TLP:CLEAR

NETTLES CONSULTING

Threat modeling in security operations

Jan Kopřiva

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

NETTLES CONSULTING

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“

NETTLES CONSULTING

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

NETTLES CONSULTING

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

NETTLES CONSULTING

Threat modeling

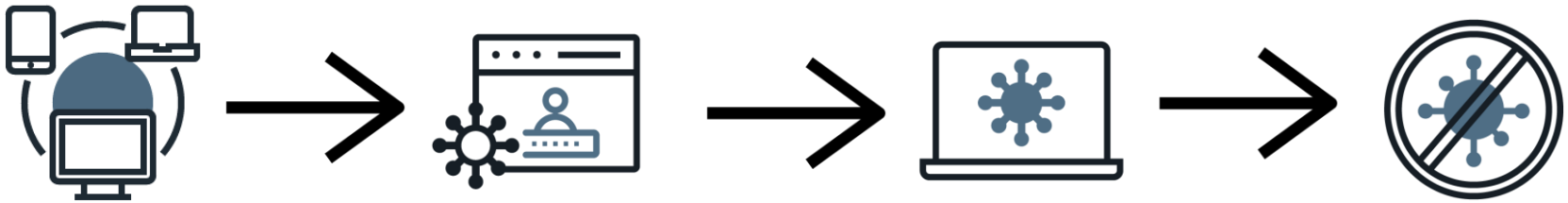
„A process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified, enumerated, and mitigations can be prioritized.“

Wikipedia

NETTLES CONSULTING

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 deteciton



NETTLES CONSULTING

Most common „open“ methodologies for threat modeling

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

NETTLES CONSULTING

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

Zdroj: OSSTMMv3

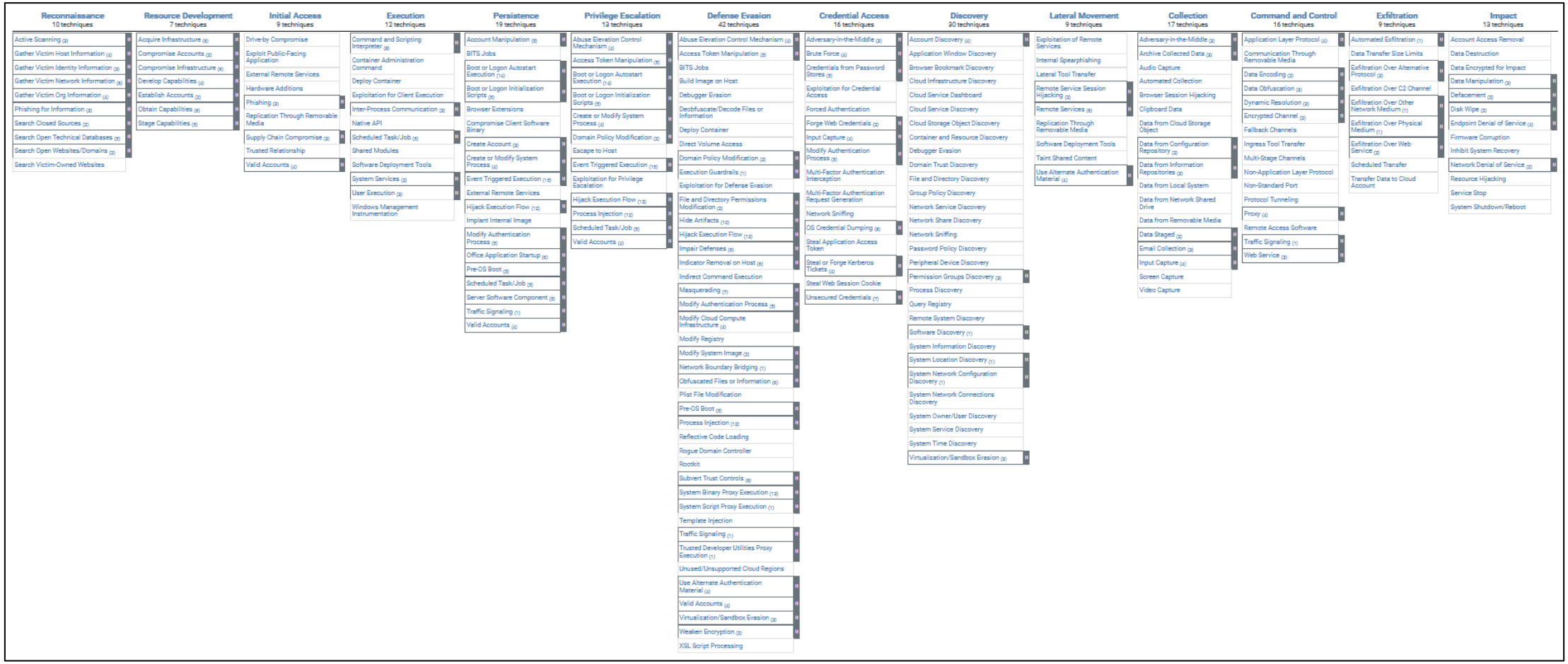
NETTLES CONSULTING

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 a tool, which describes threats on a suitable level of abstraction for a while now…

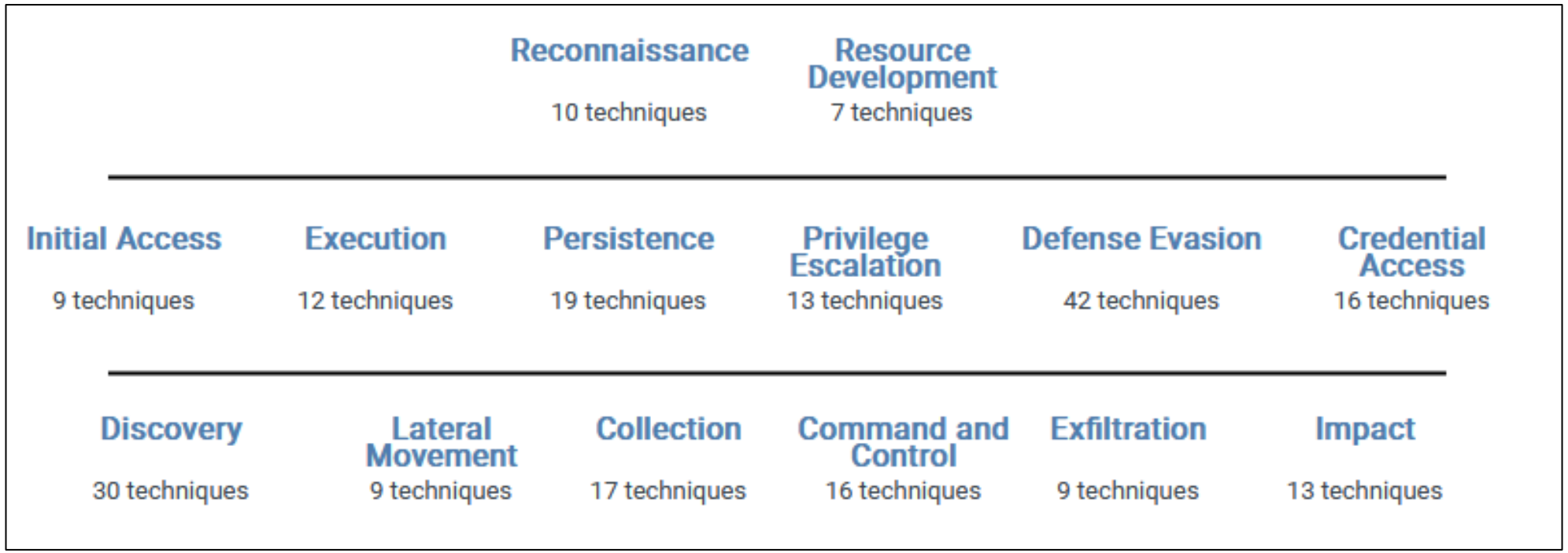
NETTLES CONSULTING

MITRE ATT&CK



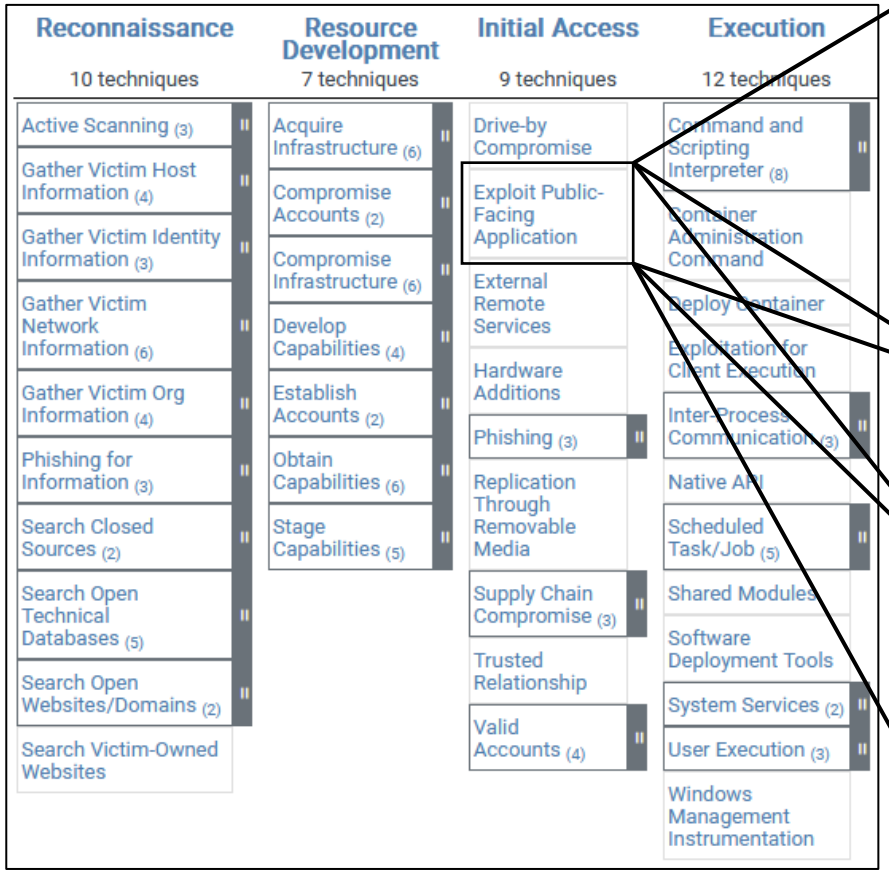
NETTLES CONSULTING

MITRE ATT&CK Enterprise



NETTLES CONSULTING

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



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.[6]

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.[8][9]
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.[10][11][12]
G0087	APT39	APT39 has used SQL injection for initial compromise.[13]

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

NETTLES CONSULTING

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

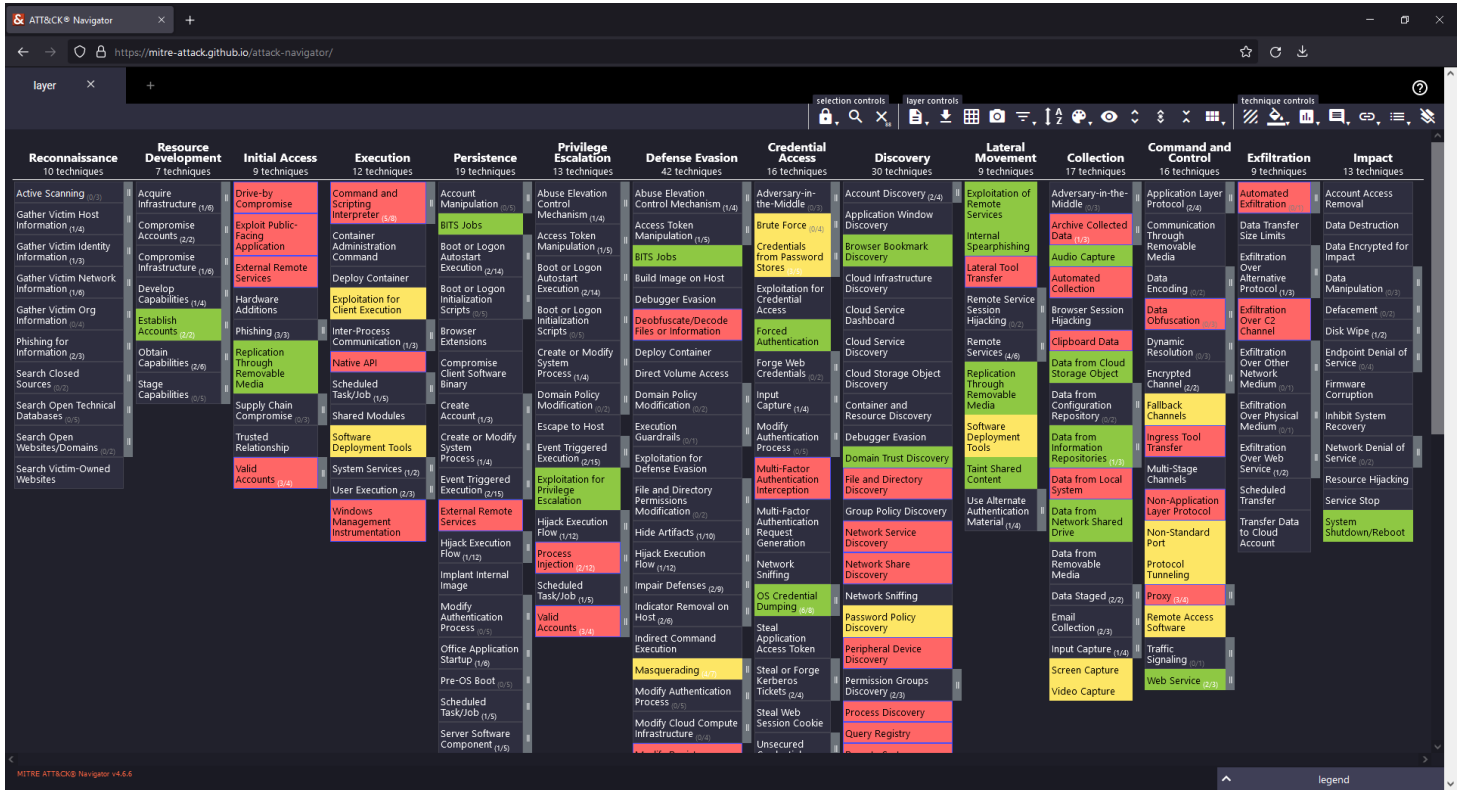
NETTLES CONSULTING

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

NETTLES CONSULTING

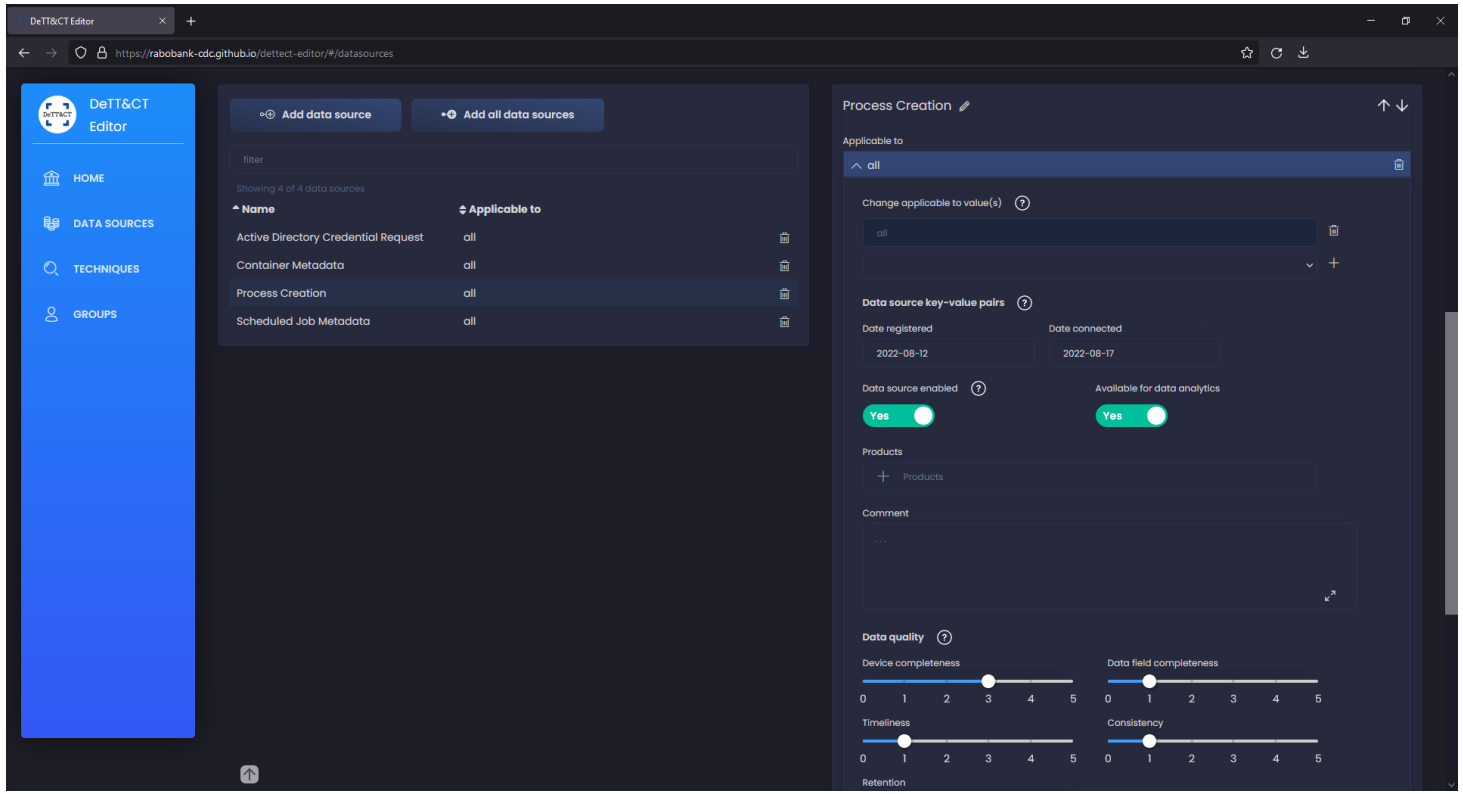
MITRE ATT&CK Navigator – mapping of threats and controls



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

NETTLES CONSULTING

DeTT&ct Editor – data source mapping



- Details at https://github.com/rabobank-cdc/DeTTECT
- Demo at https://rabobank-cdc.github.io/dettect-editor/

NETTLES CONSULTING

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

NETTLES CONSULTING

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

NETTLES CONSULTING

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.

NETTLES CONSULTING

Additional materials

http://csirt.xyz/#threat_modeling

NETTLES CONSULTING

Q&A

NETTLES CONSULTING

Thank you for your attention!

NETTLES CONSULTING