



NETTLES CONSULTING

# Threat modeling in security operations

Jan Kopriva

jan.kopriva@nettles.cz

 @jk0pr

# How do we usually handle security?

Risk assessment

- High-level identification of assets
- High-level identification of threats and vulnerabilities
- Risk assessment and specification of appropriate high-level security controls

- A look into a crystal ball?

Implementation  
of specific  
controls

- Implementation of specific technical and organizational controls relevant to some aspects of identified high-level threats and risks

# What does this mean for security operations?

- Risk assessment on the level of an entire organization requires that certain abstractions be made
- We usually lack technical detail when it comes to relevant threats and therefore can't reliably detect them
- Choice of appropriate detections and analytics (correlation rules, etc.) usually is/has to be based on „expert judgement“

# This is a problem...

*“If you know the enemy and know yourself, you need not fear the result of a hundred battles.*

*If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.*

*If you know neither the enemy nor yourself, you will succumb in every battle.”*



- Sun Tzu

# Analogous situations come up in other areas as well

- OWASP Top 10 as the only basis for security web applications
  - From an objective standpoint, all risks all probably relevant
  - Specific controls to mitigate the risks are not necessarily obvious
    - A04:2021 – Insecure design
    - A09:2021 – Security Logging and Monitoring Failures
- But... OWASP Top 10 is usually not the only basis for web application security
  - „Secure“ SDLs (e.g., with the use of ASVS) always include some threat modeling and attack surface management aspects

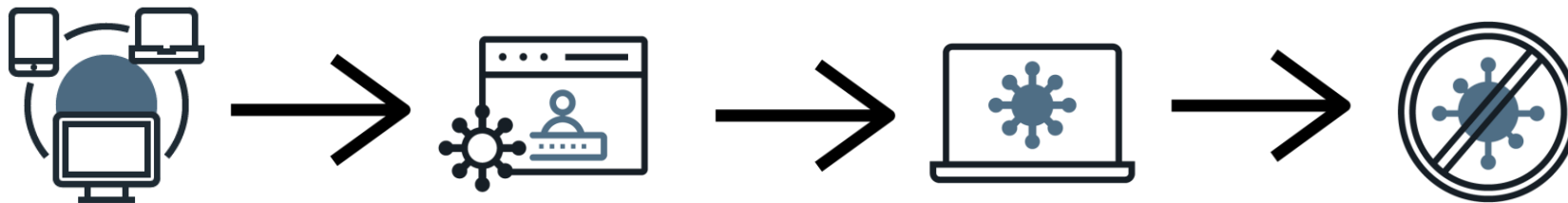
# Threat modeling

*„A process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified, enumerated, and mitigations can be prioritized.“*

Wikipedia

# Generic approach to threat modeling

1. Scope determination and creating an abstraction/decomposition of the protected system
2. Identification of factors that may affect individual components of the system or their interactions in an unfavorable manner
3. Modeling of individual scenarios related to identified factors
4. Identification of controls that eliminate threats, mitigate their impact or enable their detection



# Most common „open“ methodologies for threat modeling

- STRIDE (+DREAD)
- IDDIL/ATC
- PASTA
- Attack trees
- LINDDUN
- OCTAVE
- NIST SP 800-154



# Threat modeling for arbitrary system

- Open Source Security Testing Methodology Manual (OSSTMM) in version 3 is not (just) a methodology for penetration testing
- Analysis of „porosity“ of a system may serve as a threat modeling approach

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

# Organization-wide „technical“ threat model (not just) for security operations?

- In general, this is somewhat of a problematic concept, since we don't necessarily have full knowledge of relevant threats
  - OSSTMM may help to overcome this issue, however, it is not „user-friendly“ when it comes to threat modeling in highly complex „system of systems“ environments
- Although it is not primarily intended for threat modeling, we've had a tool, which describes threats on a suitable level of abstraction for a while now...

# MITRE ATT&CK

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

# MITRE ATT&CK Enterprise

		<b>Reconnaissance</b> 10 techniques	<b>Resource Development</b> 7 techniques		
<b>Initial Access</b> 9 techniques	<b>Execution</b> 12 techniques	<b>Persistence</b> 19 techniques	<b>Privilege Escalation</b> 13 techniques	<b>Defense Evasion</b> 42 techniques	<b>Credential Access</b> 16 techniques
<b>Discovery</b> 30 techniques	<b>Lateral Movement</b> 9 techniques	<b>Collection</b> 17 techniques	<b>Command and Control</b> 16 techniques	<b>Exfiltration</b> 9 techniques	<b>Impact</b> 13 techniques

# MITRE ATT&CK Enterprise – Details of (sub)techniques

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques
Active Scanning (3)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (3)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools
Search Victim-Owned Websites			System Services (2)
			User Execution (3)
			Windows Management Instrumentation

## Mitigations

ID	Mitigation	Description
M1048	Application Isolation and Sandboxing	Application isolation will limit what other processes and system features the exploited target can access.
M1050	Exploit Protection	Web Application Firewalls may be used to limit exposure of applications to prevent exploit traffic from reaching the application.
M1030	Network Segmentation	Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure.
M1026	Privileged Account Management	Use least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system.
M1051	Update Software	Update software regularly by employing patch management for externally exposed applications.
M1016	Vulnerability Scanning	Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure. <sup>[6]</sup>

## Detection

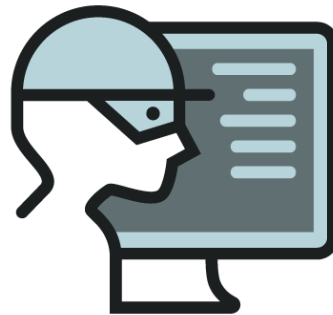
ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Detecting software exploitation may be difficult depending on the tools available. Software exploits may not always succeed or may cause the exploited process to become unstable or crash. Web Application Firewalls may detect improper inputs attempting exploitation.
DS0029	Network Traffic	Network Traffic Content	Use deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection strings or known payloads.

## Procedure Examples

ID	Name	Description
G0007	APT28	APT28 has used a variety of public exploits, including CVE 2020-0688 and CVE 2020-17144, to gain execution on vulnerable Microsoft Exchange; they have also conducted SQL injection attacks against external websites. <sup>[8][9]</sup>
G0016	APT29	APT29 has exploited CVE-2019-19781 for Citrix, CVE-2019-11510 for Pulse Secure VPNs, CVE-2018-13379 for FortiGate VPNs, and CVE-2019-9670 in Zimbra software to gain access. They have also exploited CVE-2020-0688 against the Microsoft Exchange Control Panel to regain access to a network. <sup>[10][11][12]</sup>
G0087	APT39	APT39 has used SQL injection for initial compromise. <sup>[13]</sup>

# MITRE ATT&CK as a tool for threat modeling

- We can model threats to our environment quite easily, if we know:
  - Which platforms are relevant for us
  - What groups and tools are relevant for us
  - What (sub)techniques do these tools and groups use



# MITRE ATT&CK as a tool for threat modeling

1. Identification of relevant platforms is trivial for most security teams
2. Identification of relevant groups and tools is more complicated, but not by much
  - If we have CTI mechanisms in place, we already know what's relevant for us
  - Even a quick analysis based only on which threat actor groups target similar organizations based on geography and „market vertical“ can provide highly valuable input
  - Mapping of dominant (sub)techniques on different threat actor groups is already available
3. After identification of relevant (sub)techniques, it is necessary to prioritize them

# MITRE ATT&CK as a tool for threat modeling

4. Mapping of already implemented controls and capabilities should follow
  - It is advisable to map „detection“ and „reaction“ capabilities individually
  - Making some indication of coverage of individual (sub)techniques can be beneficial
5. The final step is identification of controls to cover previously uncovered/weakly covered (sub)techniques



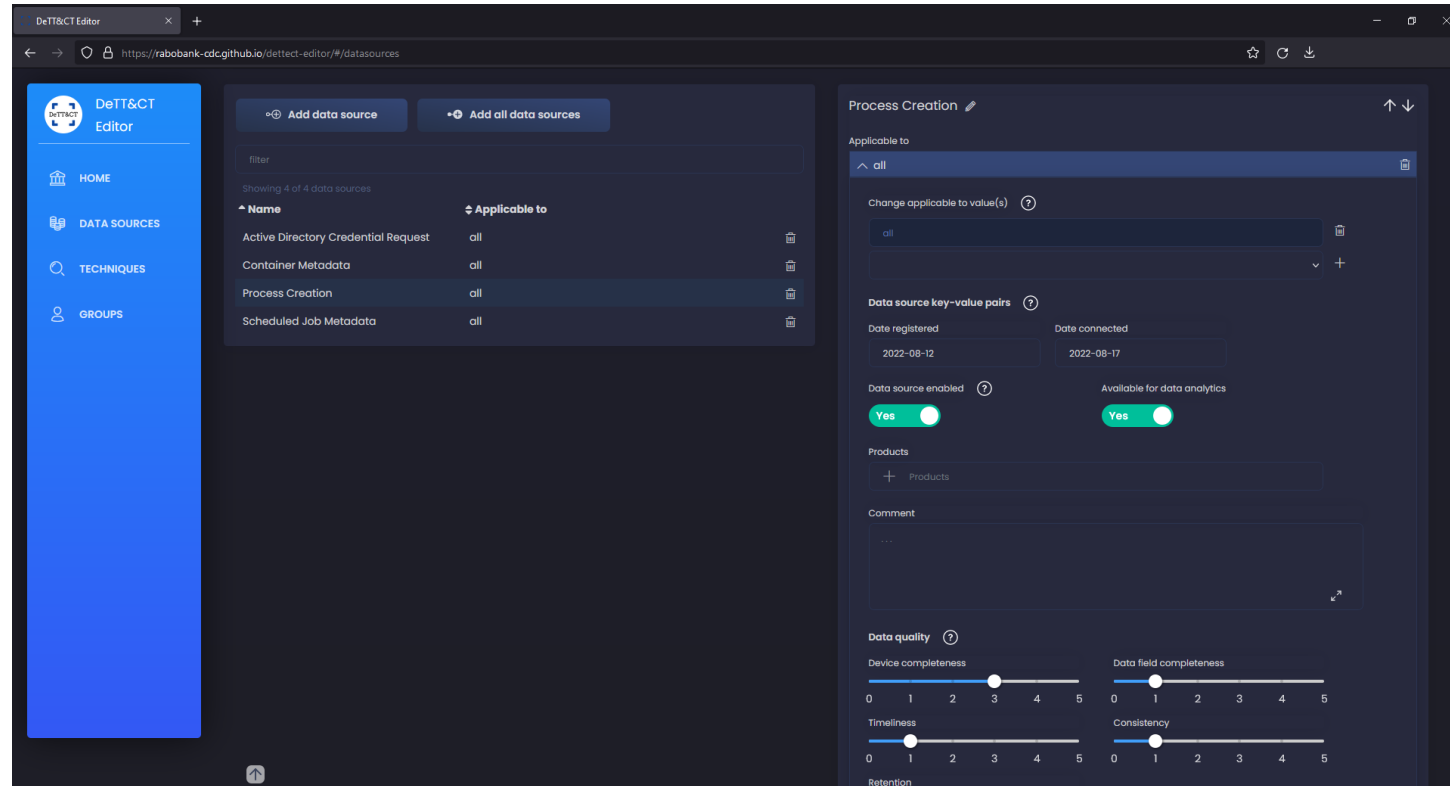
# MITRE ATT&CK Navigator – mapping of threats and controls

The screenshot displays the MITRE ATT&CK Navigator interface. The top navigation bar includes 'layer', 'selection controls', 'layer controls', and 'technique controls'. The main content area is a grid with columns representing attack phases and rows representing specific techniques. The columns are: Reconnaissance (10 techniques), Resource Development (7 techniques), Initial Access (9 techniques), Execution (12 techniques), Persistence (19 techniques), Privilege Escalation (13 techniques), Defense Evasion (42 techniques), Credential Access (16 techniques), Discovery (30 techniques), Lateral Movement (9 techniques), Collection (17 techniques), Command and Control (16 techniques), Exfiltration (9 techniques), and Impact (13 techniques). Each cell in the grid contains a technique name and a color-coded indicator (e.g., red for active, green for present, blue for not present). The interface also features a search bar, a legend, and a version number (v4.6.6) in the bottom left corner.

Reconnaissance (10 techniques)	Resource Development (7 techniques)	Initial Access (9 techniques)	Execution (12 techniques)	Persistence (19 techniques)	Privilege Escalation (13 techniques)	Defense Evasion (42 techniques)	Credential Access (16 techniques)	Discovery (30 techniques)	Lateral Movement (9 techniques)	Collection (17 techniques)	Command and Control (16 techniques)	Exfiltration (9 techniques)	Impact (13 techniques)
Active Scanning (0/3)	Acquire Infrastructure (1/6)	Drive-by Compromise	Command and Scripting Interpreter (1/4)	Account Manipulation (0/6)	Abuse Elevation Control Mechanism (1/4)	Abuse Elevation Control Mechanism (1/4)	Adversary-in-the-Middle (0/2)	Account Discovery (2/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/2)	Application Layer Protocol (2/4)	Automated Exfiltration	Account Access Removal
Gather Victim Host Information (1/4)	Compromise Accounts (2/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (1/5)	Access Token Manipulation (1/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (1/4)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (1/3)	Compromise Infrastructure (1/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (2/14)	Boot or Logon Autostart Execution (2/14)	BITS Jobs	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoded (0/2)	Efiltration Over Alternative Protocol (1/2)	Data Encrypted for Impact
Gather Victim Network Information (1/6)	Develop Capabilities (1/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data (0/2)	Data Manipulation (0/3)	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (2/2)	Phishing (3/3)	Inter-Process Communication (1/2)	Browser Extensions	Browser Extensions	Debugger Evasion	Deobfuscate/Decode Files or Information	Cloud Service Dashboard	Remote Services (4/6)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Defacement (0/2)
Phishing for Information (2/3)	Obtain Capabilities (2/4)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Compromise Client Software Binary	Deploy Container	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/3)	Defacement (0/2)
Search Closed Sources (0/2)	Stage Capabilities (0/3)	Scheduled Task/Job (1/3)	Scheduled Task/Job (1/3)	Domain Policy Modification (0/2)	Domain Policy Modification (0/2)	Direct Volume Access	Input Capture (1/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Encrypted Channel (0/2)	Firmware Corruption	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Supply Chain Compromise (0/3)	Shared Modules	Shared Modules	Create Account (1/3)	Create Account (1/3)	Execution Guardrails (0/2)	Modify Authentication Process (0/5)	Container and Resource Discovery	Software Deployment Tools	Data from Configuration Repository (0/2)	Fallback Channels	Exfiltration Over Physical Medium (0/3)	Inhibit System Recovery
Search Open Websites/Domains (0/2)	Trusted Relationship	Software Deployment Tools	Software Deployment Tools	Create or Modify System Process (1/4)	Create or Modify System Process (1/4)	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Domain Trust Discovery	Debugger Evasion	Data from Information Repositories (1/3)	Ingress Tool Transfer	Exfiltration Over Web Service (1/2)	Network Denial of Service (0/2)
Search Victim-Owned Websites	Valid Accounts (3/6)	User Execution (2/3)	User Execution (2/3)	Event Triggered Execution (2/15)	Event Triggered Execution (2/15)	Exploitation for Privilege Escalation	Multi-Factor Authentication Request Generation	File and Directory Discovery	Domain Trust Discovery	Data from Local System	Multi-Stage Channels	Scheduled Transfer	Resource Hijacking
		Windows Management Instrumentation	Windows Management Instrumentation	External Remote Services	External Remote Services	Hijack Execution Flow (1/12)	Multi-Factor Authentication Request Generation	Group Policy Discovery	Use Alternate Authentication Material (1/4)	Data from Network Shared Drive	Non-Application Layer Protocol	Transfer Data to Cloud Account	System Shutdown/Reboot
				Hijack Execution Flow (1/12)	Hijack Execution Flow (1/12)	Hijack Injection (2/12)	Network Service Discovery	Network Service Discovery		Data from Removable Media	Non-Standard Port		
				Scheduled Task/Job (1/3)	Scheduled Task/Job (1/3)	Impair Defenses (2/9)	Network Share Discovery	Network Share Discovery		Data Staged (2/2)	Proxy (2/4)		
				Implant Internal Image	Implant Internal Image	Modify Authentication Process (0/5)	OS Credential Dumping (0/5)	Network Sniffing		Email Collection (2/3)	Remote Access Software		
				Modify Authentication Process (0/5)	Modify Authentication Process (0/5)	Office Application Startup (1/6)	Steal Application Access Token	Password Policy Discovery		Input Capture (1/4)	Traffic Signaling (0/1)		
				Pre-OS Boot (0/3)	Pre-OS Boot (0/3)	Scheduled Task/Job (1/3)	Masquerading (1/1)	Peripheral Device Discovery		Screen Capture	Web Service (0/3)		
				Scheduled Task/Job (1/3)	Scheduled Task/Job (1/3)	Server Software Component (1/3)	Modify Cloud Compute Infrastructure (0/4)	Process Discovery		Video Capture			
				Unsecured	Unsecured			Query Registry					

- Details at <https://github.com/mitre-attack/attack-navigator>
- Demo at <https://mitre-attack.github.io/attack-navigator/>

# DeTT&ct Editor – data source mapping



- Details at <https://github.com/rabobank-cdc/DeTTECT>
- Demo at <https://rabobank-cdc.github.io/detect-editor/>

# Main takeaways

- Basic threat modeling approach can be quite straightforward
  1. Identify relevant platforms
  2. Identify relevant threat actor groups and tools
  3. Identify relevant (sub)techniques
  4. Map (sub)techniques to MITRE ATT&CK using ATT&CK Navigator
  5. Prioritize relevant (sub)techniques
  6. Map existing controls to the resulting threat model
  7. Identify controls for prevention and/or detection which will cover currently „uncovered“ (sub)techniques

# What will this result in?

## Risk assessment

- High-level identification of assets
- High-level identification of threats and vulnerabilities
- Risk assessment and specification of appropriate high-level security controls

## „Technical“ threat modeling

- Identification of corresponding threats on a lower level of abstraction
- Identification of specific requirements for security controls and analytics

## Implementation of specific controls

- Implementation of specific technical and organizational controls relevant to some aspects of identified high-level threats and risks

# Few thoughts to end on...

*„Anyone can invent a security system that he himself cannot break.“*

- Bruce Schneier

**True, but that doesn't mean we shouldn't try to invent the best system possible.**

# Additional materials

[http://csirt.xyz/#threat\\_modeling](http://csirt.xyz/#threat_modeling)



# Q&A



NETTLES CONSULTING

**Thank you for your  
attention!**



NETTLES CONSULTING