



# Prevence je ideální, ale detekce je nezbytná: modelování hrozeb pro oblast security operations

**Jan Kopřiva**

Senior Security Consultant

jan.kopriva@alef.com     @jk0pr



# Efektivní (nejen) modrý tým

- 3 hlavní pilíře (PPT)
  - Lidé
  - Procesy
  - Technologie



# (Ne vždy) historický pohled na SOC

- Hlídáme perimetr a stanice v interní síti
  - Perimetrová IDS/IPS
  - Analýza NetFlow
  - Logy z anti-malware nástrojů
- Vzhledem ke standardnímu fungování mnoha moderních organizací (WFH, BYOD, cloud-first, ...) již delší dobu nevyhovující koncepce

# Vhodný moderní „modrý“ technický základ

- Pokrytí 3 domén
  - Sít'
    - IPS, NetFlow/IPFIX/Service-level analytika, „always on“ web proxy
  - Koncové body
    - AV/EPP, EDR
  - Aplikace
    - Nativní logy aplikací, reverse-proxy, ...
- On-premise, mobilní i cloudové systémy

# Postačuje takový přístup?

- „Nástroje X, Y a Z nám zajišťují detekci...“
  - Žádný nástroj nedokáže zachytit vše
  - Týmy, které se omezují výhradně na využívání out-of-the-box funkcionalit bezpečnostních nástrojů si samy svazují ruce
  - Je nezbytné využívat bezpečnostní nástroje, ale i **další zdroje dat** (ne nezbytně bezpečnostní) pro bezpečnostní dohled

# Oblast hrozeb je extrémně široká

- Reálně nelze pokrýt vše...

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	42 techniques	16 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoded (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Creates or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deployment Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Trusted Relationship	System Services (2)	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Execution Guardrails (1)	Modify Authentication Process (5)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Exfiltration Over Physical Medium (1)	Firmware Corruption
Search Open Websites/Domains (2)	Valid Accounts (4)	User Execution (3)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Victim-Owned Websites		Windows Management Instrumentation	System Services (2)	External Remote Services	Hijack Execution Flow (12)	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol	Scheduled Transfer	Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (12)	Process Injection (12)	Hide Artifacts (10)	Network Sniffing	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port	Transfer Data to Cloud Account	Resource Hijacking
				Implant Internal Image	Scheduled Task/Job (5)	Hijack Execution Flow (12)	OS Credential Dumping (8)	Network Service Discovery		Data from Removable Media	Protocol Tunneling	Service Stop	System Shutdown/Reboot
				Modify Authentication Process (5)	Valid Accounts (4)	Impair Defenses (9)	Indirect Command Execution	Network Share Discovery		Data from Removable Media	Proxy (4)		
				Office Application Startup (6)		Indicator Removal on Host (6)	Masquerading (7)	Network Sniffing		Data Staged (2)	Remote Access Software		
				Pre-OS Boot (5)		Indicator Removal on Host (6)	Modify Authentication Process (5)	Password Policy Discovery		Email Collection (3)	Traffic Signaling (1)		
				Scheduled Task/Job (5)		Scheduled Task/Job (5)	Modify Cloud Compute Infrastructure (4)	Peripheral Device Discovery		Input Capture (4)	Web Service (3)		
				Server Software Component (5)		Scheduled Task/Job (5)	Modify Registry	Permission Groups Discovery (3)		Screen Capture			
						Scheduled Task/Job (5)	Modify System	Process Discovery		Video Capture			
						Server Software Component (5)		Query Registry					
								Remote System					

# Modelování hrozeb na vhodné úrovni

The image shows the MITRE ATT&CK Navigator v4.6.6 interface. The browser address bar displays <https://mitre-attack.github.io/attack-navigator/>. The interface features a top navigation bar with 'layer' and 'technique controls' tabs. Below this is a grid of attack techniques, organized into 12 columns representing different phases of an attack:

- Reconnaissance** (10 techniques): Active Scanning, Gather Victim Host Information, Gather Victim Identity Information, Gather Victim Network Information, Gather Victim Org Information, Phishing for Information, Search Closed Sources, Search Open Technical Databases, Search Open Websites/Domains, Search Victim-Owned Websites.
- Resource Development** (7 techniques): Acquire Infrastructure, Compromise Accounts, Compromise Infrastructure, Develop Capabilities, Establish Accounts, Obtain Capabilities, Stage Capabilities.
- Initial Access** (9 techniques): Drive-by Compromise, Exploit Public-Facing Application, External Remote Services, Hardware Additions, Phishing, Replication Through Removable Media, Supply Chain Compromise, Trusted Relationship, Valid Accounts.
- Execution** (12 techniques): Command and Scripting Interpreter, Container Administration Command, Deploy Container, Exploitation for Client Execution, Inter-Process Communication, Native API, Scheduled Task/Job, Software Deployment Tools, System Services, User Execution, Windows Management Instrumentation, Hijack Execution Flow, Implant Internal Image.
- Persistence** (19 techniques): Account Manipulation, BITS Jobs, Boot or Logon Autostart Execution, Boot or Logon Initialization Scripts, Browser Extensions, Compromise Client Software Binary, Create Account, Create or Modify System Process, Event Triggered Execution, External Remote Services, Hijack Execution Flow, Indicator Removal on Host, Indirect Command Execution, Office Application Startup, Pre-OS Boot, Scheduled Task/Job, Server Software Component.
- Privilege Escalation** (13 techniques): Abuse Elevation Control Mechanism, Access Token Manipulation, Boot or Logon Autostart Execution, Boot or Logon Initialization Scripts, Browser Extensions, Compromise Client Software Binary, Create or Modify System Process, Domain Policy Modification, Escape to Host, Event Triggered Execution, Exploitation for Privilege Escalation, Hijack Execution Flow, Process Injection, Scheduled Task/Job, Valid Accounts, Masquerading, Modify Authentication Process, Modify Cloud Compute Infrastructure.
- Defense Evasion** (42 techniques): Abuse Elevation Control Mechanism, Access Token Manipulation, BITS Jobs, Build Image on Host, Debugger Evasion, Deobfuscate/Decode Files or Information, Deploy Container, Direct Volume Access, Domain Policy Modification, Execution Guardrails, Exploitation for Defense Evasion, File and Directory Permissions Modification, Hide Artifacts, Hijack Execution Flow, Impair Defenses, Indicator Removal on Host, Indirect Command Execution, Masquerading, Modify Authentication Process, Modify Cloud Compute Infrastructure.
- Credential Access** (16 techniques): Adversary-in-the-Middle, Brute Force, Credentials from Password Stores, Exploitation for Credential Access, Forced Authentication, Forge Web Credentials, Input Capture, Modify Authentication Process, Multi-Factor Authentication Interception, Multi-Factor Authentication Request Generation, Network Sniffing, OS Credential Dumping, Steal Application Access Token, Steal or Forge Kerberos Tickets, Steal Web Session Cookie, Unsecured Credentials.
- Discovery** (30 techniques): Account Discovery, Application Window Discovery, Browser Bookmark Discovery, Cloud Infrastructure Discovery, Cloud Service Dashboard, Cloud Service Discovery, Cloud Storage Object Discovery, Container and Resource Discovery, Debugger Evasion, Domain Trust Discovery, File and Directory Discovery, Group Policy Discovery, Network Service Discovery, Network Share Discovery, Network Sniffing, Password Policy, Peripheral Device Discovery, Process Discovery, Query Registry.
- Lateral Movement** (9 techniques): Exploitation of Remote Services, Internal Spearphishing, Lateral Tool Transfer, Remote Service Session Hijacking, Remote Services, Replication Through Removable Media, Software Deployment Tools, Taint Shared Content, Use Alternate Authentication Material.
- Collection** (17 techniques): Adversary-in-the-Middle, Archive Collected Data, Audio Capture, Automated Collection, Browser Session Hijacking, Clipboard Data, Data from Cloud Storage Object, Data from Configuration Repository, Data from Information Repositories, Data from Local System, Data from Network Shared Drive, Data from Removable Media, Data Staged, Email Collection, Input Capture, Screen Capture, Video Capture.
- Command and Control** (16 techniques): Application Layer Protocol, Communication Through Removable Media, Data Encoding, Data Obfuscation, Dynamic Resolution, Encrypted Channel, Fallback Channels, Ingress Tool Transfer, Multi-Stage Channels, Non-Application Layer Protocol, Non-Standard Port, Protocol Tunneling, Proxy, Remote Access Software, Traffic Signaling, Web Service.
- Exfiltration** (9 techniques): Automated Exfiltration, Data Transfer Size Limits, Data Encrypted for Impact, Data Manipulation, Defacement, Disk Wipe, Endpoint Denial of Service, Firmware Corruption, Inhibit System Recovery, Network Denial of Service, Resource Hijacking, Service Stop, System Shutdown/Reboot.
- Impact** (13 techniques): Account Access Removal, Data Destruction, Data Encrypted for Impact, Data Manipulation, Defacement, Disk Wipe, Endpoint Denial of Service, Firmware Corruption, Inhibit System Recovery, Network Denial of Service, Resource Hijacking, Service Stop, System Shutdown/Reboot.

The bottom left corner of the interface shows 'MITRE ATT&CK® Navigator v4.6.6' and the bottom right corner shows a 'legend' button.

# Optimální stav

- Pokrytí (nejen) relevantního modelu hrozeb
    - Z pohledu prevence
    - Z pohledu detekce
    - Z pohledu reakce
  - Vhodné vytvoření samostatných modelů pro jednotlivé oblasti
- Pro efektivní defenzivu platí, že prevence je ideální, detekce je nezbytná



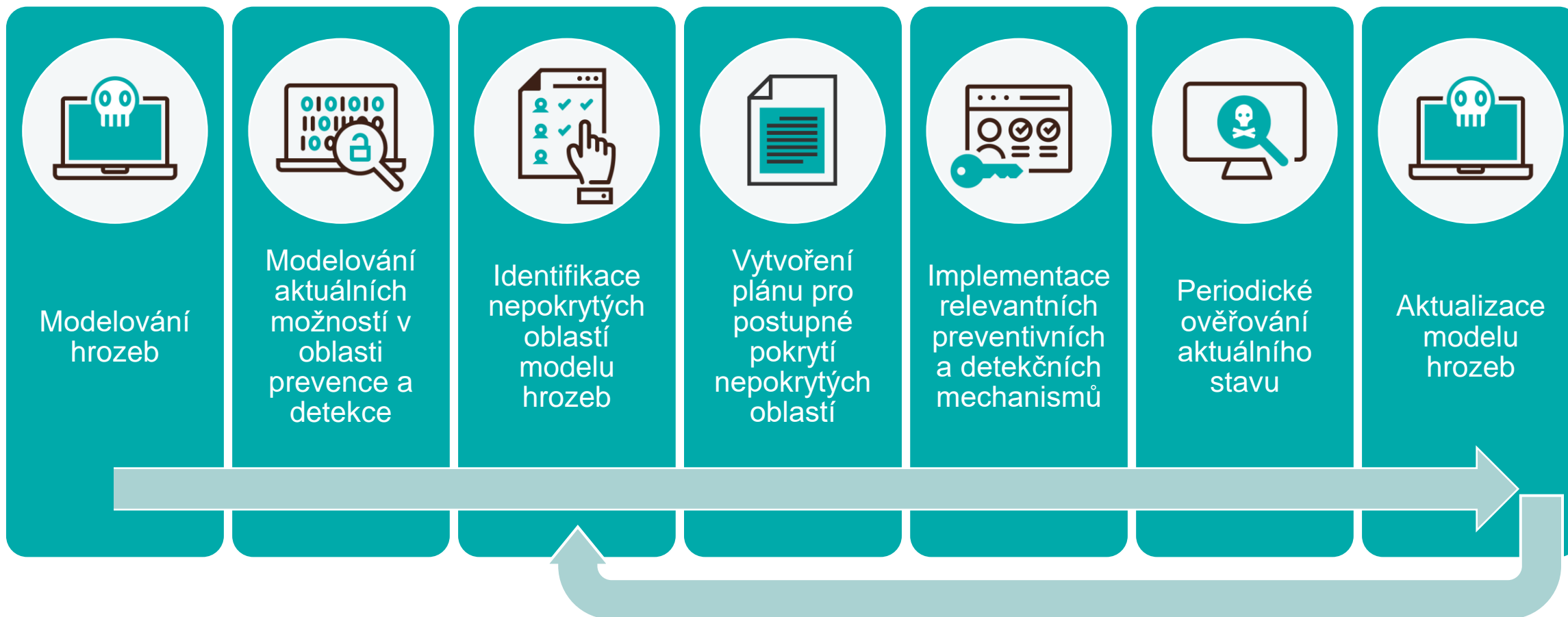
# Jak na nepokryté oblasti modelu hrozeb?

- Vlastní analytické mechanismy
  - Korelační pravidla a signatury „na míru“
- Méně obvyklé zdroje dat
  - Specifické logy z OS, pokročilé nástroje (Sysmon, eBPF, ...)
- „Kompenzační“ datové zdroje pro chybějící vstupy (nejen) na úrovni aplikací
- Silná automatizace s pomocí SIEM, SOAR a/nebo skriptů
  - Externí vstupy pro obohacení dat

# Jak postupovat?

- Začínat s „out-of-the-box“ funkcemi bezpečnostních nástrojů je v pořádku
- Je však nezbytné u nich neskončit
  - Vedle technických detekčních mechanismů vhodné zhodnotit i možnosti využívání threat huntingu
- Prostor pro rozšíření (nejen) detekčních kapacit „modrých“ týmů je téměř neomezený
  - Rozvoj nezbytné (alespoň do jisté míry) řídit

# Jak postupovat?



# Periodické ověřování stavu

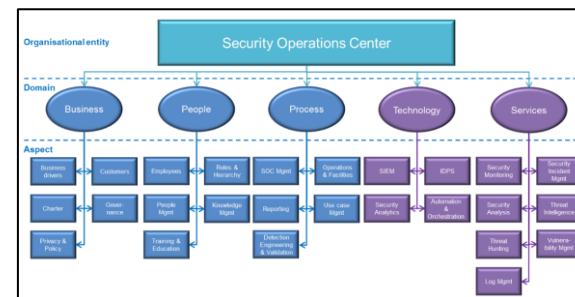
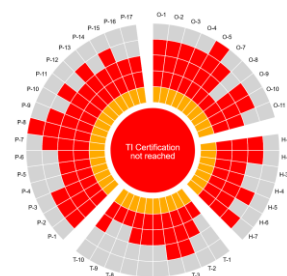
- Audit a (sebe)hodnocení
  - SIM3
  - SOC-CMM (a 4CERT)
  - MITRE ATT&CK a D3FEND
- Praktické testy
  - Red teaming
  - Purple teaming

# Metodiky nejen pro audity a (sebe)hodnocení

SIM3

SOC-CMM  
4CERT

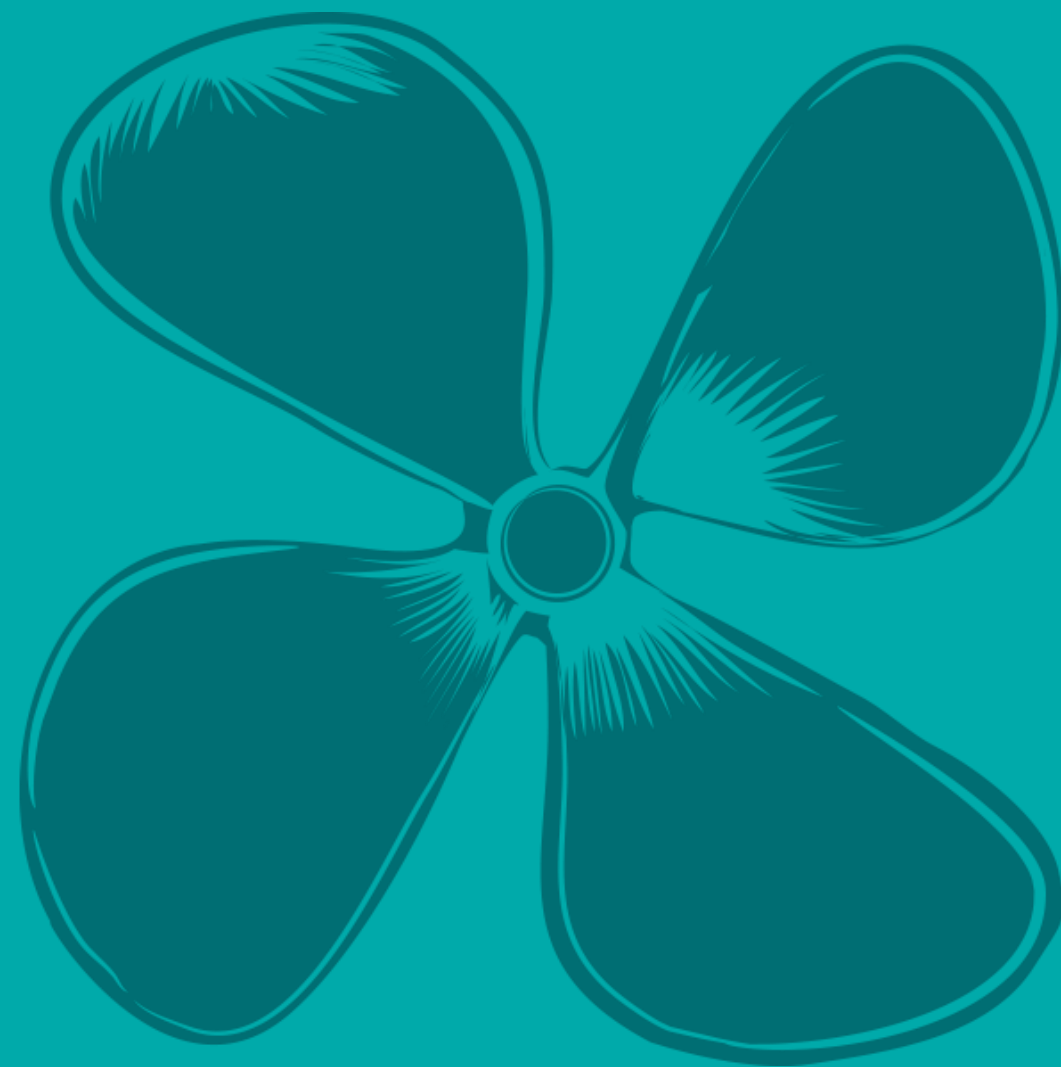
MITRE ATT&CK



Requirements	Process Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Local Admin	Collection	Command and Control	Exfiltration	Impact
...	...	...	...	...	...	...	...	...	...	...	...	...	...

**X ALEF**

**Prostor pro Vaše  
dotazy**



**ALEF**

**Děkuji Vám za  
pozornost**

