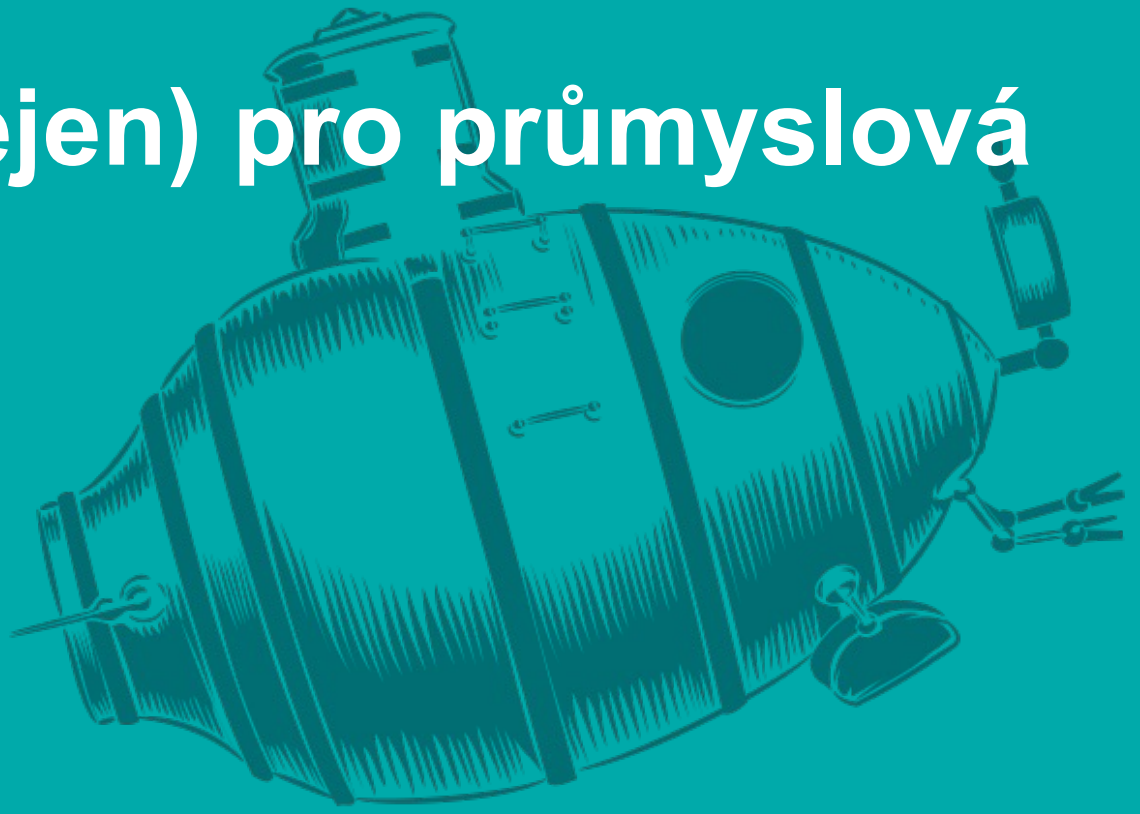
ALEF

Modelování hrozeb (nejen) pro průmyslová prostředí



Jan Kopřiva

jan.kopriva@alef.com @jk0pr

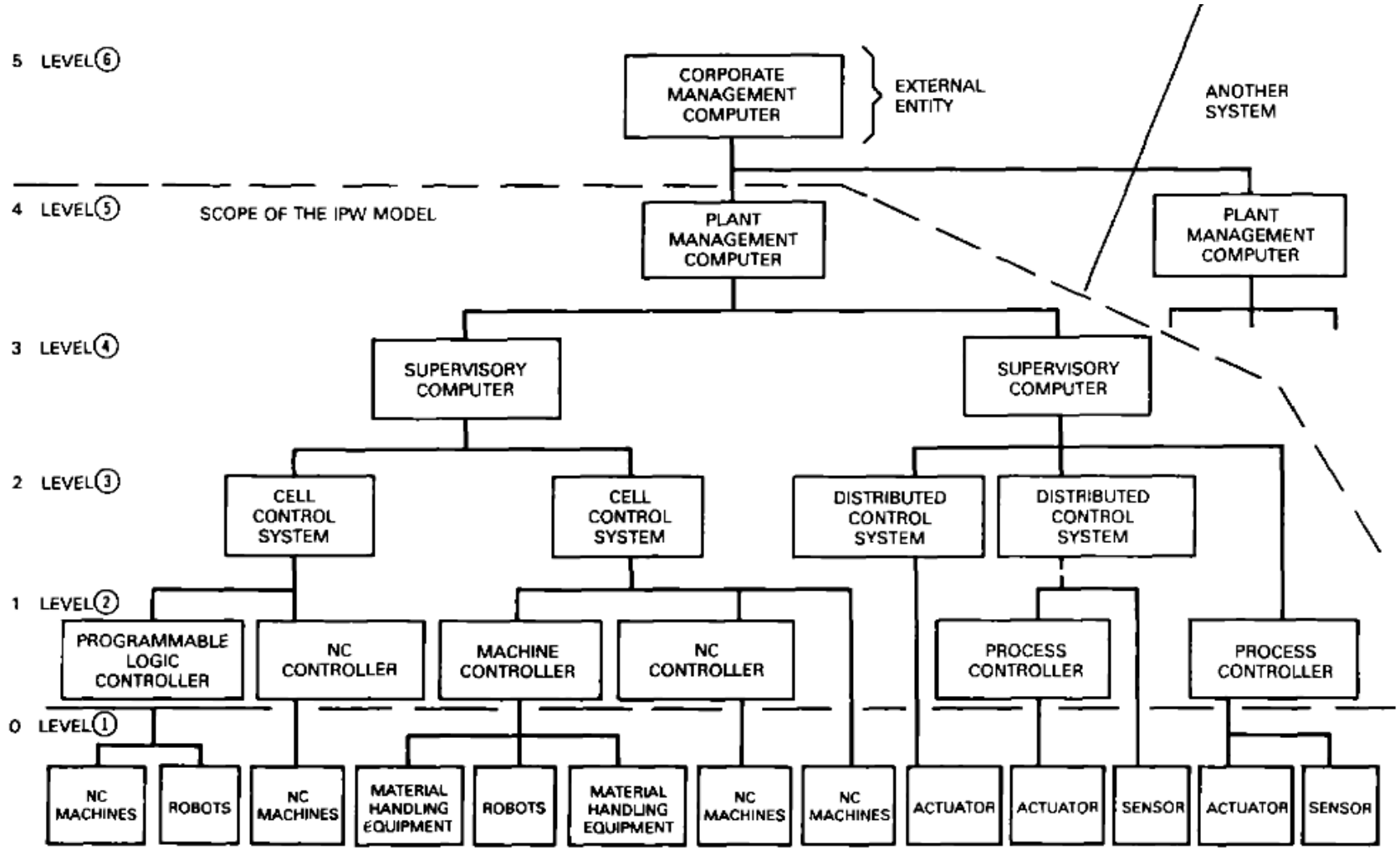
Když se řekne průmyslový a specifický systém

- ICS, IACS, SCADA, IIoT, HIoT, …
- Historické sítě a systémy
  - Velmi dlouhý životní cyklus
  - Často proprietární, uzavřená řešení
- Moderní systémy blízké IT, historické spíše tradiční automatizační a zabezpečovací technice – specifické požadavky na bezpečnost
- Nezřídka neformalizovaný přístup k bezpečnosti

Relevantní normativy a standardy

- Standardy se vztahem k vývoji, průmyslu a bezpečnostnímu inženýrství
  - ISO (21827:2008 – SSE-CMM)
  - NIST (SP 800-82, SP 800-160)
- (Nově vznikající) normativy a standardy pro specifické oblasti
  - Silniční doprava, kolejová doprava, IIoT,…
- I po letech stále relevantní
  - ISA/IEC 62443
  - PERA

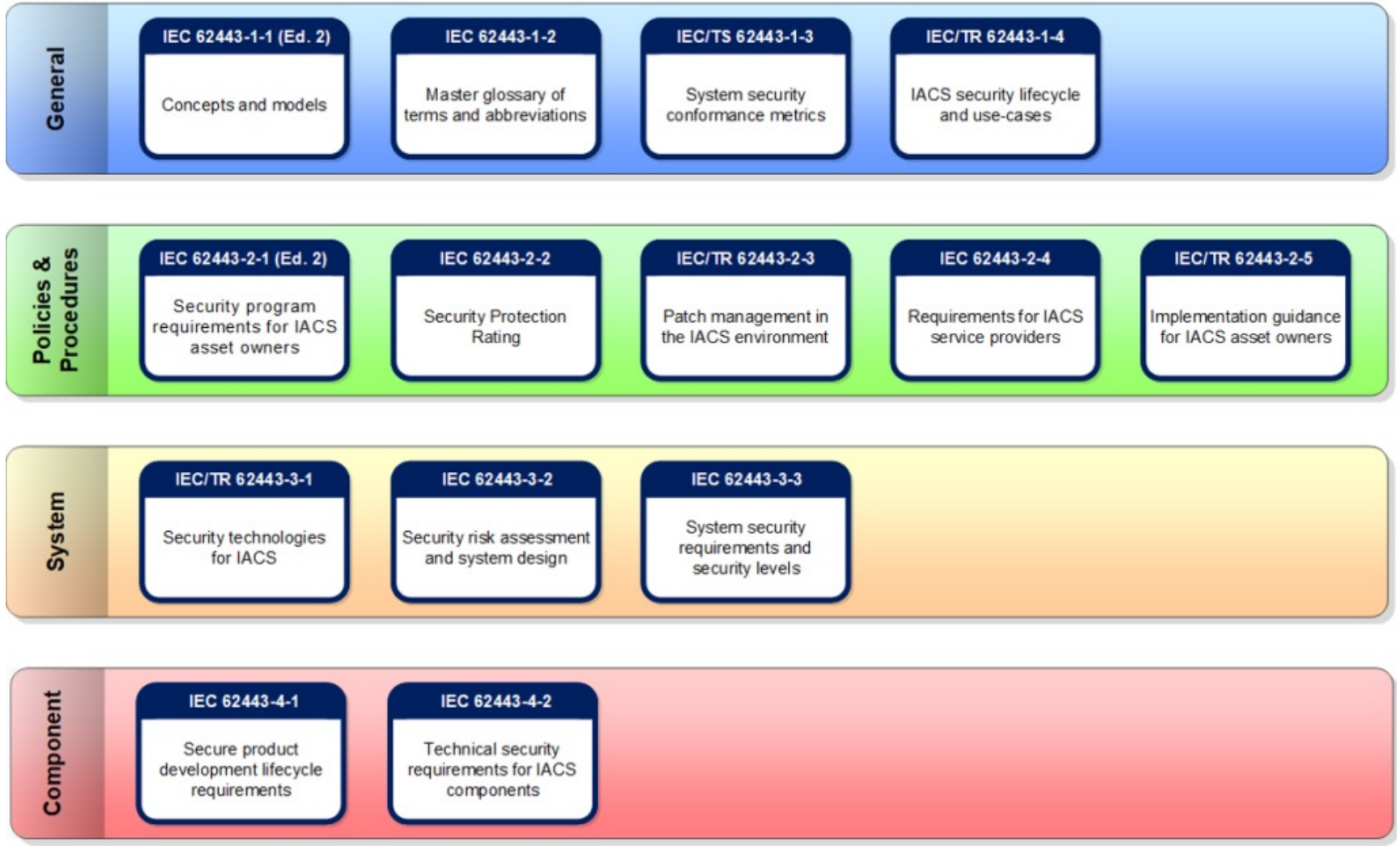
Purdue Enterprise Reference Architecture (PERA)



ALEF

Zdroj: NIST

IEC 62443



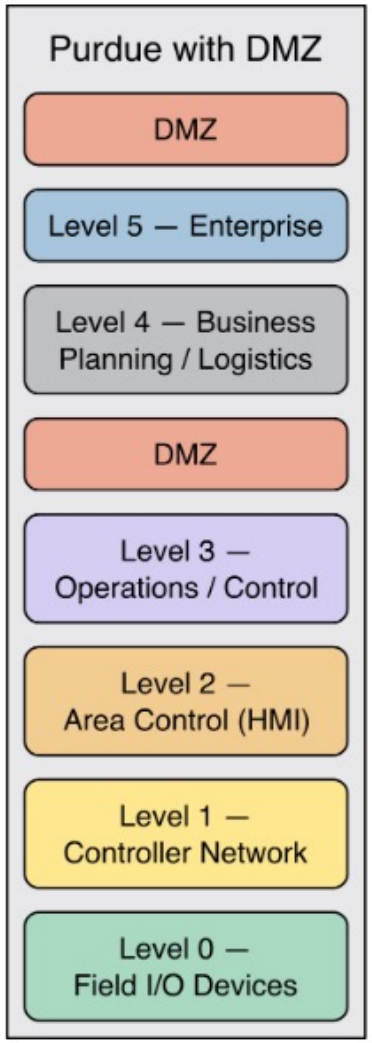
ALEF

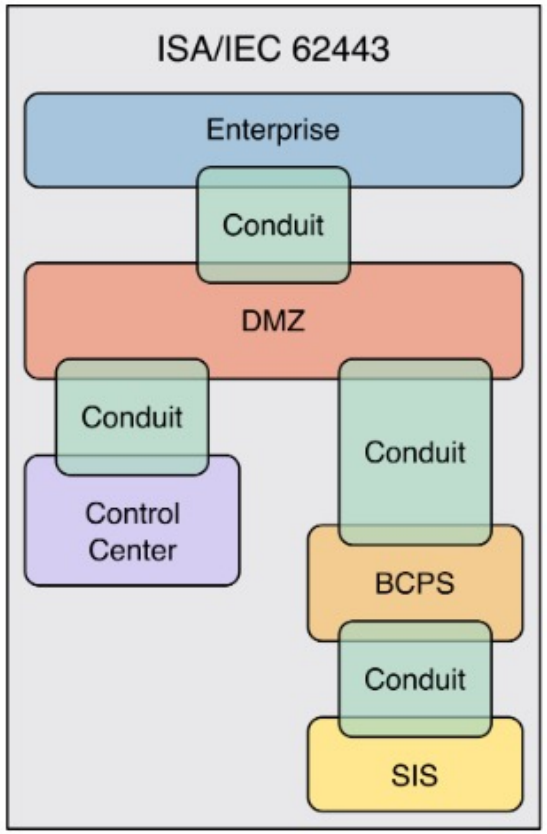
Zdroj: IEC

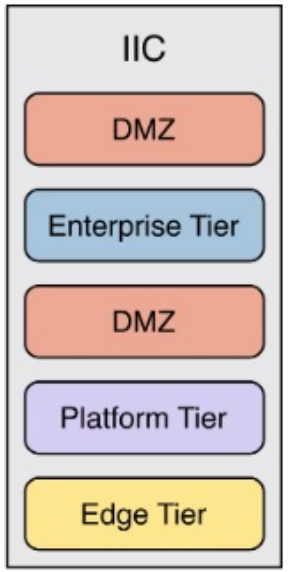
Tradiční přístup

- PERA (levels) i IEC 62443 (zones & conduits) vychází z myšlenky logického či fyzického oddělení průmyslových systémů a sítí od zbytku světa a rigidního řízení přístupů k nim
- V současnosti zpravidla stále optimální, ne vždy však dosažitelné/možné (logování, IIoT, HIoT, vozidla,…)
- Obvyklým obecným řešením přístup přes vhodnou architekturu a řízení rizik

Architektura na úrovni sítě







ALEF

Zdroj: NIST

Rizika v průmyslových a specifických systémech

- Standardní přístupy k určování rizik plně validní
  - Zejména u „safety“ (resp. RAMS) mnohdy více než u IT
- Naturogenní hrozby zpravidla jednoduché určit
- U antropogenních hrozeb je situace o něco složitější
  - Specifické typy technických aktiv i procesů spojeny se specifickými útočnými postupy a vektory
  - Interakční povrch (attack surface) systémů i prostředí (SoS) ne vždy zjevný

Modelování hrozeb pro průmyslové systémy

- Řízení rizik
  - IEC 62443-3-2 – ZCR 5.1: Identify threats
- Bezpečnostní monitoring
  - IEC 62443 Foundational Requirement 6 - Timely response to events

Modelování hrozeb pro průmyslové systémy

- Vývoj systémů
  - IEC 62443-4-1 – SR-2: Threat model
    - Data flows, trust boundaries, processes, data stores, interaction with external entities, communication protocols, externally-accessible physical ports, circuit board connections (e.g., JTAG), attacks on HW, external dependencies, …
    - Explicitně zmíněna metodika STRIDE

Modelování hrozeb pro průmyslové systémy

- Jak smysluplně postupovat
  - Tradiční metodiky pro modelování hrozeb
    - Úzce či naopak velmi široce zaměřené
    - Méně tradiční metodiky?

STRIDE

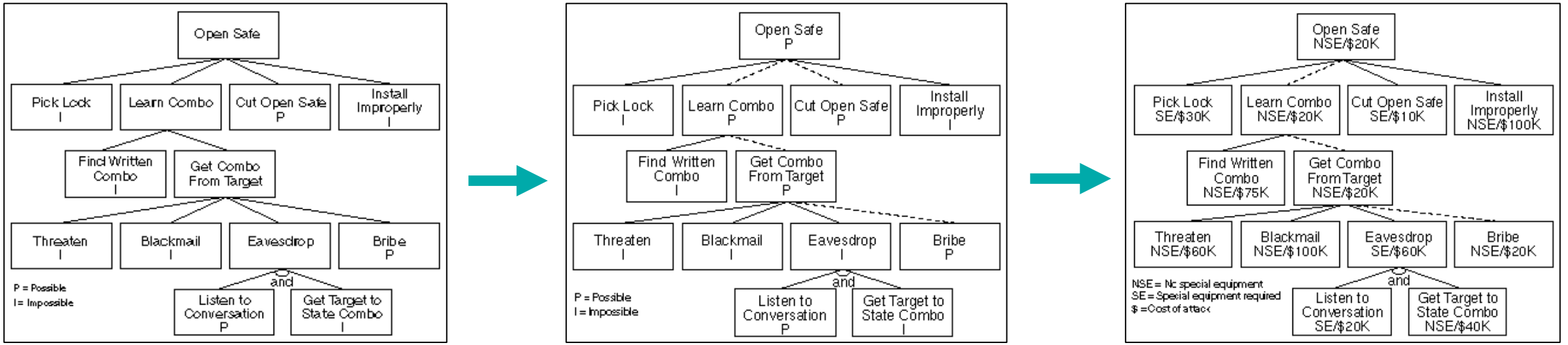
- Metodika pro modelování hrozeb primárně pro SW produkty
- Využitelná potenciálně i v jiných oblastech, kde ale není nezbytně vhodná
- Kategorie hrozeb
  - Spoofing
  - Tampering
  - Repudiation
  - Information dislosure
  - Denial of Service
  - Elevation of privilege

Další relevantní metodiky pro modelování hrozeb

- Tradiční
  - Attack Trees
- Méně tradiční, avšak vysoce efektivní
  - OSSTMM
  - MITRE ATT&CK

Stromy útoků (attack trees)

- Vysoce generická formální metodika pro modelování hrozeb pro libovolný (a tedy i průmyslový/specifický) systém
- Postupné vytváření stromu v němž cíl útoku je kořenem a listy jsou různými způsoby jeho dosažení



ALEF

Zdroj: Bruce Schneier

OSSTMM

- Ve verzi 3 není OSSTMM (jen) metodikou pro bezpečnostní testování
- Velmi dobrá vazba na segmentaci do „zones and conduits“ a identifikaci „logical and physical access points“ dle IEC 62443, stejně tak na „levels“ v PERA
- Nepracuje s rizikem, ale s „porézností“ systému (velikostí interakčního povrchu)

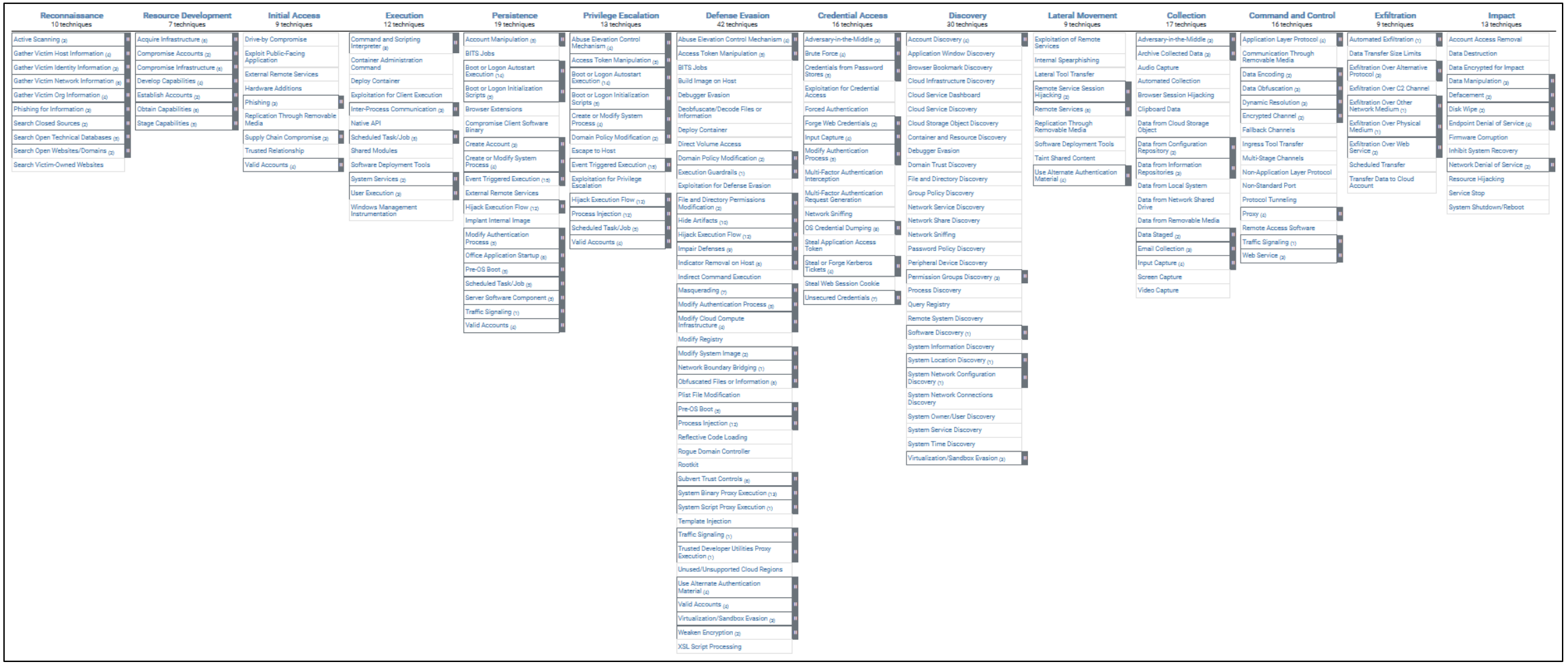
OSSTMM

Category		OpSec	Limitations
Operations		Visibility	Exposure
		Access	Vulnerability
		Trust	
Controls	Class A - Interactive	Authentication	Weakness
		Indemnification	
		Resilience	
		Subjugation	
		Continuity	
	Class B - Process	Non-Repudiation	Concern
		Confidentiality	
		Privacy	
		Integrity	
		Alarm	
			Anomalies

ALEF

Zdroj: OSSTMM

MITRE ATT&CK



ALEF

Zdroj: MITRE

MITRE ATT&CK ICS

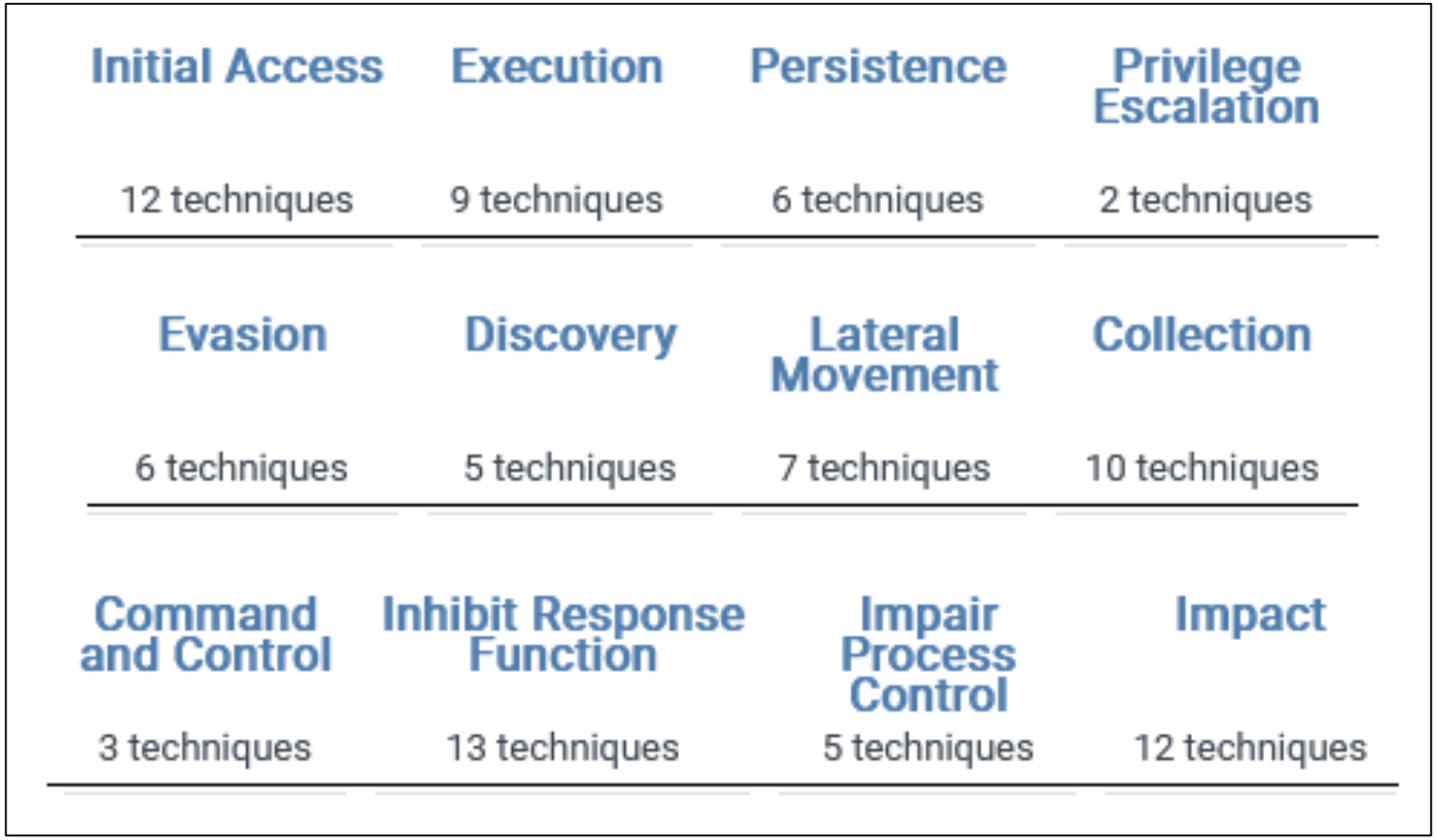
Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	10 techniques	3 techniques	13 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Detect Operating Mode		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	I/O Image		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	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		

Last modified: 06 May 2022

ALEF

Zdroj: MITRE

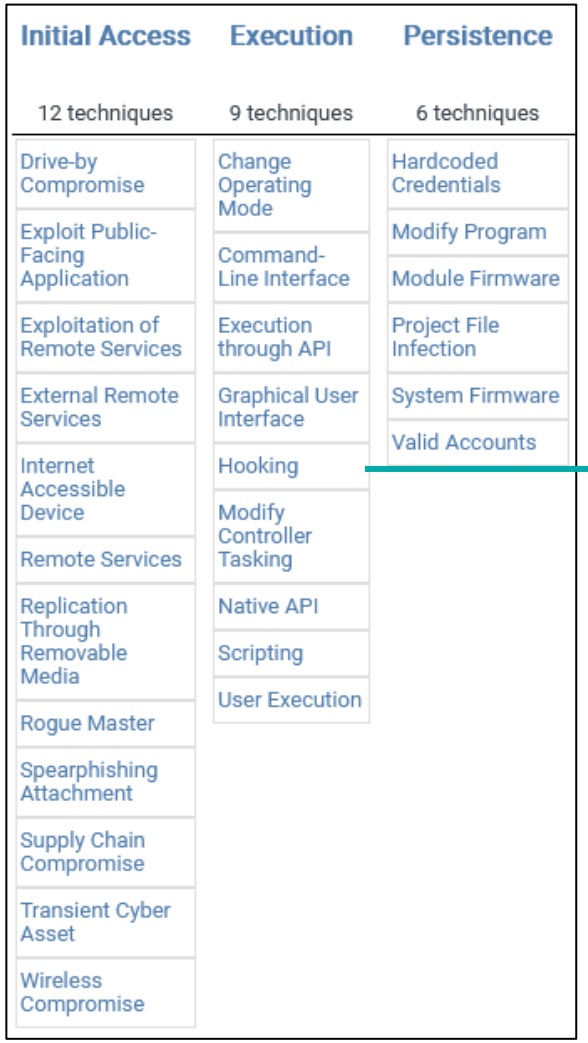
MITRE ATT&CK ICS



ALEF

Zdroj: MITRE

MITRE ATT&CK ICS



Initial Access	Execution	Persistence
12 techniques	9 techniques	6 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials
Exploit Public-Facing Application	Command-Line Interface	Modify Program
Exploitation of Remote Services	Execution through API	Module Firmware
External Remote Services	Graphical User Interface	Project File Infection
Internet Accessible Device	Hooking	System Firmware
Remote Services	Modify Controller Tasking	Valid Accounts
Replication Through Removable Media	Native API	
Rogue Master	Scripting	
Spearphishing Attachment	User Execution	
Supply Chain Compromise		
Transient Cyber Asset		
Wireless Compromise		

Procedure Examples

ID	Name	Description
S0603	Stuxnet	Stuxnet modifies the Import Address Tables DLLs to hook specific APIs that are used to open project files. [2]
S1009	Triton	Triton's injector, inject.bin, changes the function pointer of the 'get main processor diagnostic data' TriStation command to the address of imain.bin so that it is executed prior to the normal handler. [3]

Mitigations

ID	Mitigation	Description
M0947	Audit	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses. Perform periodic integrity checks of the device to validate the correctness of the firmware, software, programs, and configurations. Integrity checks, which typically include cryptographic hashes or digital signatures, should be compared to those obtained at known valid states, especially after events like device reboots, program downloads, or program restarts.
M0944	Restrict Library Loading	Restrict the use of untrusted or unknown libraries, such as remote or unknown DLLs.

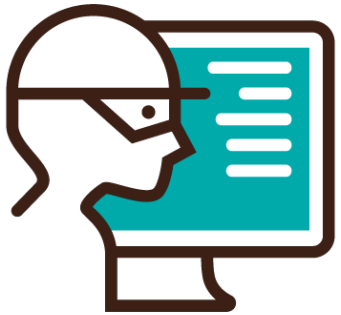
Detection

ID	Data Source	Data Component	Detects
DS0009	Process	OS API Execution	Monitor for API calls that can be used to install a hook procedure, such as the SetWindowsHookEx and SetWinEventHook functions.[4][5] Also consider analyzing hook chains (which hold pointers to hook procedures for each type of hook) using tools[5][6][7] or by programmatically examining internal kernel structures.[8][9]
		Process Metadata	Verify integrity of live processes by comparing code in memory to that of corresponding static binaries, specifically checking for jumps and other instructions that redirect code flow.

ALEF

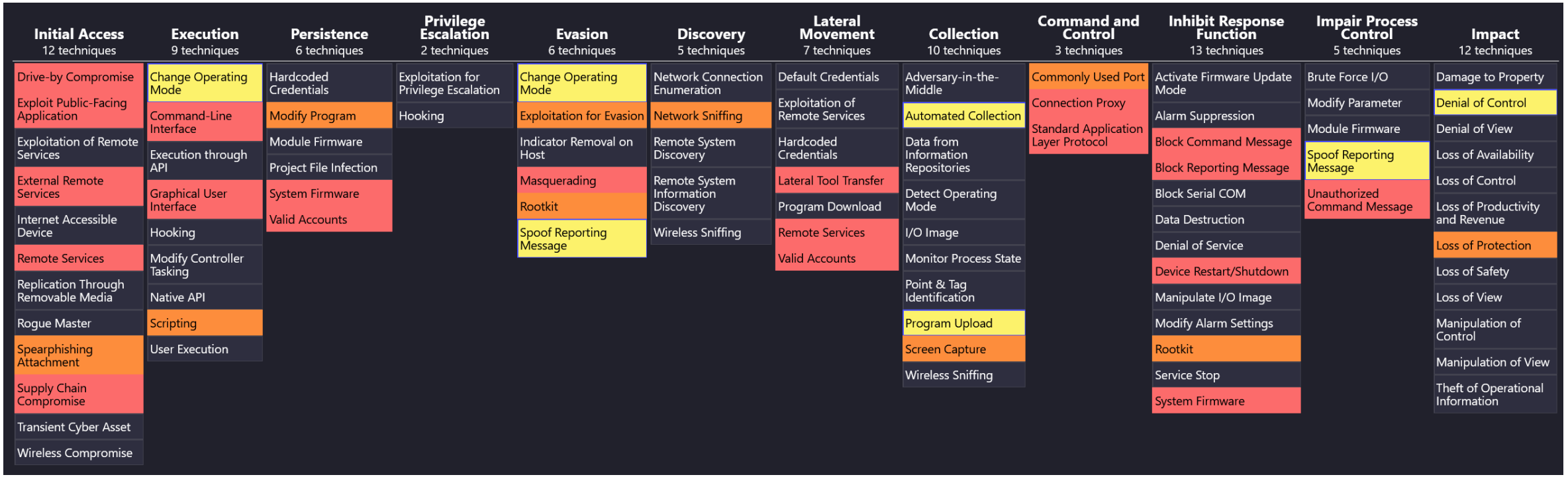
MITRE ATT&CK jako základ pro model hrozeb

- Možnost přímočarého mapování relevantních hrozeb:
  - Jaké skupiny škodlivých aktérů a jaké nástroje jsou pro nás relevantní?
  - S jakými (sub)technikami jsou spojené?
- Nezbytný alespoň elementární CTI program



ALEF

MITRE ATT&CK Navigator – modelování hrozeb



ALEF

Zdroj: MITRE

MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

help changelog theme

Create New Layer — Create a new empty layer

Enterprise | Mobile | ICS

More Options

Open Existing Layer — Load a layer from your computer or a URL

Create Layer from other layers — Choose layers to inherit properties from

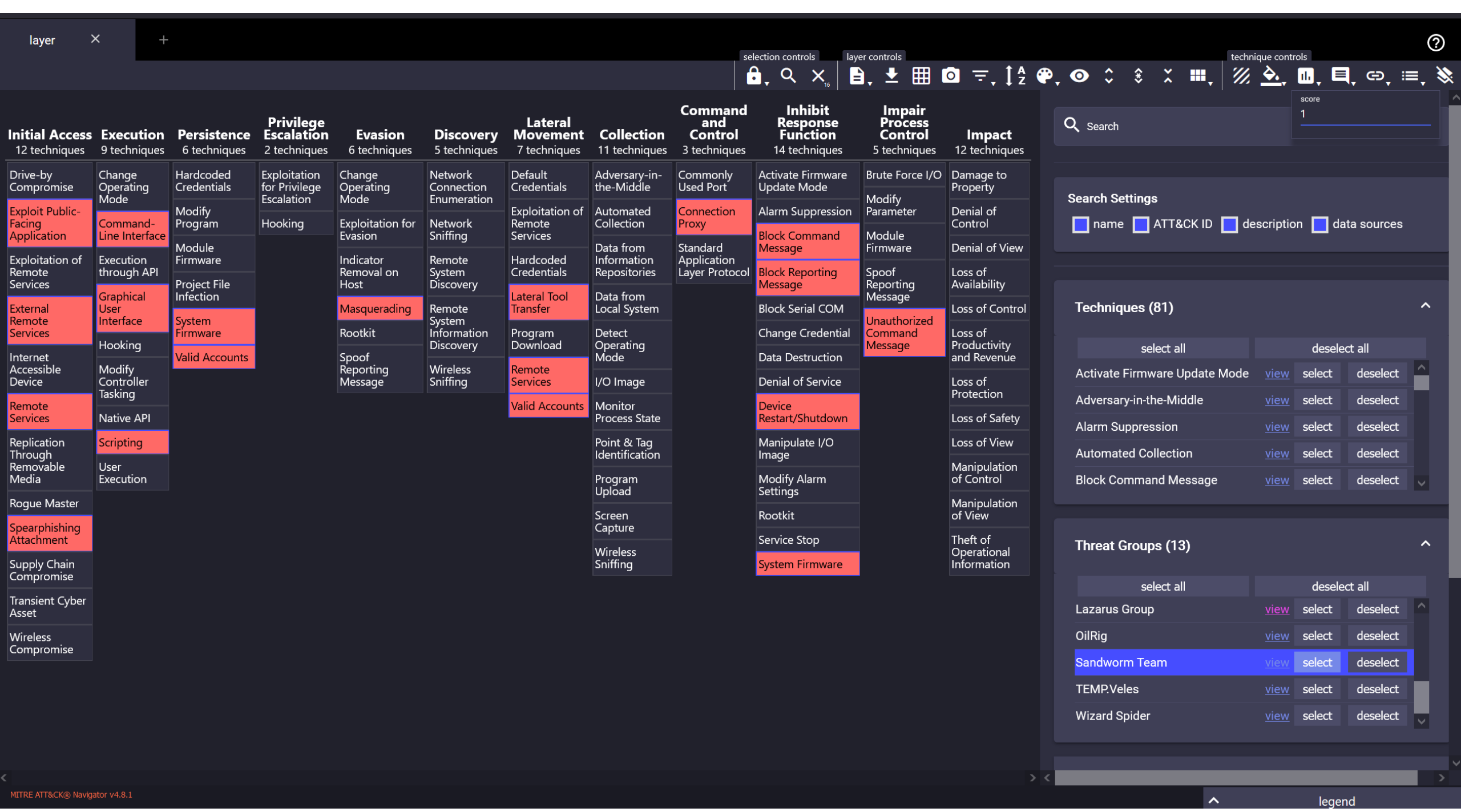
Create Customized Navigator — Create a hyperlink to a customized ATT&CK Navigator

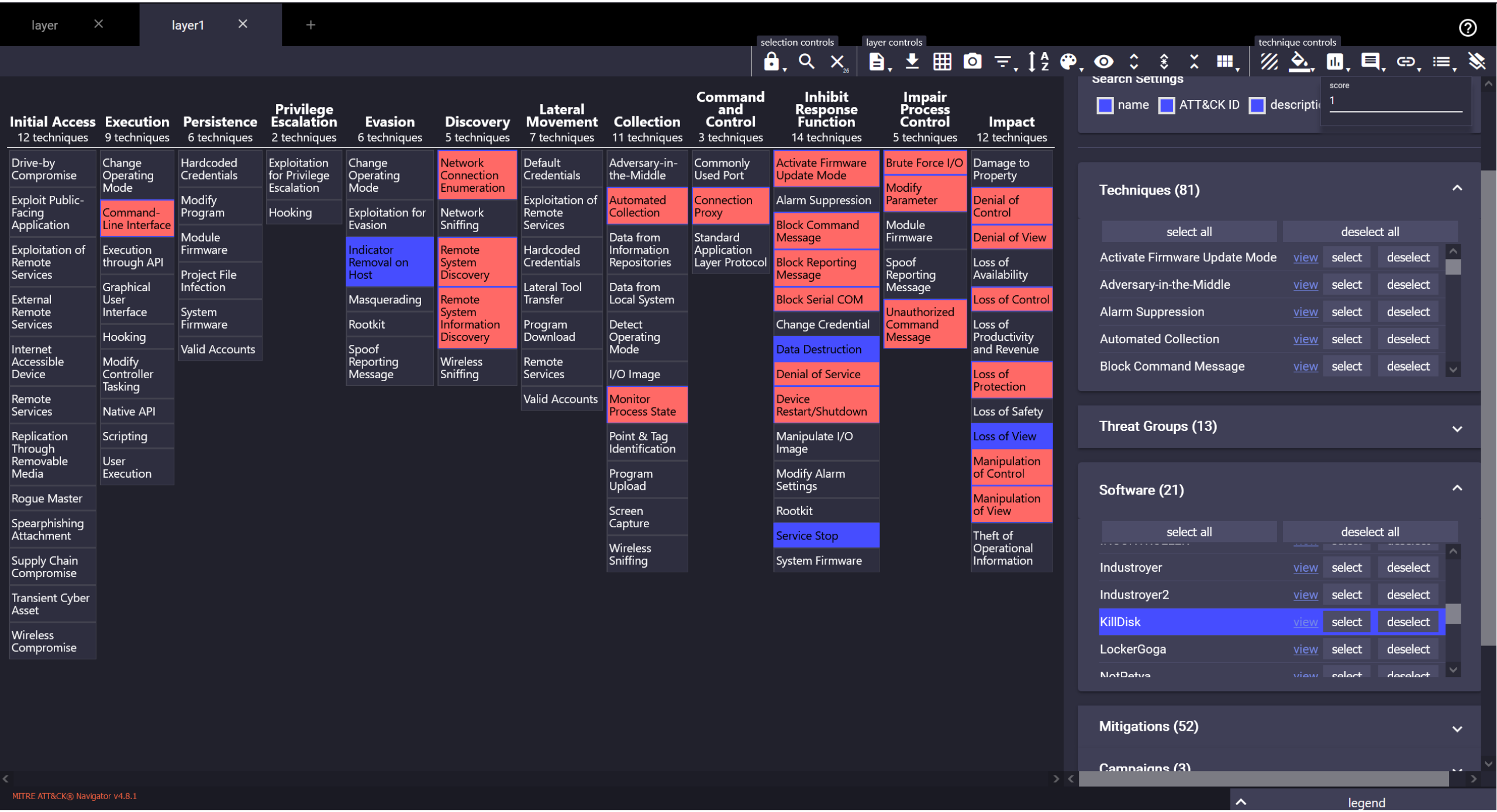
layer

selection controls | layer controls | technique controls

Initial Access 12 techniques	Execution 9 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

legend


layer
selection controls
layer controls
technique controls
score
1
Search
Initial Access
12 techniques
Drive-by Compromise
Exploit Public-Facing Application
Exploitation of Remote Services
External Remote Services
Internet Accessible Device
Remote Services
Replication Through Removable Media
Rogue Master
Spearphishing Attachment
Supply Chain Compromise
Transient Cyber Asset
Wireless Compromise
Execution
9 techniques
Change Operating Mode
Command-Line Interface
Execution through API
Graphical User Interface
Hooking
Modify Controller Tasking
Native API
Scripting
User Execution
Persistence
6 techniques
Hardcoded Credentials
Modify Program
Module Firmware
Project File Infection
System Firmware
Valid Accounts
Privilege Escalation
2 techniques
Exploitation for Privilege Escalation
Hooking
Evasion
6 techniques
Change Operating Mode
Exploitation for Evasion
Indicator Removal on Host
Masquerading
Rootkit
Spoof Reporting Message
Discovery
5 techniques
Network Connection Enumeration
Network Sniffing
Remote System Discovery
Remote System Information Discovery
Wireless Sniffing
Lateral Movement
7 techniques
Default Credentials
Exploitation of Remote Services
Hardcoded Credentials
Lateral Tool Transfer
Program Download
Remote Services
Valid Accounts
Collection
11 techniques
Adversary-in-the-Middle
Automated Collection
Data from Information Repositories
Data from Local System
Detect Operating Mode
I/O Image
Monitor Process State
Point & Tag Identification
Program Upload
Screen Capture
Wireless Sniffing
Command and Control
3 techniques
Commonly Used Port
Connection Proxy
Standard Application Layer Protocol
Inhibit Response Function
14 techniques
Activate Firmware Update Mode
Alarm Suppression
Block Command Message
Block Reporting Message
Block Serial COM
Change Credential
Data Destruction
Denial of Service
Device Restart/Shutdown
Manipulate I/O Image
Modify Alarm Settings
Rootkit
Service Stop
System Firmware
Impair Process Control
5 techniques
Brute Force I/O
Modify Parameter
Module Firmware
Spoof Reporting Message
Unauthorized Command Message
Impact
12 techniques
Damage to Property
Denial of Control
Denial of View
Loss of Availability
Loss of Control
Loss of Productivity and Revenue
Loss of Protection
Loss of Safety
Loss of View
Manipulation of Control
Manipulation of View
Theft of Operational Information
Search Settings
name
ATT&CK ID
description
data sources
Techniques (81)
select all
deselect all
Activate Firmware Update Mode view select deselect
Adversary-in-the-Middle view select deselect
Alarm Suppression view select deselect
Automated Collection view select deselect
Block Command Message view select deselect
Threat Groups (13)
select all
deselect all
Lazarus Group view select deselect
OilRig view select deselect
Sandworm Team view select deselect
TEMP.Veles view select deselect
Wizard Spider view select deselect
MITRE ATT&CK® Navigator v4.8.1
legend


layer
layer1
selection controls
layer controls
technique controls
Initial Access
12 techniques
Drive-by Compromise
Exploit Public-Facing Application
Exploitation of Remote Services
External Remote Services
Internet Accessible Device
Remote Services
Replication Through Removable Media
Rogue Master
Spearphishing Attachment
Supply Chain Compromise
Transient Cyber Asset
Wireless Compromise
Execution
9 techniques
Change Operating Mode
Command-Line Interface
Execution through API
Graphical User Interface
Hooking
Modify Controller Tasking
Native API
Scripting
User Execution
Persistence
6 techniques
Hardcoded Credentials
Modify Program
Module Firmware
Project File Infection
System Firmware
Valid Accounts
Privilege Escalation
2 techniques
Exploitation for Privilege Escalation
Hooking
Evasion
6 techniques
Change Operating Mode
Exploitation for Evasion
Indicator Removal on Host
Masquerading
Rootkit
Spoof Reporting Message
Discovery
5 techniques
Network Connection Enumeration
Network Sniffing
Remote System Discovery
Remote System Information Discovery
Wireless Sniffing
Lateral Movement
7 techniques
Default Credentials
Exploitation of Remote Services
Hardcoded Credentials
Lateral Tool Transfer
Program Download
Remote Services
Valid Accounts
Collection
11 techniques
Adversary-in-the-Middle
Automated Collection
Data from Information Repositories
Data from Local System
Detect Operating Mode
I/O Image
Monitor Process State
Point & Tag Identification
Program Upload
Screen Capture
Wireless Sniffing
Command and Control
3 techniques
Commonly Used Port
Connection Proxy
Standard Application Layer Protocol
Inhibit Response Function
14 techniques
Activate Firmware Update Mode
Alarm Suppression
Block Command Message
Block Reporting Message
Block Serial COM
Change Credential
Data Destruction
Denial of Service
Device Restart/Shutdown
Manipulate I/O Image
Modify Alarm Settings
Rootkit
Service Stop
System Firmware
Impair Process Control
5 techniques
Brute Force I/O
Modify Parameter
Module Firmware
Spoof Reporting Message
Unauthorized Command Message
Impact
12 techniques
Damage to Property
Denial of Control
Denial of View
Loss of Availability
Loss of Control
Loss of Productivity and Revenue
Loss of Protection
Loss of Safety
Loss of View
Manipulation of Control
Manipulation of View
Theft of Operational Information
Search Settings
name
ATT&CK ID
score
1
Techniques (81)
select all
deselect all
Activate Firmware Update Mode view select deselect
Adversary-in-the-Middle view select deselect
Alarm Suppression view select deselect
Automated Collection view select deselect
Block Command Message view select deselect
Threat Groups (13)
Software (21)
select all
deselect all
Industroyer view select deselect
Industroyer2 view select deselect
KillDisk view select deselect
LockerGoga view select deselect
Mitigations (52)
Campaigns (3)
MITRE ATT&CK® Navigator v4.8.1
legend

layer a | layer1 b | new tab | +

MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

help changelog theme ▾

Create New Layer — Create a new empty layer

Open Existing Layer — Load a layer from your computer or a URL

Create Layer from other layers — Choose layers to inherit properties from

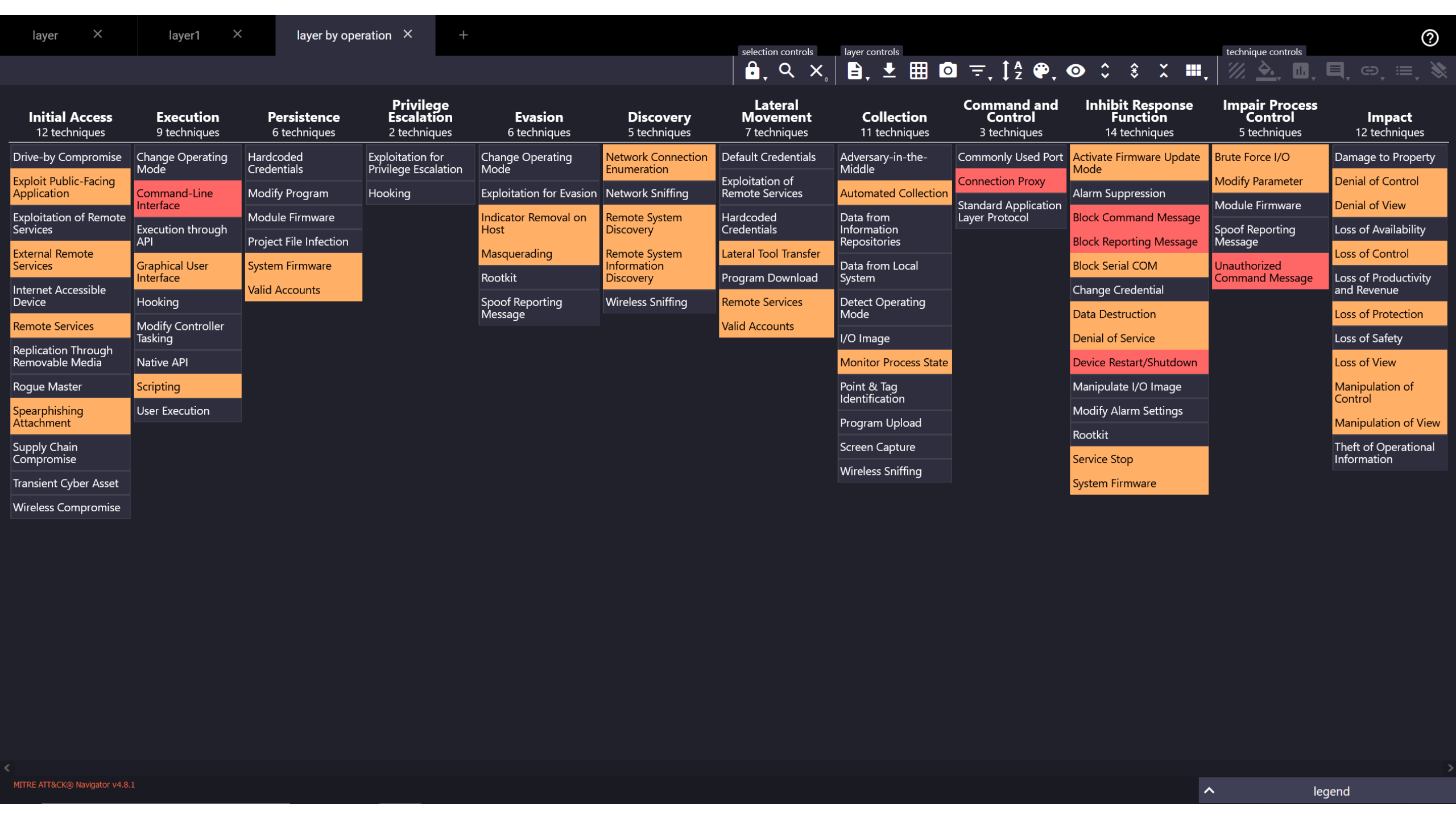
domain *
ICS ATT&CK v13
Choose the domain and version for the new layer. Only layers of the same domain and version can be merged.

score expression
a + b
Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found here. Leave blank to initialize scores to 0. Here's a list of available layer variables:

- a (layer)
- b (layer1)

gradient
Choose which layer to import the scoring gradient from. Leave blank to initialize with the default scoring gradient.

coloring
Choose which layer to import manually assigned colors from. Leave blank to initialize with no colors.


layer
layer1
layer by operation
selection controls
layer controls
technique controls
Initial Access
12 techniques
Drive-by Compromise
Exploit Public-Facing Application
Exploitation of Remote Services
External Remote Services
Internet Accessible Device
Remote Services
Replication Through Removable Media
Rogue Master
Spearphishing Attachment
Supply Chain Compromise
Transient Cyber Asset
Wireless Compromise
Execution
9 techniques
Change Operating Mode
Command-Line Interface
Execution through API
Graphical User Interface
Hooking
Modify Controller Tasking
Native API
Scripting
User Execution
Persistence
6 techniques
Hardcoded Credentials
Modify Program
Module Firmware
Project File Infection
System Firmware
Valid Accounts
Privilege Escalation
2 techniques
Exploitation for Privilege Escalation
Hooking
Evasion
6 techniques
Change Operating Mode
Exploitation for Evasion
Indicator Removal on Host
Masquerading
Rootkit
Spoof Reporting Message
Discovery
5 techniques
Network Connection Enumeration
Network Sniffing
Remote System Discovery
Remote System Information Discovery
Wireless Sniffing
Lateral Movement
7 techniques
Default Credentials
Exploitation of Remote Services
Hardcoded Credentials
Lateral Tool Transfer
Program Download
Remote Services
Valid Accounts
Collection
11 techniques
Adversary-in-the-Middle
Automated Collection
Data from Information Repositories
Data from Local System
Detect Operating Mode
I/O Image
Monitor Process State
Point & Tag Identification
Program Upload
Screen Capture
Wireless Sniffing
Command and Control
3 techniques
Commonly Used Port
Connection Proxy
Standard Application Layer Protocol
Inhibit Response Function
14 techniques
Activate Firmware Update Mode
Alarm Suppression
Block Command Message
Block Reporting Message
Block Serial COM
Change Credential
Data Destruction
Denial of Service
Device Restart/Shutdown
Manipulate I/O Image
Modify Alarm Settings
Rootkit
Service Stop
System Firmware
Impair Process Control
5 techniques
Brute Force I/O
Modify Parameter
Module Firmware
Spoof Reporting Message
Unauthorized Command Message
Impact
12 techniques
Damage to Property
Denial of Control
Denial of View
Loss of Availability
Loss of Control
Loss of Productivity and Revenue
Loss of Protection
Loss of Safety
Loss of View
Manipulation of Control
Manipulation of View
Theft of Operational Information
MITRE ATT&CK® Navigator v4.8.1
legend

MITRE ATT&CK ICS – postup modelování hrozeb

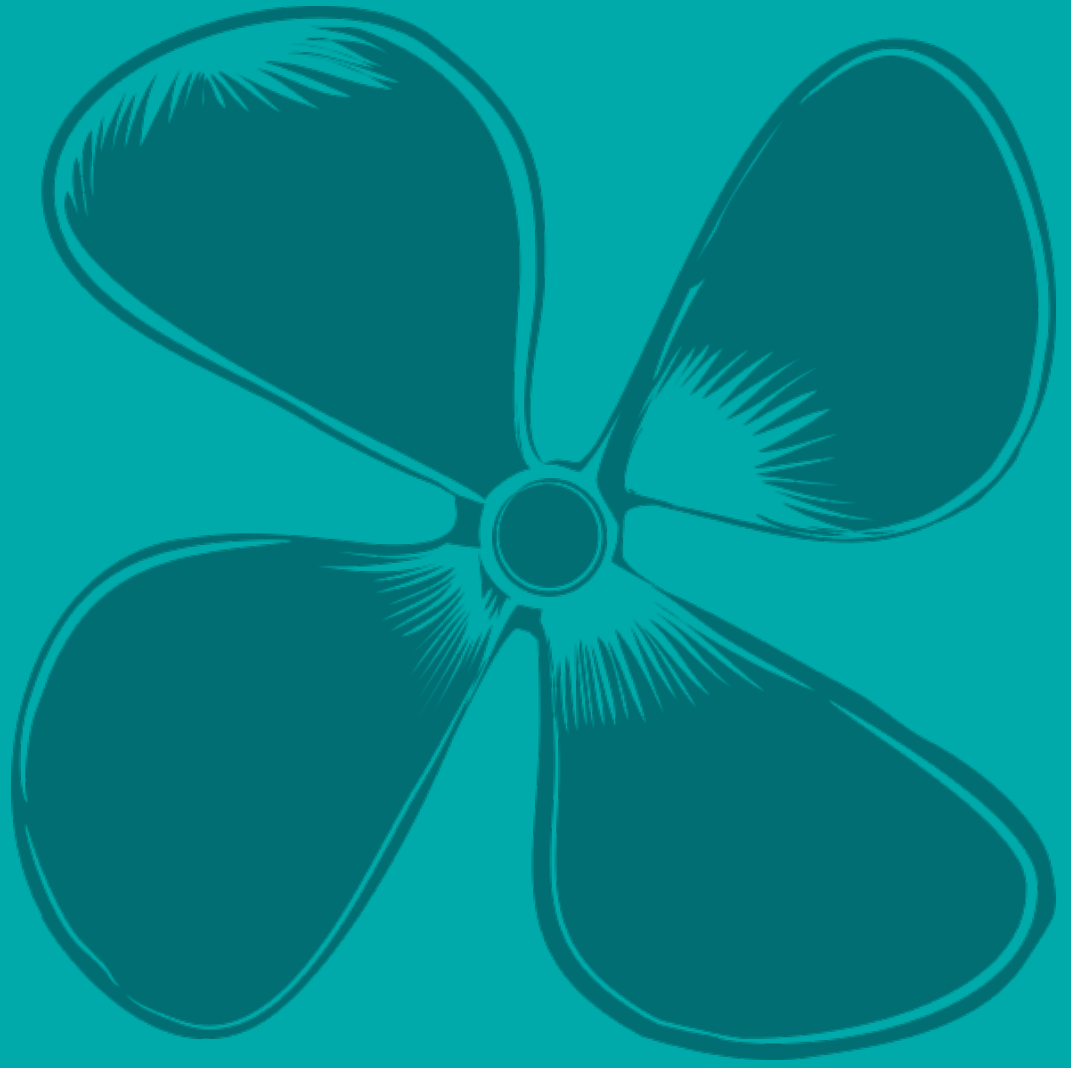
1. Stanovení rozsahu prostředí
2. Identifikace relevantních škodlivých aktérů a nástrojů
3. Identifikace relevantních technik
4. Mapování technik na MITRE ATT&CK v nástroji Navigator
5. Prioritizace relevantních technik
6. Zmapování pokrytí modelu existujícími opatřeními
7. Identifikace opatření pro pokrytí prozatím nepokrytých (sub)technik

Co říci na závěr?

- Přínosy modelování hrozeb při vývoji i ochraně průmyslových a specifických systémů (případně SoS) jsou neoddiskutovatelné
- Vycházení z tradičních „katalogů hrozeb“ je přinejmenším nevhodné
- Využívání metodik a postupů určených původně pro IT, vývoj softwaru, či jiné průmyslové/specifické oblasti může být v případě konkrétních OT systémů pro zajištění bezpečnosti relativně zajímavé

ALEF

Prostor pro Vaše dotazy



ALEF

Děkuji Vám za pozornost