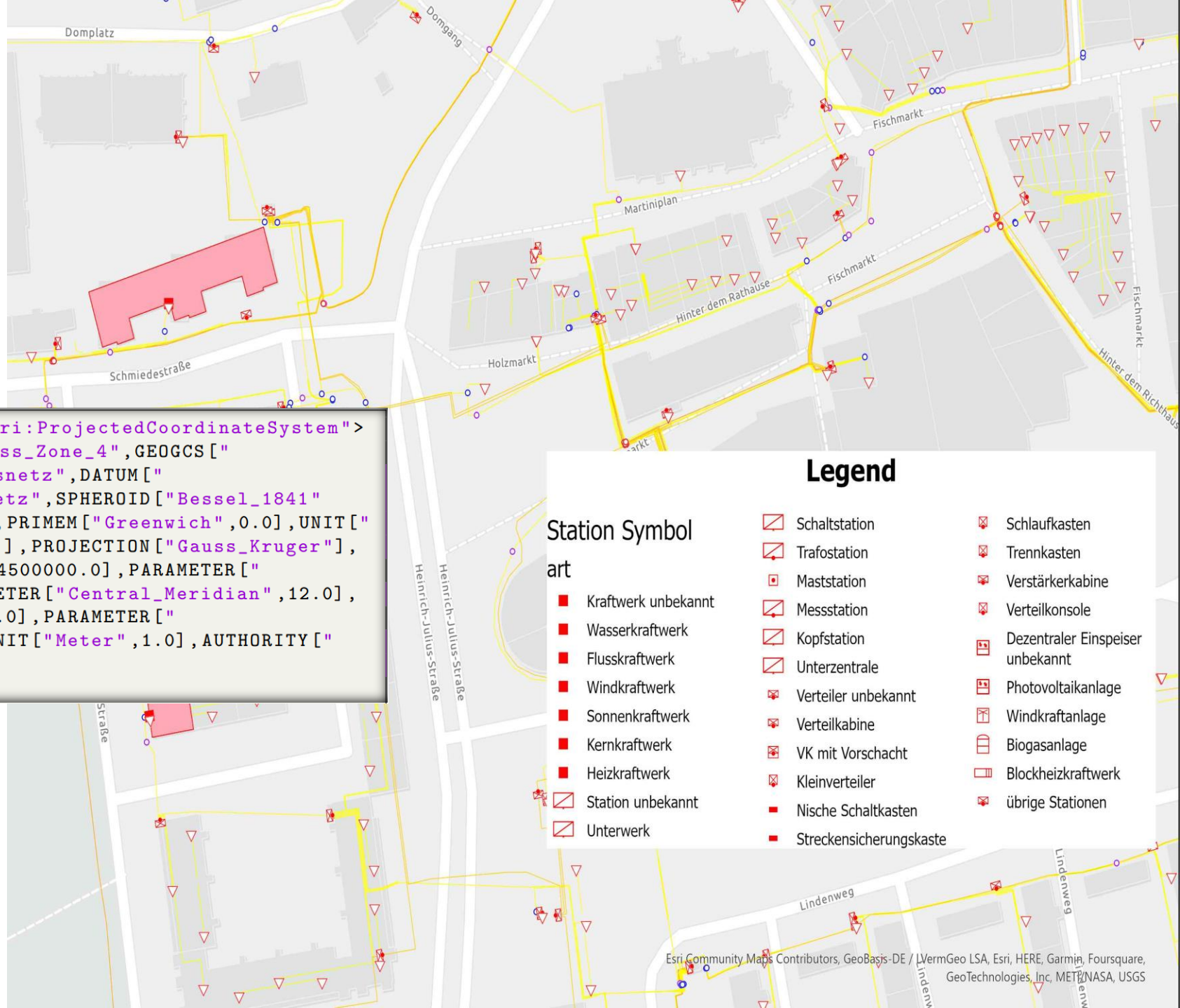



```
<SpatialReference xsi:type="esri:ProjectedCoordinateSystem">
<WKT>PROJCS["DHDN_3_Degree_Gauss_Zone_4",GEOGCS["
    GCS_Deutsches_Hauptdreiecksnetz",DATUM["
    D_Deutsches_Hauptdreiecksnetz",SPHEROID["Bessel_1841"
    ,6377397.155,299.1528128]],PRIMEM["Greenwich",0.0],UNIT["
    Degree",0.0174532925199433]],PROJECTION["Gauss_Kruger"],
    PARAMETER["False_Easting",4500000.0],PARAMETER["
    False_Northing",0.0],PARAMETER["Central_Meridian",12.0],
    PARAMETER["Scale_Factor",1.0],PARAMETER["
    Latitude_Of_Origin",0.0],UNIT["Meter",1.0],AUTHORITY["
    EPSG",31468]]</WKT>
...
```

GIS…Geografisches Informationssystem

der Bundeswehr Universität München

esri Deutschland



MITRE ATT&CK Objektmodell

Zuweisung von Assets

Quelle: Internet

https://collaborate.mitre.org/attackics/img_auth.php/3/37/ATT&CK_for_ICS_-_Philosophy_Paper.pdf

Aufgerufen am 27.01.2023

Data Item	Type	Description
Name*	Field	The name of the technique.
ID*	Tag	Unique identifier for the technique within the knowledgebase. Format: T####.
Tactic*	Tag	The tactic objectives that the technique can be used to accomplish. Techniques can be used to perform one or multiple tactics.
Data Sources*	Tag	Source of information collected by a sensor or logging system, e.g., packet capture, file monitoring, that can be used to obtain relevant information for identifying the action being performed, sequence of events, or the results of the actions by an adversary, including the state of systems and processes. The data source list can incorporate different variations of how the action could be performed across different assets for a particular technique. This attribute is intended to restrict data source inclusion to a defined list, to allow technique coverage analysis based on unique data sources. (For example, "what techniques can I detect if I have alarm history in place?")
Description*	Field	Information about the technique, what it is, what it is typically used for, how an adversary can take advantage of it, and variations on how it could be used. Include references to authoritative articles describing technical information related to the technique as well as in-the-wild use references as appropriate.
Asset*†	Relationship/Field	Asset to which the technique can be applied, e.g., Data Historian. Each asset is associated with a high-level function and a consistent role with respect to the system in which it is used.
Contributor	Tag	List of non-MITRE contributors (individual and organization) from first to most recent that contributed information on, about, or supporting the development of a technique.

der Bundeswehr Universität München

esri Deutschland

Agenda

- Motivation
- Cyber Threat Intelligence
- Verortung cyber-physischer Objekte
- Verkettung der Informationsmodelle
- Use Case: SIEM Alarmierung

KRITIS…Kritische Infrastrukturen
CTI……Cyber Threat Intelligence
ICS……Industrial Control Systems
SIEM…..Security Information and Event Management

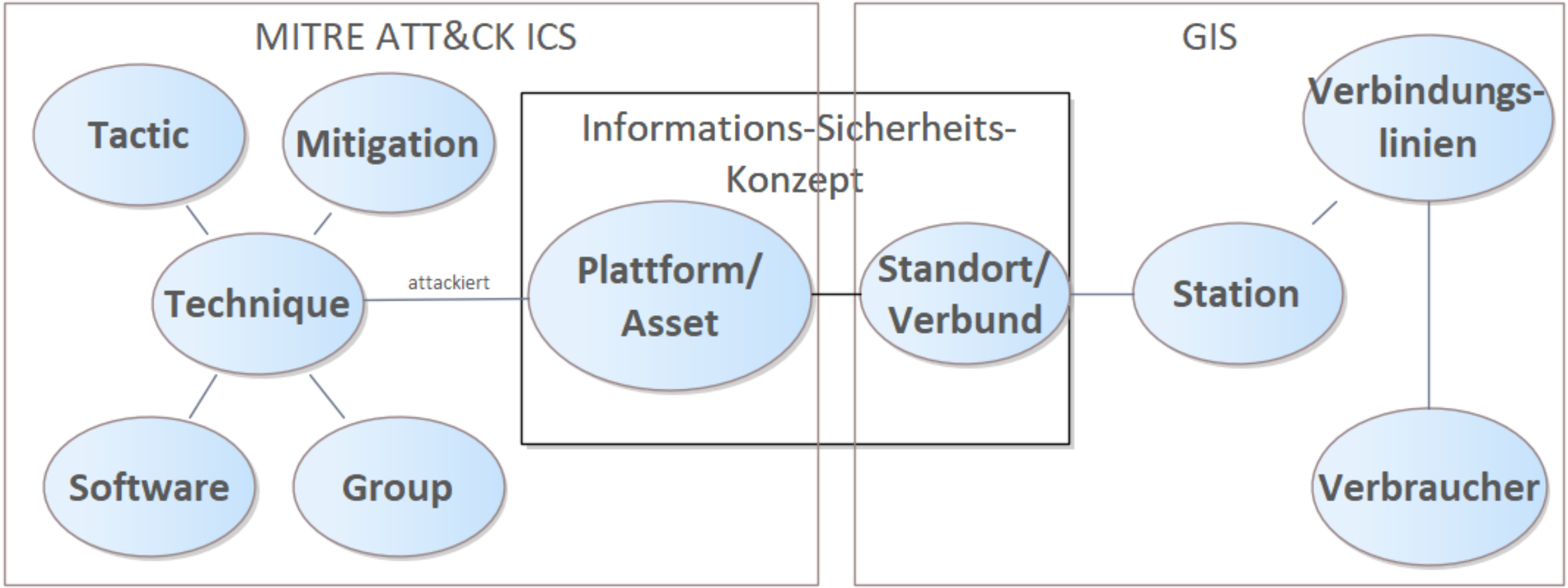
Information Security Management System (ISMS)

Erfassung von Metadaten gem. BSI IT-Grundschutz 200-2 für jedes IT-System und Gerät

- Eindeutige Bezeichnung (beispielsweise der vollständige Hostname oder eine Identifikationsnummer)
- Typ und Funktion (beispielsweise Datenbank-Server für Anwendung X),
- zugrunde liegende Plattform (d. h. Hardware-Plattform und Betriebssystem)
- der Standort (beispielsweise Gebäude- und Raumnummer)
- zuständige Administrator
- vorhandenen Kommunikationsschnittstellen (z. B. Internetanschluss, Bluetooth, WLAN Adapter) sowie
- Art der Netzanbindung und die Netzadresse

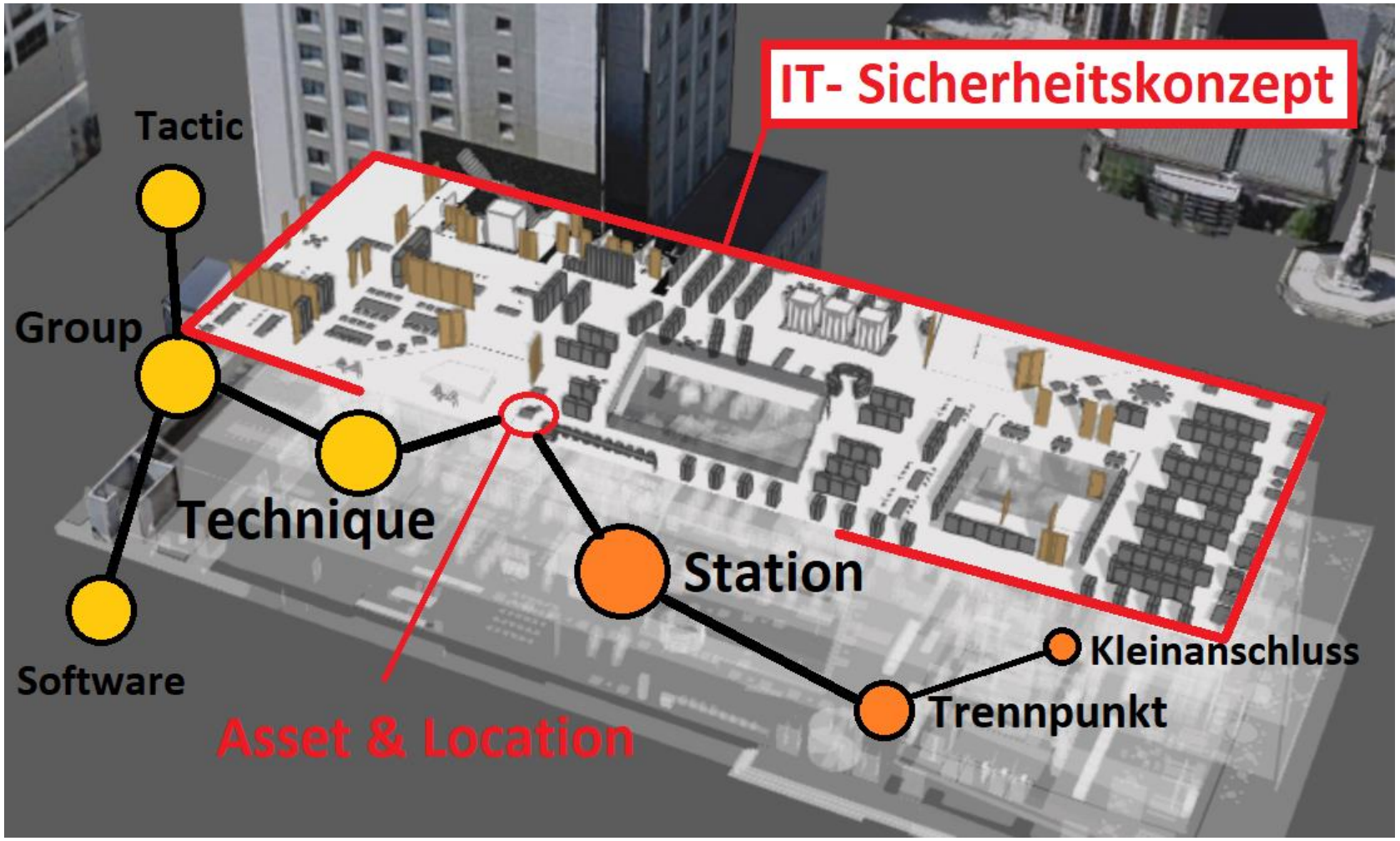
Information Security Management System (ISMS)

Direkte oder mittelbare Zuordnung der Vermögenswerte zu Positionen



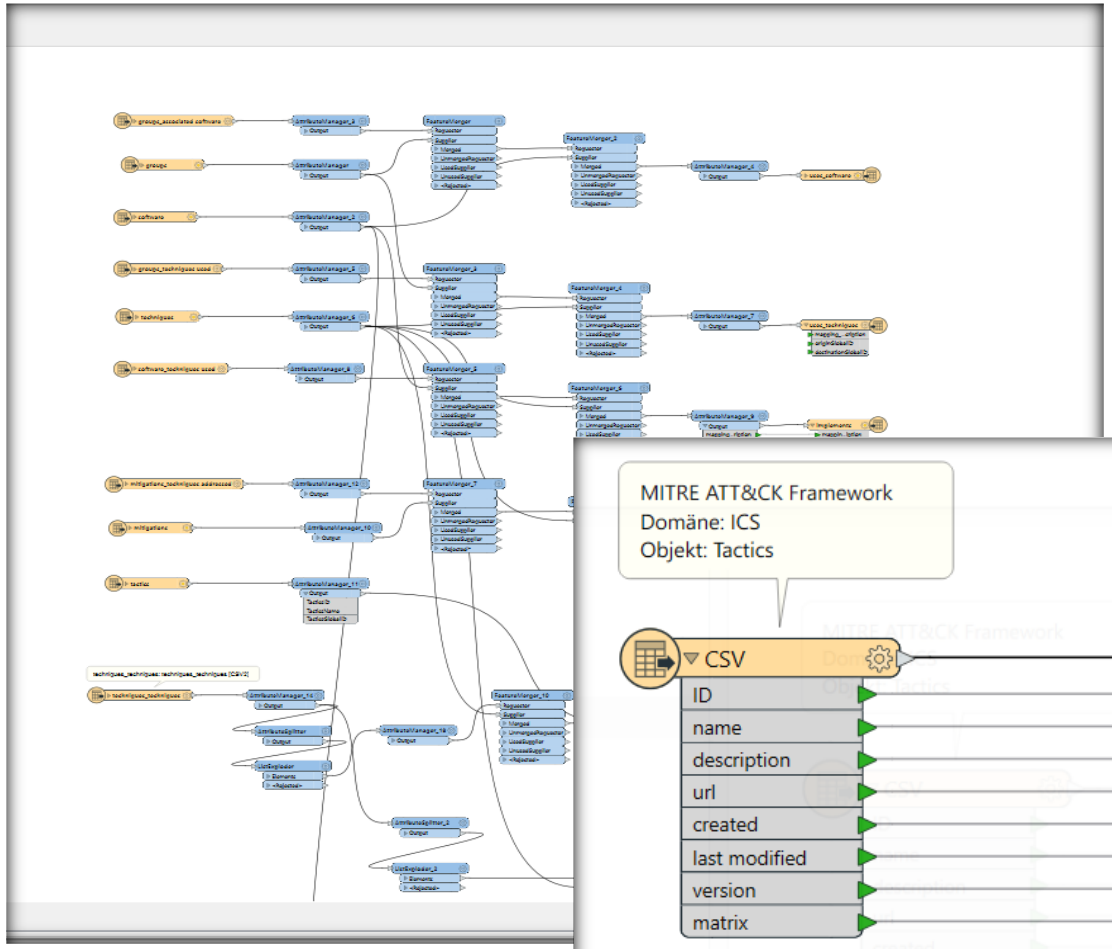
Information Security Management System (ISMS)

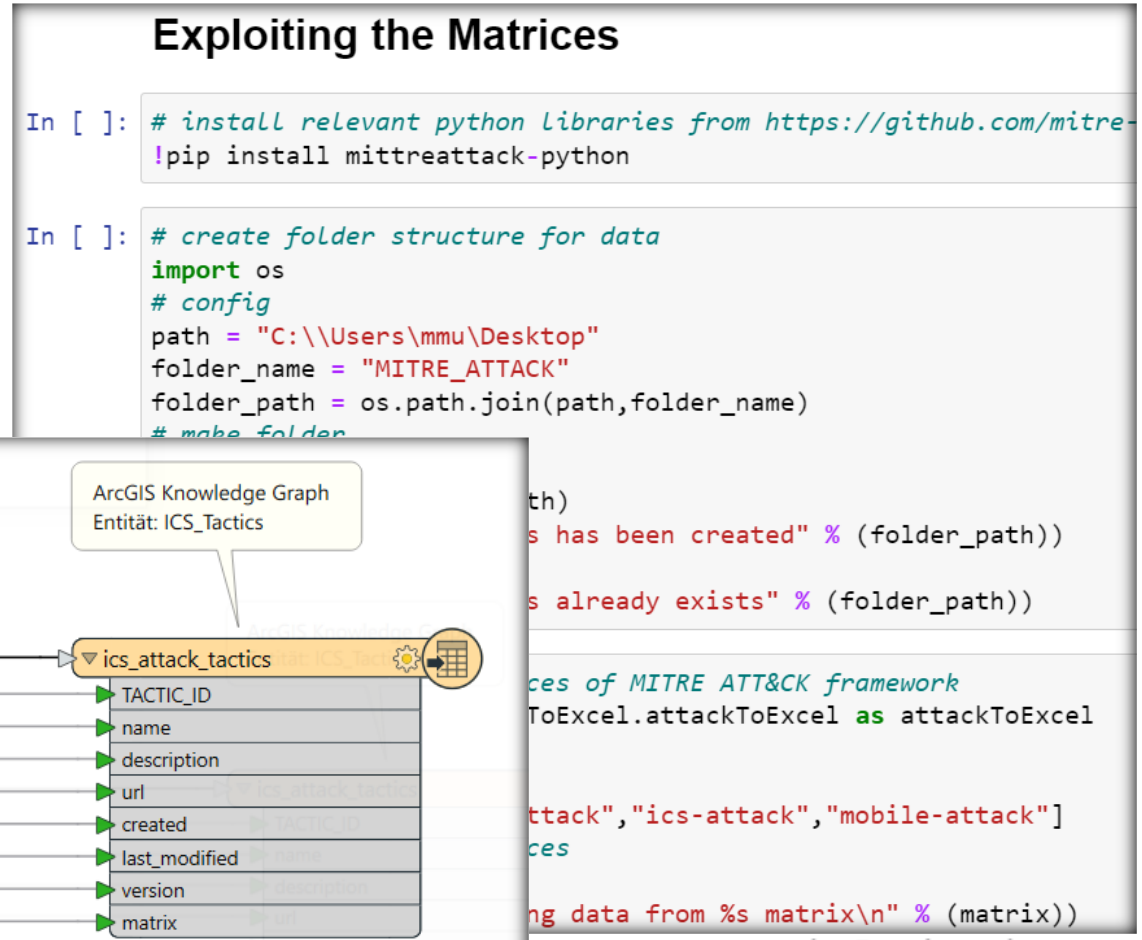
Direkte oder mittelbare Zuordnung der Vermögenswerte zu Positionen

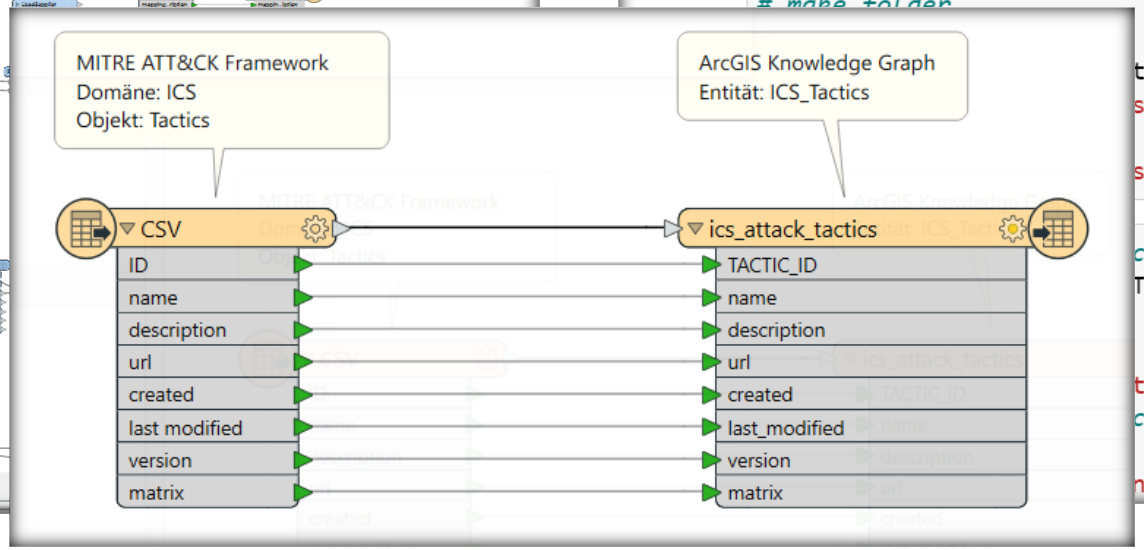


Datenpipeline

Transformation der Objekte in Entitäten und Relationen zueinander

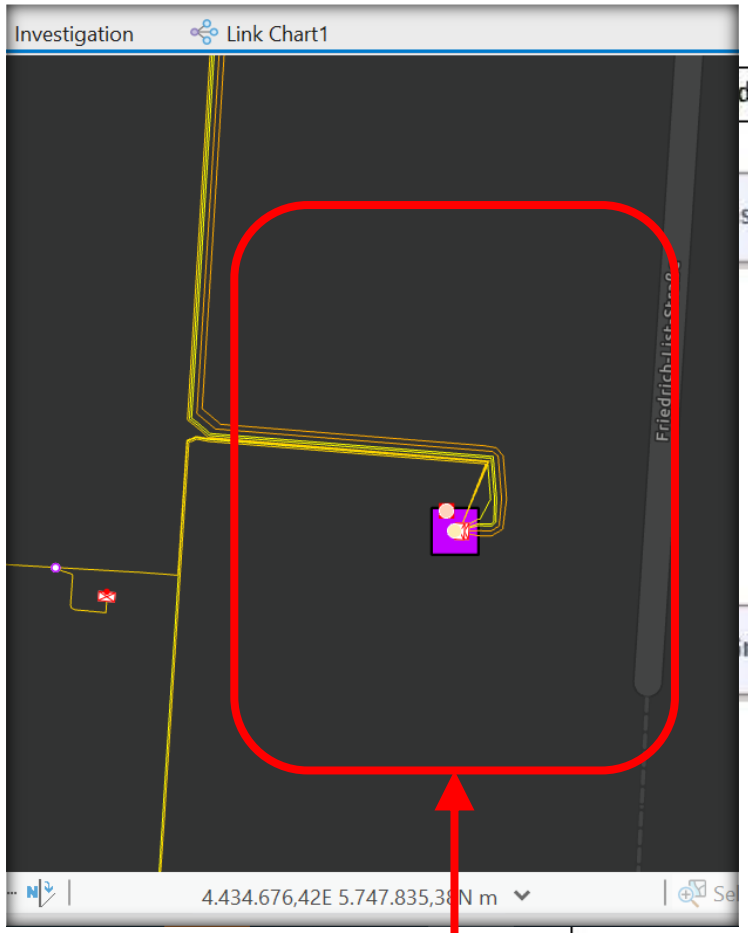


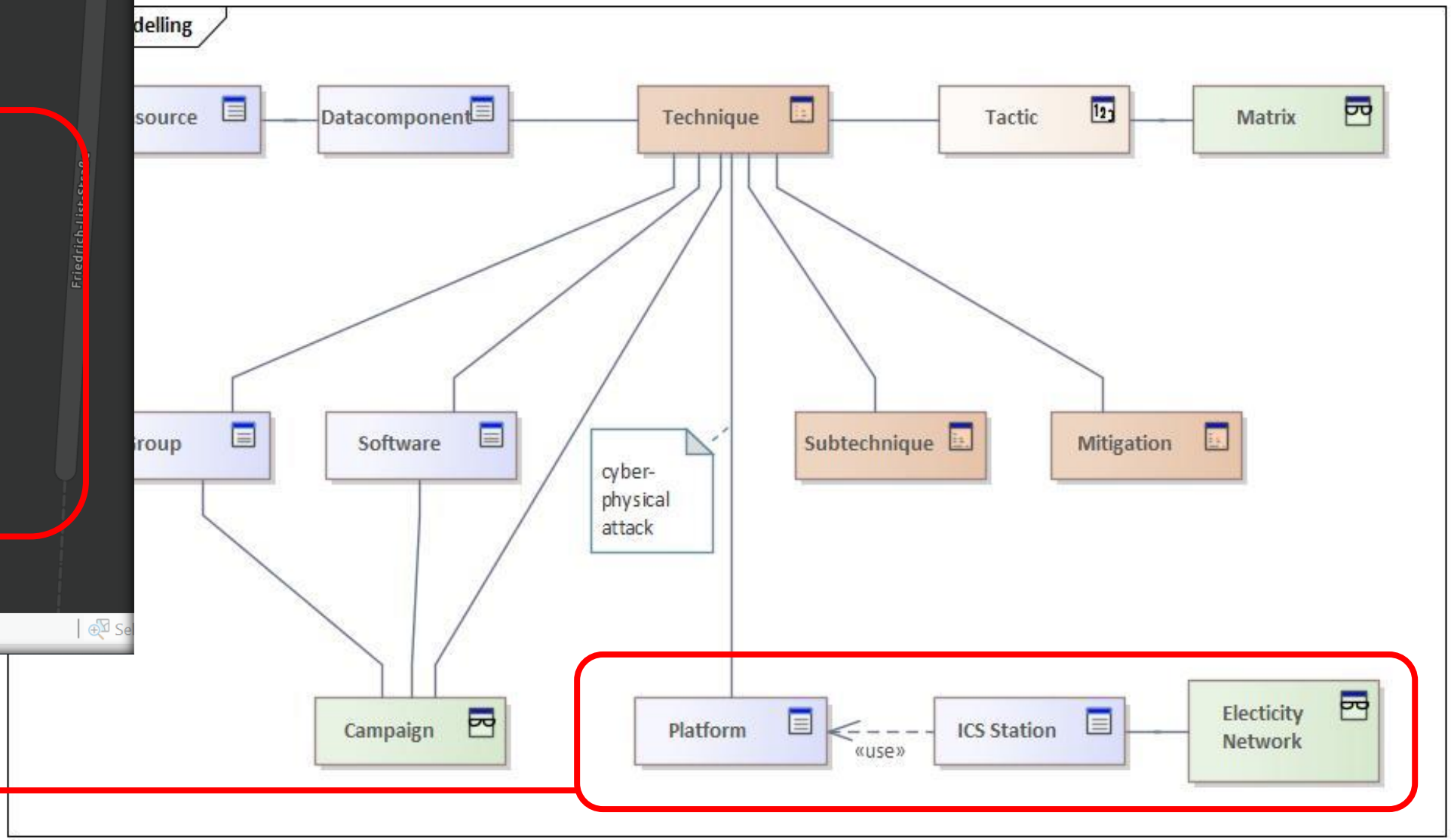




Datenpipeline

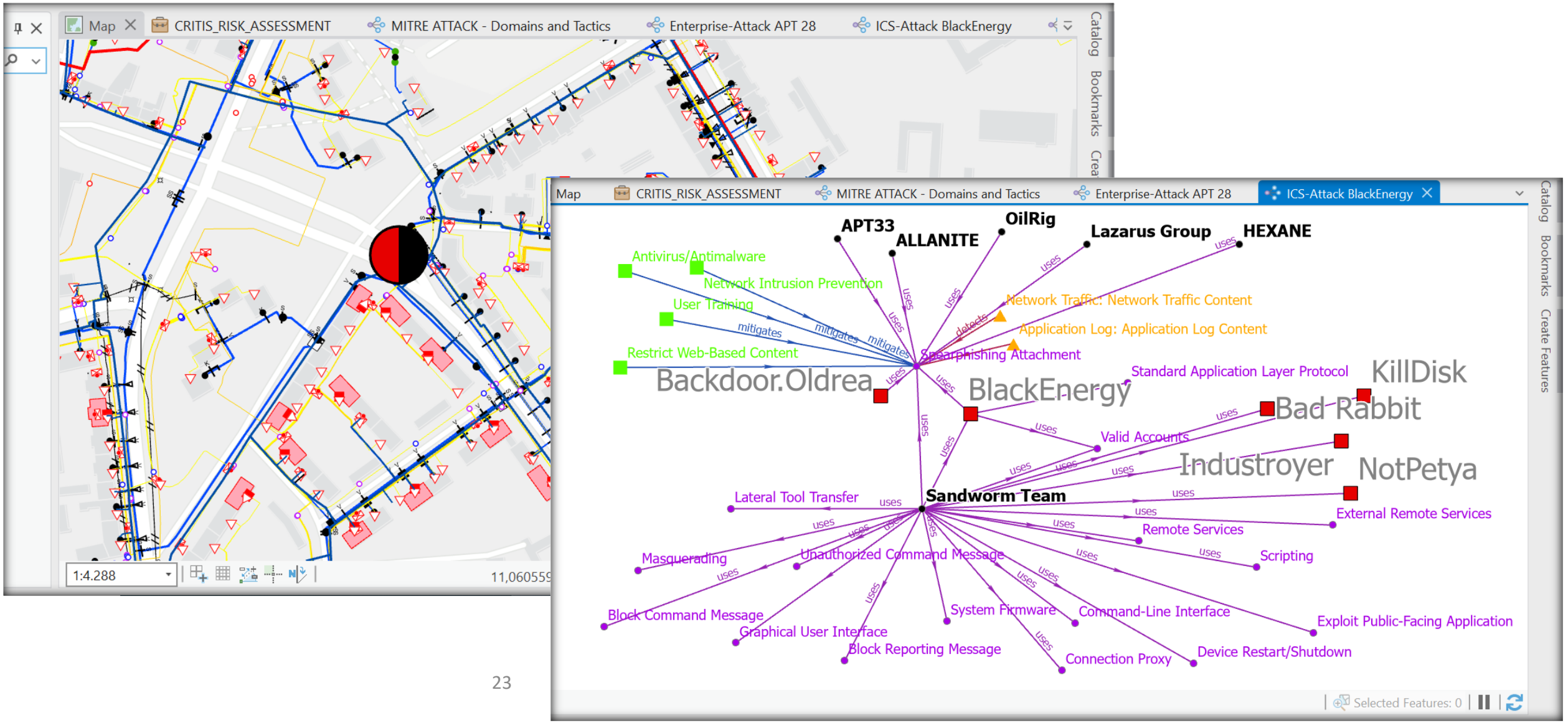
Transformation der Objekte in Entitäten und Relationen zueinander





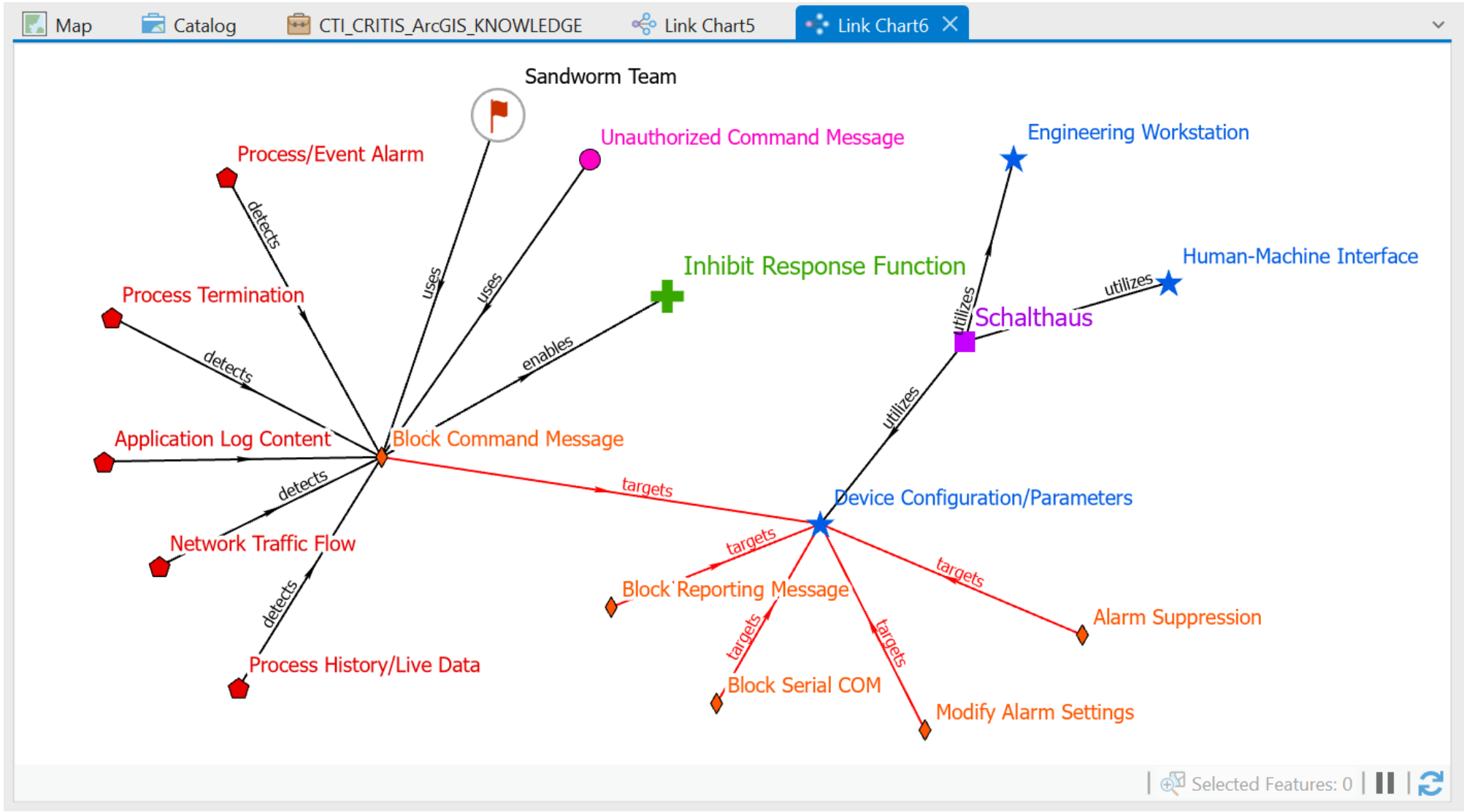
Semantisches Netzwerk (Knowledge Graph)

Logische Verkettung beider Objektmodelle zugunsten einer ganzheitlichen Betrachtung



Semantisches Netzwerk (Knowledge Graph)

Logische Verkettung beider Objektmodelle zugunsten einer ganzheitlichen Betrachtung



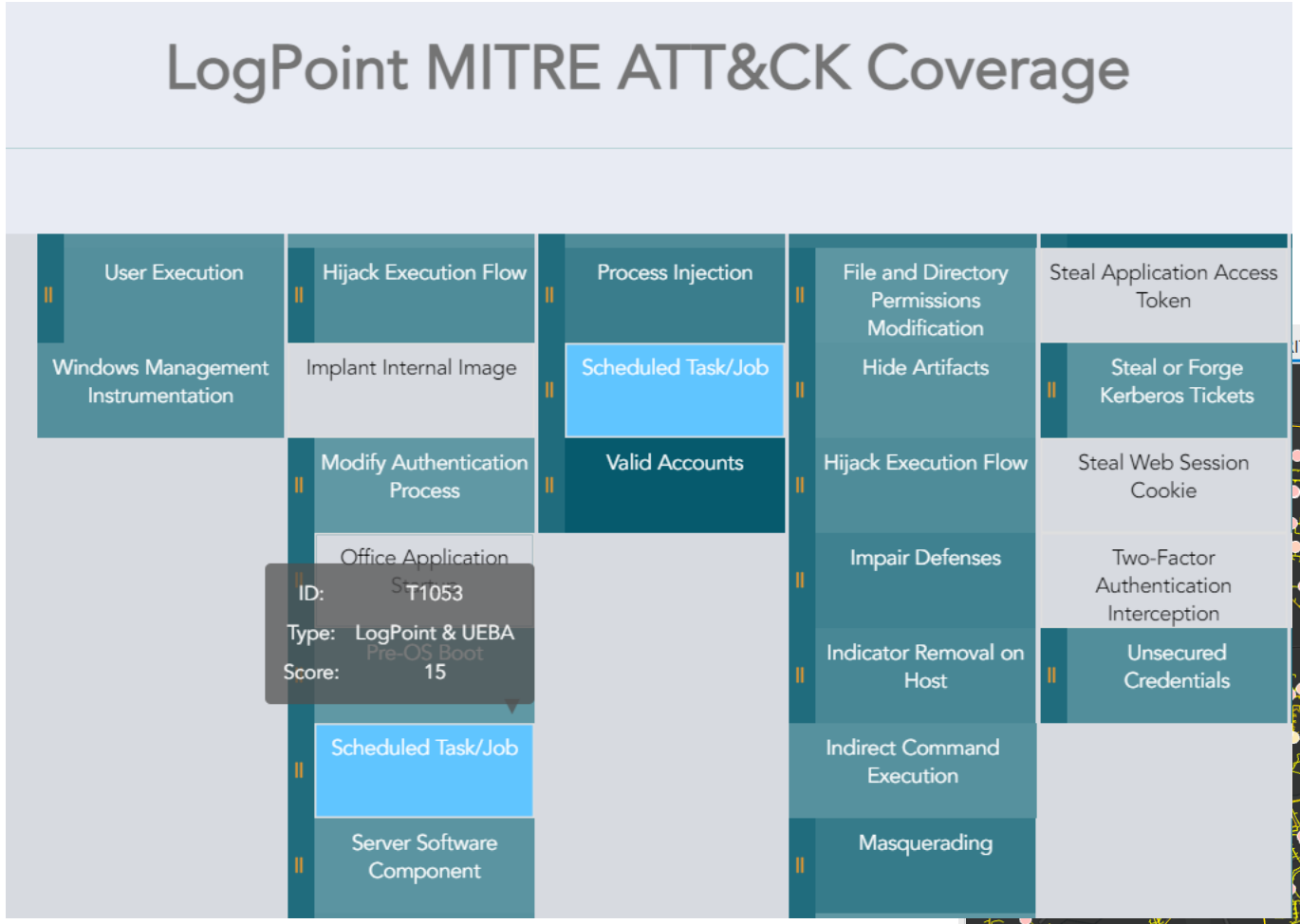
Agenda

- Motivation
- Cyber Threat Intelligence
- Verortung cyber-physischer Objekte
- Verkettung der Informationsmodelle
- Use Case: SIEM Alarmierung

KRITIS…Kritische Infrastrukturen
CTI……Cyber Threat Intelligence
ICS……Industrial Control Systems
SIEM…..Security Information and Event Management

SIEM Lösung: Logpoint

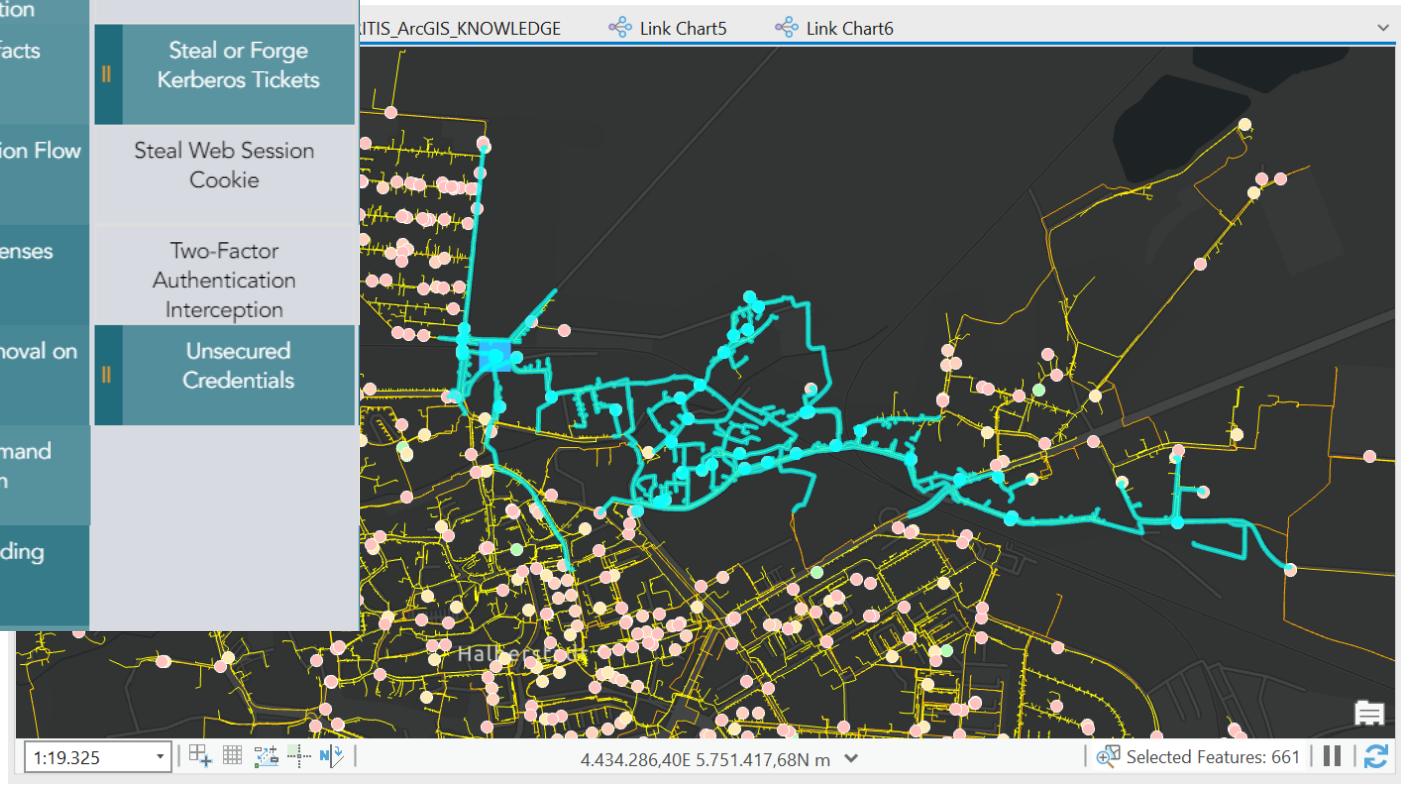
Zuordnung von Ereignissen zu „Techniques“ aus dem MITRE ATT&CK-Framework



Quelle: Internet

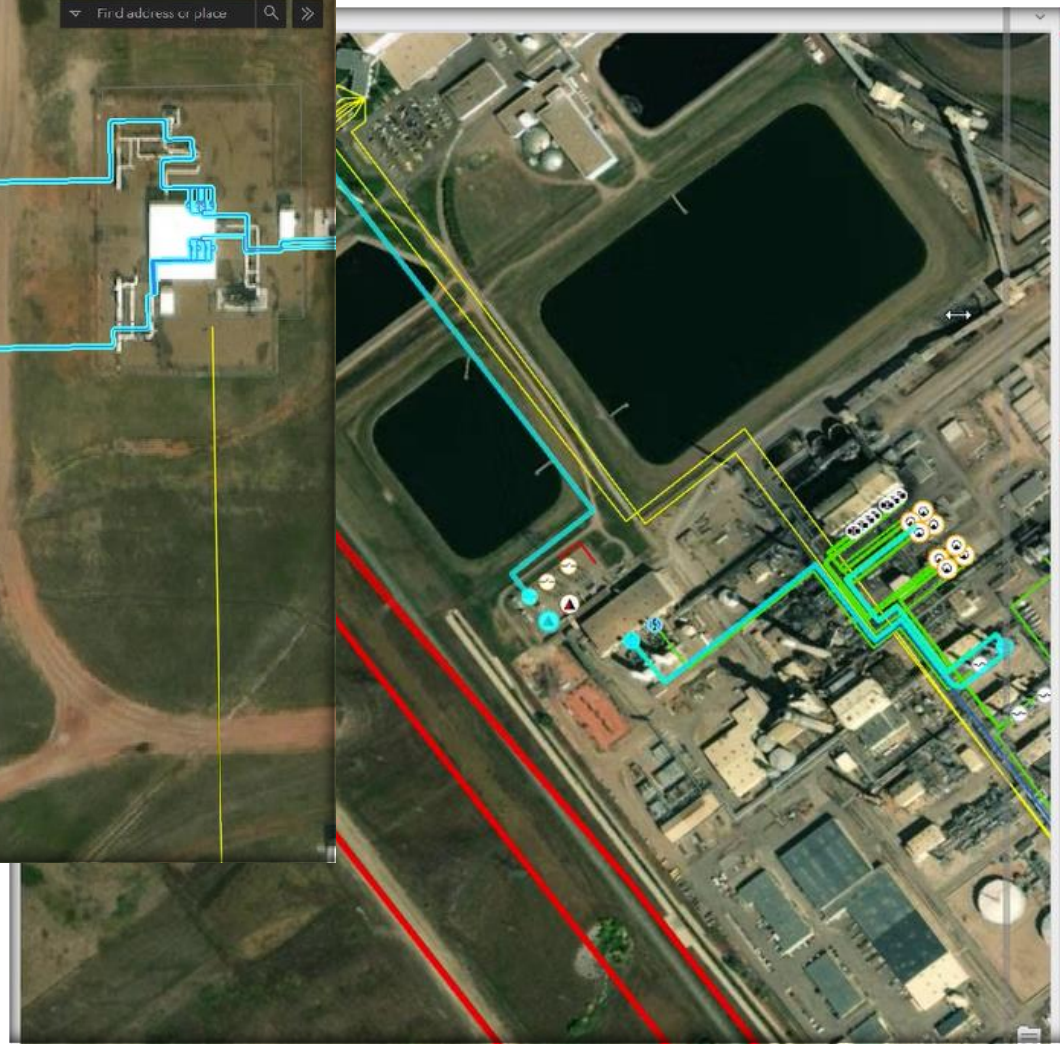
https://docs.logpoint.com/mitre//

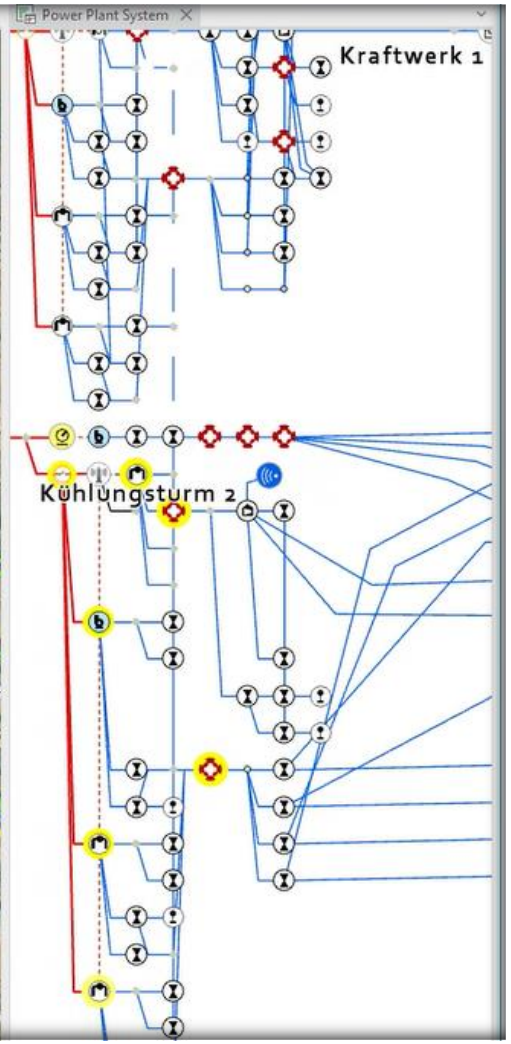
Aufgerufen am 29.01.2023



Quantitative Bewertung des Risikos

Abbildung inhärenter, operativer Zusammenhänge KRITIS

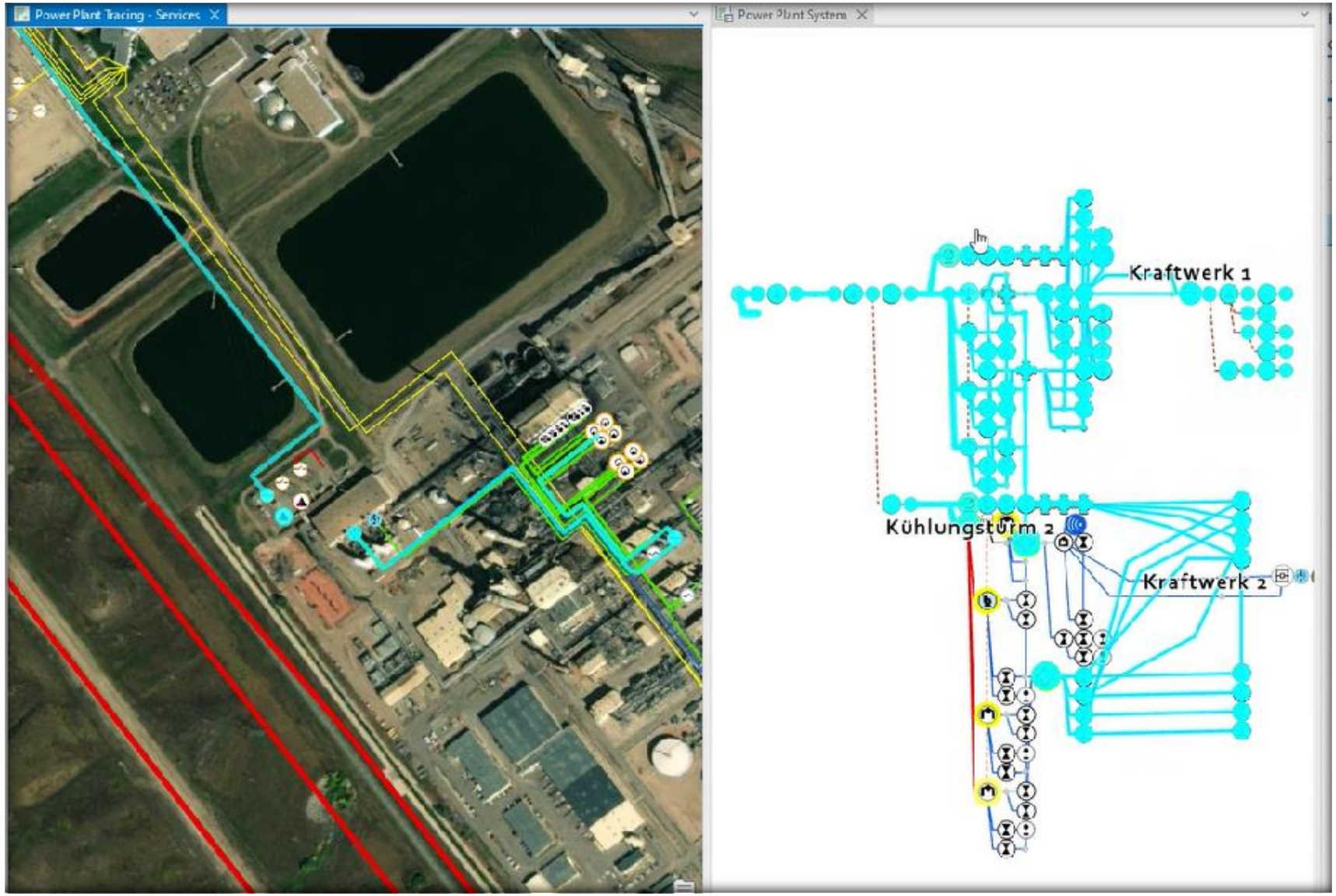




esri Deutschland

Quantitative Bewertung des Risikos

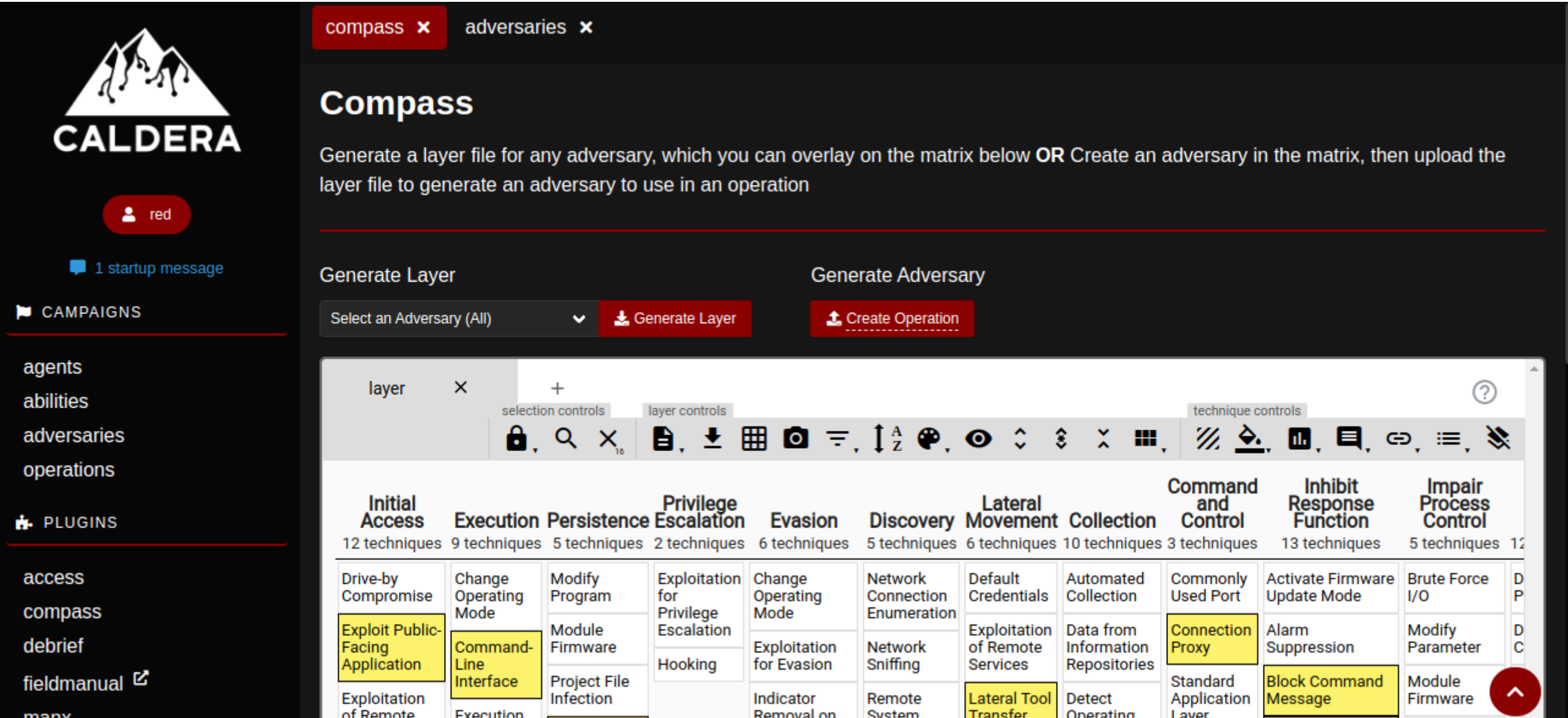
Berücksichtigung vorhandener Resilienz-Mechanismen



MITRE Caldera Framework

Automatisierte Emulation gegnerischer Aktivitäten

DFN CERT®



Microsoft Azure Threat Analytics

Gezielte Simulation bekannter Bedrohungen

Threat analytics

Ransomware	Phishing	Vulnerability	Activity group
59	22	68	72

Email notification settings Help resources

Latest threats

Tool profile: Purple Fox exploit kit	0/0
Attacker technique profile: Abuse of remote monitoring and management tools	0/0
Threat Insights: OAuth consent phishing trust abuse	0/0
SystemBC tool used in human-operated ransomware intrusions	0/0

No alerts Resolved alerts Active alerts

High-impact threats

Credentials Management API abuse	0/1
2018 Shamoon (DistTrack) wiper attacks	0/0
CVE-2018-8653 scripting engine vulnerability	0/0
Living-off-the-la	

No alerts R

Highest exposure threats

SystemBC tool used in human-operated ransomware intrusions	27 - Low
DEV-0300 ransomware activity	27 - Low
DEV-0846 offers "Royal" successor to Conti ransomware	27 - Low

Search

Threat	Ale
Tool profile: Purple Fox exploit kit	0 a
Attacker technique profile: Abuse of remote monitoring and management tools	0 a
Threat Insights: OAuth consent phishing trust abuse	0 a
SystemBC tool used in human-operated ransomware intrusions	0 a

Your evaluation lab

Manage your test devices, attack simulations and reports. Learn and experience the Microsoft Defender for Endpoint capabilities through a guided walkthrough in the trial environment. See it in action as it prevents, detects, and remediates the most sophisticated attacks.

Overview Devices User Actions Simulations Report

Device allocation

0 active devices

Only 16 test devices are provided. Once provisioned, it is only available for 12 hours. Depending on your monthly allotted resource consumption, you may be able to request for more devices.

Add device

Simulations overview

Add simulations

Create simulation

Go to simulations gallery

Report overview

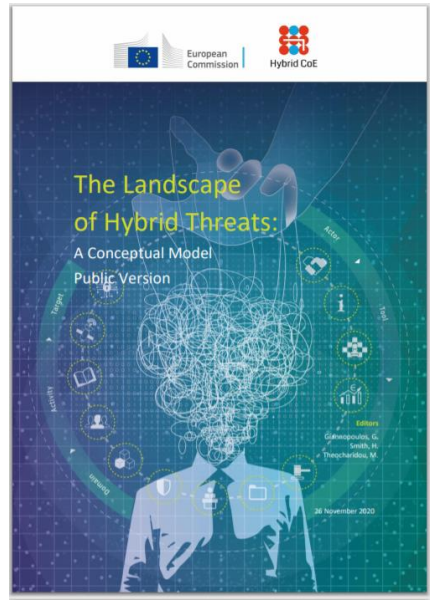
0 Alerts in
0 Incidents
0 Actions taken in
0 Investigations
0 Key findings

View full report

Kernaussagen

- Das MITRE ATT&CK hat sich zum best-practice Ansatz entwickelt
- GIS wird zur Betriebsunterstützung von KRITIS verwendet
- Sicherheitslösungen implementieren ATT&CK
- Geschickte Kombination optmiert die Bewertung von APT-Risiken
- Der gezeigte Lösungsansatz hilft, den Schutz kritischer Infrastrukturen und ihrer unterstützenden IT-Services proaktiver zu gestalten

Zukünftige Ansätze gegen hybride Bedrohungen



EU-HYBNET's Ansatz

Quelle: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305

Vielen Dank für Ihre Aufmerksamkeit

Fragen?

Glossar

- APT Advanced Persistent Threat
- ATT&CK Adversarial Tactics, Techniques and Common Knowledge
- KRITIS Kritische Infrastrukturen
- CTI Cyber Threat Intelligence
- DMZ Demilitarisierte Zone
- GIS Geografisches Informationssystem
- ICS Industry Control Systems
- ISMS Informations-Sicherheits-Management-System
- ISAC Information Sharing and Analysis Center
- SIEM Security Information and Event Management