



NETTLES CONSULTING

Free Nation-Scale Threat Models as a Public Service: A New Czech Cybersecurity Initiative

Jan Kopriva

jan.kopriva@nettles.cz

<https://www.linkedin.com/in/jan-kopriva/>

What do we need to protect ourselves from?

- Security controls should be chosen based on relevant, realistic threats to the specific environment
 - Common basis is an organization-level risk assessment
 - For technical work (i.e., choosing specific detection rules or configuring specific protection capabilities), we need more in-depth requirements definition
 - MITRE ATT&CK is a de facto standard for CTI as well as “tactical” threat modeling



- ATT&CK-based threat models commonly consist of heatmaps that show and/or score (sub-)techniques based on their relevance for a specific entity



NETTLES
CONSULTING

Threat modeling with ATT&CK

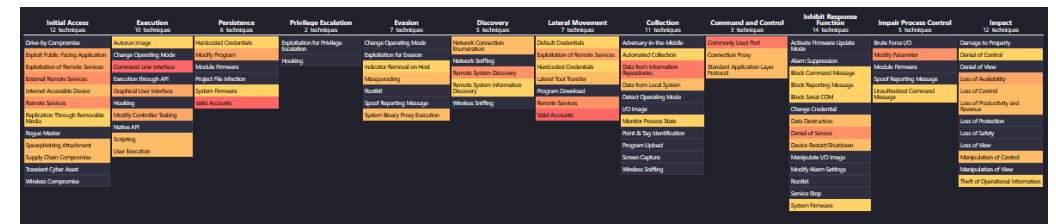
- Regardless of methodology, certain basic principles are seen as ubiquitous
 - (Sub-)techniques most relevant to a specific entity are those which are:
 - Used by threat actors relevant to that entity – either directly (historical incidents, security monitoring data, ...) or due to its sectoral and/or geographic profile or due to its technology stack
 - Associated with malware and tools that are relevant for that entity – either directly (historical incidents, security monitoring data, ...) or due to its geographic profile or technology stack

A tale of threat modeling for a ministerial department...



Chosen approach

- Given the Ministry's purview, it was decided to develop 3 (4) models
 - Generic Enterprise-based model for Czech organizations regardless of sector
 - Specific Enterprise-based model for Czech governmental departments and other public institutions
 - Generic Enterprise-based and ICS-based models for Czech industrial organizations
 - Specific Enterprise-based and ICS-based models for Czech energy companies and pipeline operators



Chosen approach

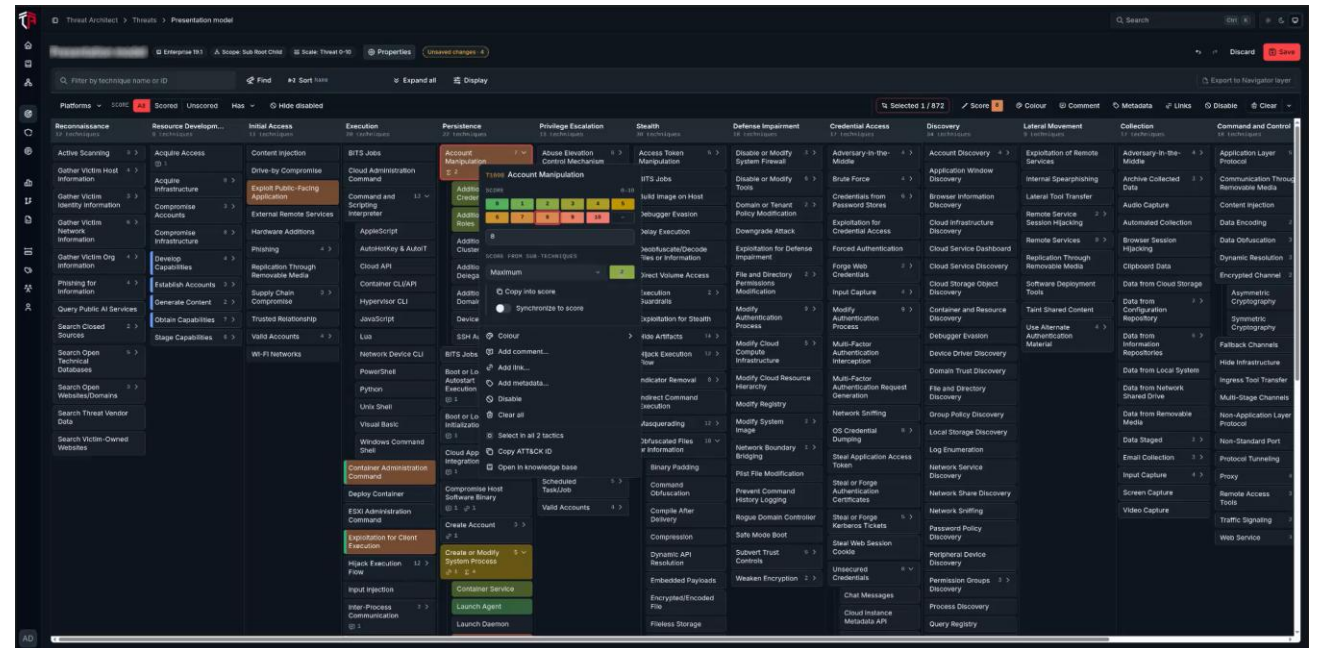
- First batch of models to be made available in Q4 2025
- Highly permissive license allowing for use in commercial settings
- Models to be distributed for free, but not made available publicly
 - Any private or public entity in the Czech Republic can request and receive the model(s) appropriate to its sector, along with documented methodology describing their use
- Updates to correspond with new ATT&CK releases (slightly staggered)
- At first, e-mail to be used as the sole distribution channel
 - Distribution through the official portal of the Czech National Cyber and Information Security Agency is currently being implemented

How does it work on the inside?

- Multiple “partial” models/layers are developed based on various inputs and CTI assessments
 - Some models/layers based on proprietary data (e.g., data from partner organizations providing security monitoring or incident response services, data from organizations in the industry, etc.)
 - Some models/layers based on open sources (third-party analyses of threat actor activities, malware statistics, etc.)
- “Partial” models are weighted and used to create a “final” model for each group of organizations
- Some “partial” models are made available alongside the “final” models
 - Organizations may choose to create their own models based on their own data and on some of the “partial” models provided by the Ministry

How does it work on the inside?

- All layers/models built in the first batch were created with the help of Navigator
 - Navigator is a great tool, but does not easily lend itself to modeling using dozens of unique, periodically updated layers
 - We are currently developing an “enterprise-level” platform to help ease the creation of more complex models and enable organizations to more effectively model threats for their environments



Are the models used in practice?

- Currently, more than 100 Czech organizations across all sectors receive models from the Ministry
 - Some of these are large corporations with multiple subsidiaries, so the final number of organizations using the models is significantly higher



Threat-Informed Defense – practical use cases for the models

- The models can be used as a basis for developing a truly Threat-Informed approach to defense in organizations
 - Security controls may be mapped to ATT&CK, and a gap assessment can then be conducted to identify uncovered/minimally covered/optimally covered techniques
 - Appropriate additional controls can then be identified in a measurable way
 - SOC stakeholders identify areas where detection coverage should be increased
 - Hardening baselines may be updated based on gaps
 - Discussion of „what should our new EDR actually do“ move from „detect threats“ to „detect these attack techniques as a priority“

One small recommendation to end on

- To anyone from a national CSIRT (or a large governmental department, regional regulatory body etc.): consider doing the same as the Czech Ministry of Industry and Trade
 - Even in 2026, only a small percentage of organizations have the capability to develop a more advanced ATT&CK-based threat model than “APT28 + APT29” and if your organization can provide a more complex model, it can help raise level of cyber security nation-wide at a very low cost
 - As we’ve shown, you don’t need much to start with – a few CTI analysts, some relevant data, MITRE ATT&CK Navigator, and an e-mail as a distribution channel can work just fine if nothing else is available

Q&A



NETTLES CONSULTING

Thank you for your attention!



NETTLES CONSULTING