NETTLES CONSULTING

Od hrozeb k měřitelné bezpečnosti: Threat-Informed Defense v praxi

Jan Kopřiva

jan.kopriva@nettles.cz

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

CYBER_CON 2026

Agenda workshopu

- Proč nestačí generické hrozby a generická opatření
- Threat-Informed Defense a role CTI
- Modelování hrozeb a rámec MITRE ATT&CK
- Modely hrozeb poskytované ze strany MPO
- Práce s modely hrozeb v nástroji ATT&CK Navigator
- Mezery v pokrytí modelů hrozeb a smysluplný výběr nových bezpečnostních opatření

NETTLES CONSULTING

Praktická část – co budete potřebovat

- Vlastní laptop s aktuálním webovým prohlížečem
- ATT&CK Navigator
  - https://mitre-attack.github.io/attack-navigator/
- Stažený soubor s generickými modely hrozeb
  - https://0x90.cz/x/cybercon/
  - Heslo: Fw8gEeSo
- Vhodné, pokud máte orientační přehled o:
  - Vlastních technických a procesních bezpečnostních opatřeních
  - Vlastní analýze rizik

NETTLES CONSULTING

Proč nestačí generické hrozby?

NETTLES
CONSULTING

Kybernetická bezpečnost jako „babylonská věž“

- Efektivní zajištění kybernetické bezpečnosti z principu vyžaduje spolupráci řady různých rolí a týmů
  - Management, řízení rizik, architektura, administrace infrastruktury, SOC, CSIRT, ofenzivní specialisté, …
- Jednotlivé specializace pracují s odlišnou terminologií, metrikami i cíli
  - Chybí jasně definované vazby mezi aktivitami jednotlivých rolí a týmů
  - Fakticky přitom všechny řeší tentýž problém, tedy „jak efektivně zabezpečit organizaci?“
- Důsledky této fragmentace nejsou pouze akademický problém:
  - Obtížné prokazování efektivity implementovaných bezpečnostních opatření
  - Nejasné mapování rizik na konkrétní technické nástroje a konfigurace
  - Mezery mezi očekávanými a reálnými detekčními schopnostmi organizace

NETTLES CONSULTING

Limity tradičních přístupů k řízení bezpečnosti

- Většina standardů a metodik je založena na analýze a řízení rizik
  - Výsledkem jejich použití je (resp. může být) odpověď na otázku, co by organizace obecně dělat měla
  - Typicky na jejich základě není možné říci, jak konkrétně specifická opatření implementovat
    - Aneb „co má vlastně pokrývat ten náš bezpečnostní monitoring, který potřebujeme?“
- I kvalitně zpracovaná analýza rizik je primárně strategický materiál
  - Bez provázání na taktickou a operační úroveň neposkytuje smysluplné vstupy pro návrh preventivních ani detekčních opatření na technické úrovni ani pro konfiguraci nástrojů
- V praxi tak vznikají generická opatření odpovídající obecným hrozbám
- Chybí systematická měřitelnost skutečné efektivity opatření
  - Organizace deklaruje, že opatření hrozbu pokrývá, ale nemá jak to ověřit, řízení bezpečnosti je pak založeno na „expertním odhadu“, nikoli na měřitelných objektivních datech

NETTLES CONSULTING

Praktický příklad – hrozba typu „škodlivý kód“

- Analýza rizik: „hrozba škodlivého kódu má vysokou pravděpodobnost realizace a střední dopad“
  - Ponechme stranou smysluplnost kvalitativního stanovení jednotlivých faktorů rizika…
- Odvozené opatření: nasazení anti-malware nástroje či platformy typu EDR
  - Konceptuálně zcela smysluplné opatření – problém je v tom, co následuje
- Bez znalosti konkrétního chování relevantního škodlivého kódu nelze určit:
  - Jak má být řešení nakonfigurováno a jaké detekční mechanismy má implementovat
  - Jak ověřit, že opatření skutečně funguje proti tomu, co organizaci reálně ohrožuje
- Stejný problém vzniká v bezpečnostním dohledu (zde jsou výsledkem generická detekční pravidla) a v dalších oblastech
  - Shrnuto a podrženo – z výstup z analýzy rizik zpravidla není zřejmé, nejen na základě jakých dat bylo hodnocení hrozby stanoveno, ale ani co konkrétně v kontextu dané organizace znamená

NETTLES CONSULTING

Threat-Informed Defense

NETTLES
CONSULTING

Threat-Informed Defense (TID)

- Přístup, který staví návrh a řízení bezpečnosti na dokumentované znalosti reálných hrozeb
- Místo abstraktních kategorií hrozeb pracuje s konkrétním, pozorovaným chováním útočníků (příp. škodlivého kódu apod.) a s jeho realistickými dopady na vlastní prostředí organizace
- CTI zde není jedním z možných vstupů, ale základním referenčním zdrojem
- Výsledkem řízení bezpečnosti s pomocí principů TID je architektura odvozená ne od splnění konkrétní normy, ale od průkazné a měřitelné schopnosti čelit technikám konkrétních aktérů

NETTLES CONSULTING

TID není náhrada řízení rizik, ale jeho rozšíření

- Koncept není v rozporu s tradičními přístupy k řízení KB – ty dobrou znalost hrozeb konec konců implicitně předpokládají
  - Každý ISMS založený na řízení rizik by měl být automaticky založen i na principech TID, v praxi však modelování hrozeb i CTI často zcela chybí a vazba na reálné hrozby je tak slabá
- TID předpokládá, že CTI bude primárním vstupem napříč všemi úrovněmi řízení KB a že všechny úrovně budou vzájemně propojeny:

  Strategická – analýza rizik, bezpečnostní strategie, plánování investic, …

  Operační – bezpečnostní architektura, modely hrozeb, plány pro red teaming, …

  Taktická – detekční pravidla, konfigurace nástrojů, zaměření threat hunting aktivit, …
- Přínosem TID je tedy (mj.) propojení strategické roviny s praktickou implementací opatření

NETTLES CONSULTING

Modelování hrozeb a rámec MITRE ATT&CK

NETTLES
CONSULTING

Modelování hrozeb

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

Wikipedia

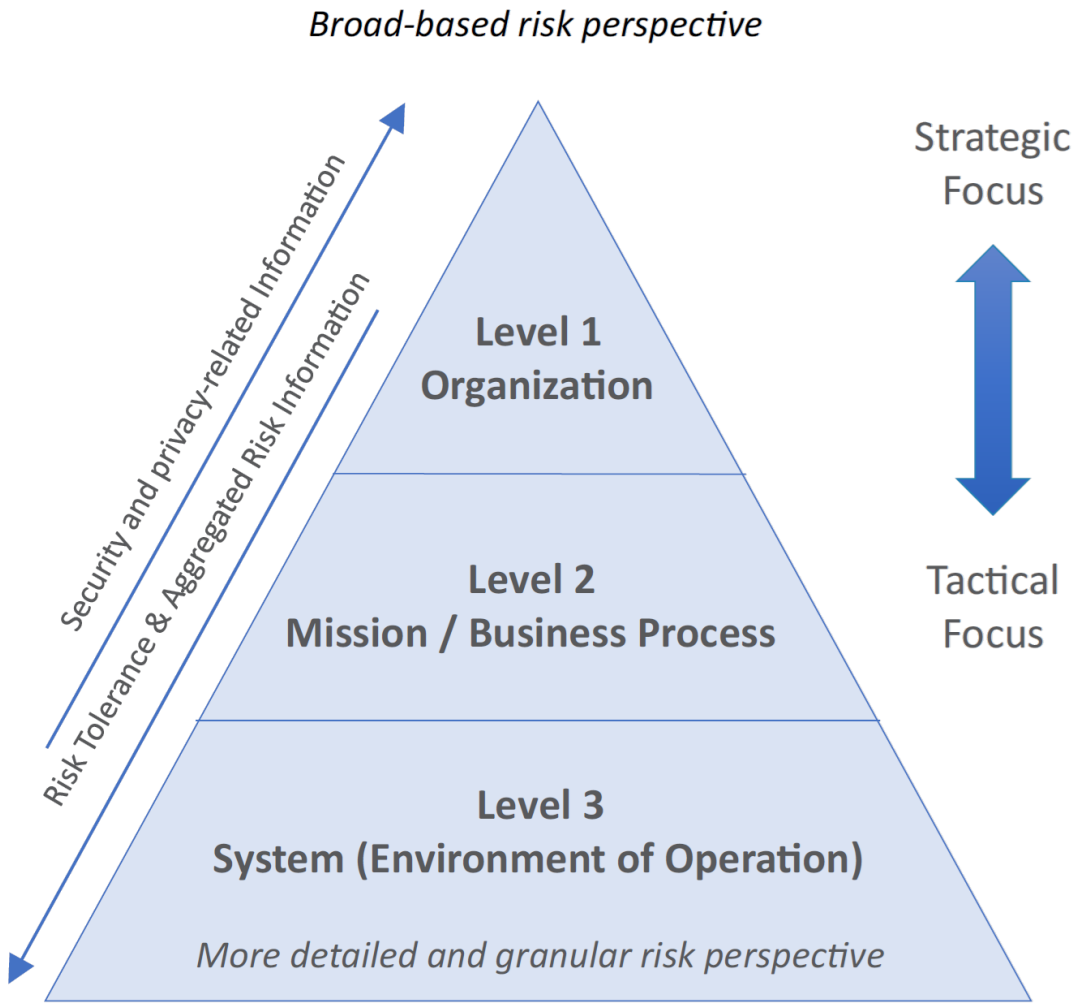
NETTLES CONSULTING

Generický přístup k modelování hrozeb

1. Stanovení rozsahu zájmového systému a jeho dekompozice
2. Identifikace faktorů, které mohou nežádoucím způsobem ovlivnit systém, jeho komponenty nebo interakci těchto komponent
3. Identifikace jednotlivých možných realizací a vektorů spojených s identifikovanými faktory

NETTLES CONSULTING

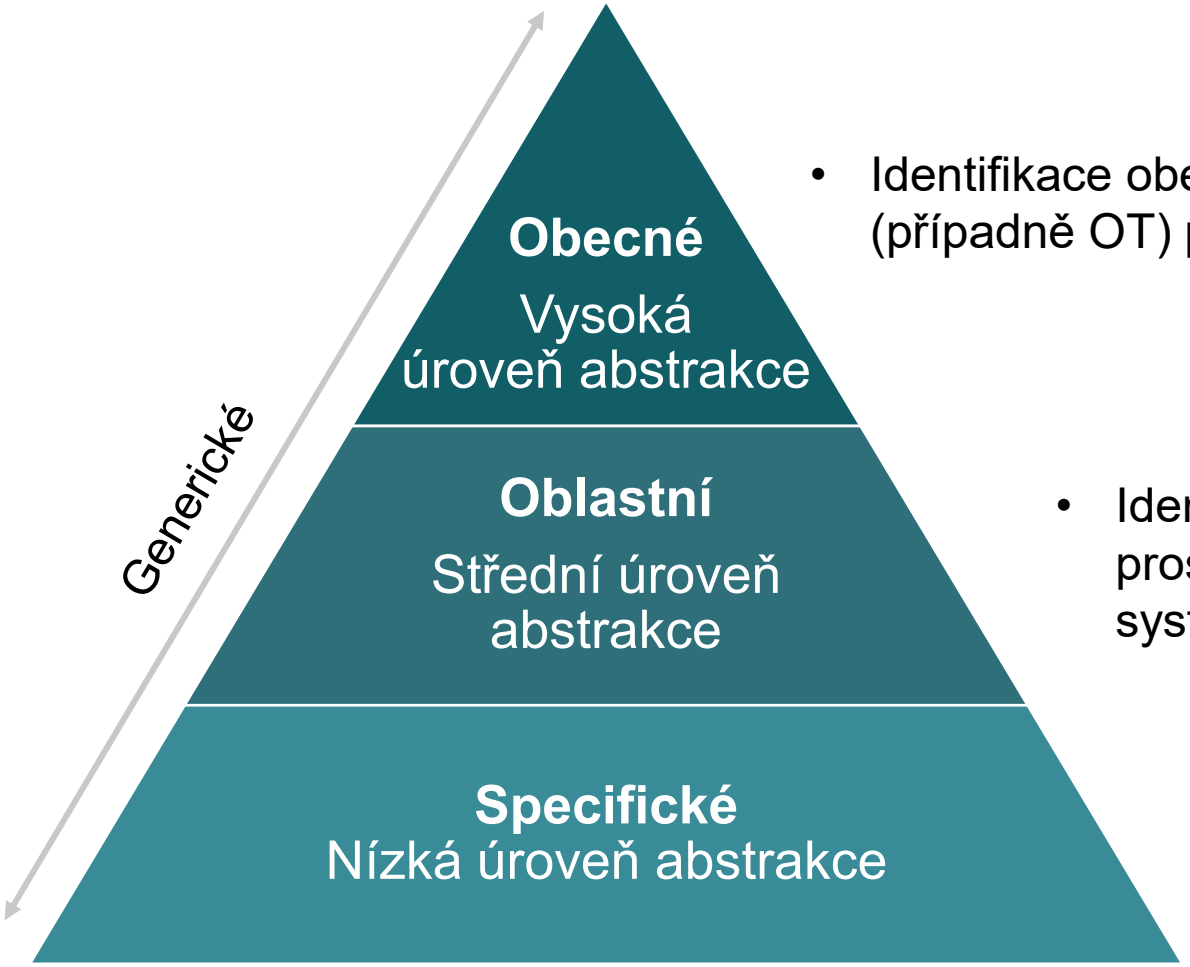
Různé úrovně řízení rizik (nejen) v IT



Zdroj: NIST SP 800-82

NETTLES CONSULTING

Různé metodiky pro modelování hrozeb (nejen) v IT



- Identifikace obecných hrozeb relevantních pro celou organizaci a její IT (případně OT) prostředí a systémy a v nich probíhající procesy

- Identifikace specifických hrozeb pro IT (případně OT) prostředí organizace či širší prostředí určitého „systému systémů“

- Identifikace specifických hrozeb pro konkrétní IT (případně OT) systém, např. specifickou aplikaci apod.

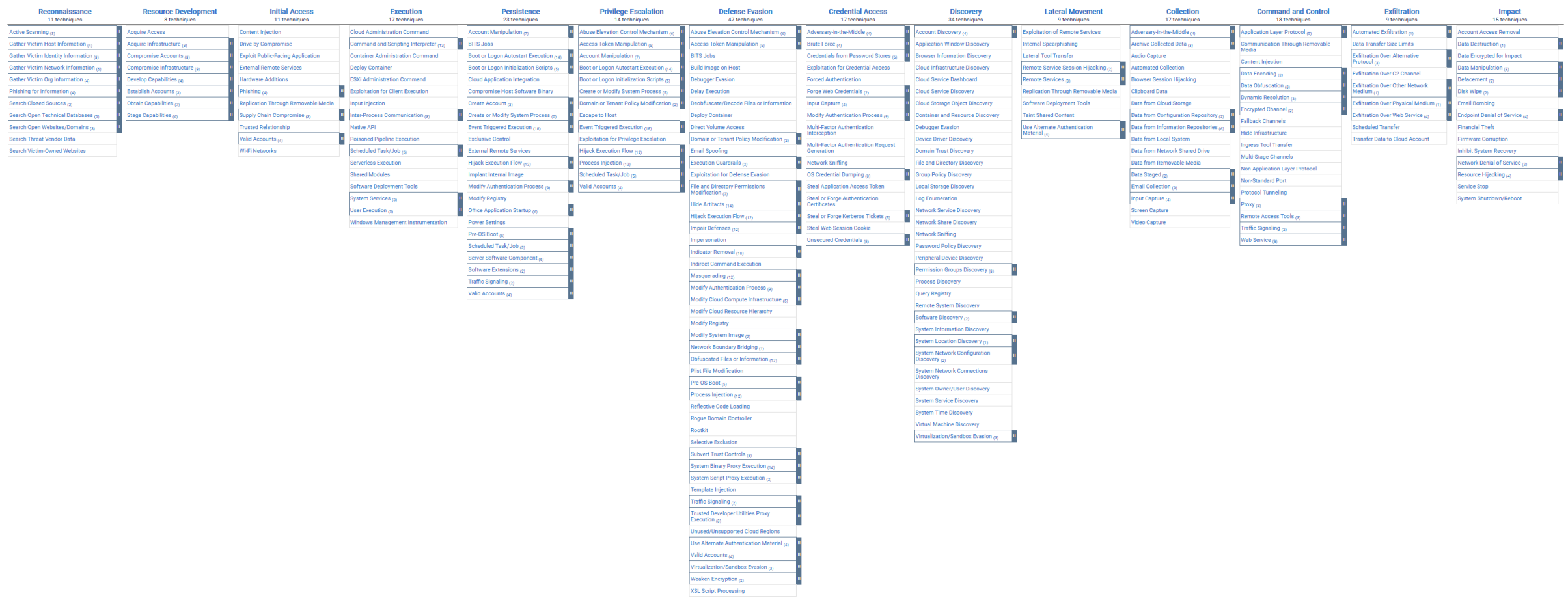
NETTLES CONSULTING

MITRE ATT&CK

- Původně „Adversarial Tactics, Techniques, and Common Knowledge“
  - https://attack.mitre.org/
- Katalog tzv. TTP (taktik, technik a procedur) známých způsobů postupu škodlivých aktérů při útocích
  - Znalostní báze masivně využívaná ze strany bezpečnostní komunity – výrobců technologií i „uživatelů“
- Aktuálně ve verzi 19 obsahující 3 „Matice“ – Enterprise, Mobile a ICS
  - Matice Enterprise obsahuje prokazatelně užívané postupy při útocích na IT prostředí a systémy moderních organizací
  - Matice ICS obsahuje prokazatelně užívané postupy při útocích na OT systémy moderních organizací

NETTLES CONSULTING

MITRE ATT&CK Enterprise



NETTLES CONSULTING

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	11 techniques	3 techniques	14 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	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		

NETTLES CONSULTING

Zdroj: MITRE

MITRE ATT&CK jako nástroj pro modelování hrozeb

- Hrozby relevantní pro určité prostředí je obecně možné mapovat na ATT&CK relativně snadno, pokud známe
  - TTP relevantní vzhledem k jejich využívání ze strany geograficky a sektorově relevantních škodlivých aktérů
  - TTP spojená s incidenty detekovanými ve vlastní organizaci
  - TTP spojená s incidenty detekovanými v obdobných organizacích
  - …
- Relevance technik z rámce ATT&CK je různá pro různé organizace
  - Pro banky v USA jsou relevantní jiné techniky než pro státní správu v Číně
- Pro organizace působící ve stejném sektoru a stejném geografickém regionu je však vždy relevantní i určitá společná množina technik

NETTLES CONSULTING

ATT&CK jako nástroj pro operacionalizaci CTI

- Aby šlo CTI využít i mimo strategickou úroveň, je nutný strukturovaný model pro evidenci hrozeb
- Tuto roli dnes plní v podstatě výhradně MITRE ATT&CK – de facto standard pro popis TTP
  - Umožňuje převést heterogenní CTI vstupy a (vybrané) bezpečnostní potřeby a výstupy z analýzy rizik do jednotné, dále využitelné struktury
- Díky němu je možné:
  - Mapovat CTI reporty z různých zdrojů na techniky relevantní pro organizaci
  - Odvozovat z nich požadavky na detekční a preventivní opatření
  - Měřit pokrytí jednotlivých technik implementovanými opatřeními
  - Kvantitativně řídit rozvoj bezpečnosti podle zjištěných mezer v pokrytí požadavků

NETTLES CONSULTING

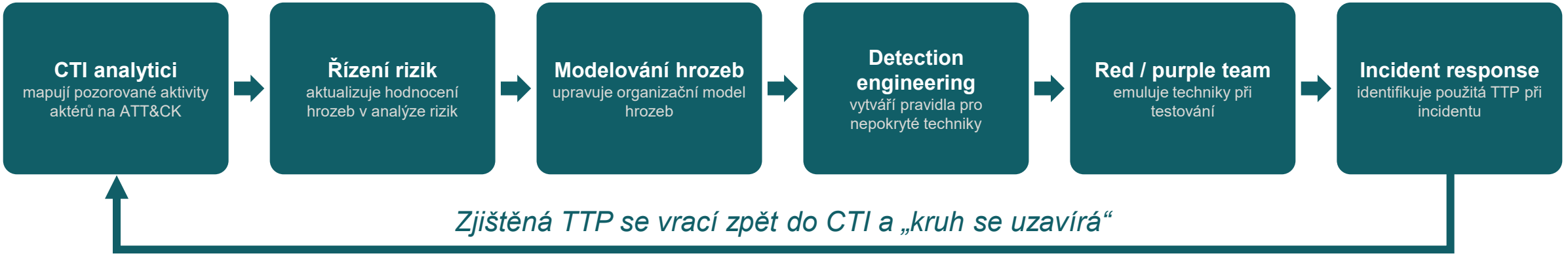
Od obecné hrozby ke konkrétnímu a měřitelnému požadavku

- Generický požadavek: „organizace by měla být schopná detekovat kompromitaci účtů“
  - Něco takového z principu nelze jednoznačně implementovat, prokázat ani otestovat (aneb zkuste takový požadavek dát AD administrátorovi…)
- Požadavek odvozený z modelu hrozeb: „technika T1003.005 – OS Credential Dumping: Cached Domain Credentials je pro nás vysoce relevantní“ – co s tím?
  - Logování – jaké zdroje a jaké konkrétní události z nich musíme agregovat
  - Detekce – konkrétní detekční pravidlo v SIEM či EDR
  - Prevence – konkrétní konfigurace systémů (např. omezení počtu cachovaných údajů)
  - Testování – konkrétní scénář pro emulaci techniky a ověření fungování detekčních i preventivních opatření
- Rozdíl je podstatný: druhý požadavek je **konkrétní**, **implementovatelný**, **testovatelný** a **měřitelný**

NETTLES CONSULTING

ATT&CK jako společný jazyk / „pivot model“

Využití ATT&Cku umožňuje jednotlivým rolím a týmům pracovat se stejným referenčním modelem, byť každý tak bude činit z jiné perspektivy:



ATT&CK ve výše uvedeném příkladu neplní pouze roli klasifikačního rámce – funguje jako „pivot model“, který propojuje jednotlivé bezpečnostní disciplíny a zajišťuje mezi nimi konzistentní tok informací napříč strategickou, operační i taktickou rovinou.
Technika identifikovaná při incidentu se tak přes CTI dostane jak do analýzy rizik, tak i modelu hrozeb a odtud do detekčních pravidel i do plánu testování – a její pokrytí lze následně měřit.

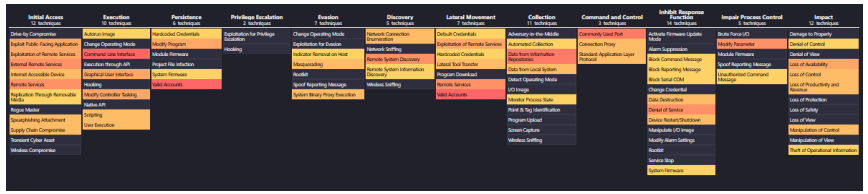
NETTLES CONSULTING

Modely hrozeb od MPO

NETTLES
CONSULTING

Modely hrozeb poskytované ze strany MPO

- Od prosince 2025 připravuje MPO pro české organizace zdarma modely hrozeb založené na rámci MITRE ATT&CK
  - Modely jsou doplněny o metodické materiály detailněji popisující možnosti použití a jsou aktualizovány každých 6 měsíců
  - Pro české organizace obecně je k dispozici model založený na matici Enterprise
  - **Pro sektor energetiky a produktovodů** a **průmyslové organizace obecně** jsou k dispozici modely zaměřené adresně na **průmyslová a specifická prostředí** založené na maticích Enterprise a ICS
  - O přístup k modelům je možné požádat zasláním e-mailu na adresu kb@mpo.gov.cz



NETTLES CONSULTING

Co modely hrozeb od MPO obsahují

- Výběr technik a sub-technik rámce ATT&CK, které lze na základě provedených analýz považovat za aktuálně nejvýznamnější pro české organizace
- Model má podobu „heat mapy“ – numerické skóre 0-100 vyjadřuje relevanci jednotlivých (sub-)technik
  - Je tedy zřejmé, co je vysoce významné a co naopak potenciálně méně problematické
- Vstupy pro stanovení relevance jednotlivých technik:
  - TTP komoditního i dalšího škodlivého kódu relevantního pro prostředí ČR
  - TTP ransomwarových skupin a jimi používaných nástrojů
  - TTP hacktivistických a dalších skupin škodlivých aktérů
  - TTP odpovídající často detekovaným aktivitám a často řešeným typům incidentů v ČR
  - další CTI analýzy vyhodnocující relevanci technik pro prostředí ČR

NETTLES CONSULTING

Co modely hrozeb od MPO obsahují

Name	Date modified	Type	Size
Dilci_modely	22.05.2026 9:02	File folder	
model-cz-26h1-ent.json	22.05.2026 9:04	JSON File	81 KB
model-cz-26h1-ent.svg	22.05.2026 9:04	Microsoft Edge HTML Document	329 KB

Name	Date modified	Type
dilci_model-cz-dalsi_vstupy-26h1-ent.json	22.05.2026 9:04	JSON File
dilci_model-cz-globalni_statistiky-26h1-ent.json	22.05.2026 9:04	JSON File
dilci_model-cz-lotl-26h1-ent.json	22.05.2026 9:04	JSON File
dilci_model-cz-malware-26h1-ent.json	22.05.2026 9:04	JSON File
dilci_model-cz-ransomware-26h1-ent.json	22.05.2026 9:04	JSON File
dilci_model-cz-skupiny-26h1-ent.json	22.05.2026 9:04	JSON File
dilci_model-cz-statistiky_cz-26h1-ent.json	22.05.2026 9:04	JSON File
dilci_model-cz-statistiky_evropa-26h1-ent.json	22.05.2026 9:04	JSON File

NETTLES
CONSULTING

Možnosti využití modelů hrozeb poskytovaných ze strany MPO

- Soubory JSON je možné otevřít v nástroji ATT&CK Navigator (instruktážní video popisující ovládací prvky je k dispozici na https://x90.cz/x/navigator-zaklady)
- Tyto materiály je v návaznosti na vyspělost mechanismů pro řízení kybernetické bezpečnosti v jednotlivých organizacích možné využít mj.:
  - Pro identifikaci případných slabých míst kybernetické bezpečnosti
  - Pro obohacení hodnocení rizik/analýz rizik
  - Pro tvorbu, obohacování a zpřesňování vlastních modelů hrozeb

NETTLES CONSULTING

Praktická část – práce s modelem hrozeb

NETTLES
CONSULTING

ATT&CK Navigator – co to je a jak s ním začít

- Webový nástroj od MITRE pro vizualizaci, anotaci a správu matic ATT&CK
  - K dispozici veřejná instance https://mitre-attack.github.io/attack-navigator/, alternativně možnost spustit instanci lokálně (optimálně v kontejneru)
  - Nástroj běží pouze v prohlížeči a nic neodesílá na server
- Model hrozeb má v Navigatoru podobu tzv. vrstvy („layer“) ve formátu JSON
  - Obsahuje výběr technik, jejich skóre, barvy, komentáře, metadata apod.
- Základní ovládací prvky, které dnes budeme potřebovat:
  - Open Existing Layer – načtení modelu ze souboru nebo z URL
  - Selection controls – výběr a vyhledávání technik, taktik, aktérů a softwaru
  - Layer controls – skóre, barevná paleta, komentáře, export do JSON, Excelu či SVG
  - Technique controls – zobrazení, filtrování a skrývání technik

NETTLES CONSULTING

Vrstvy (layers) a jejich kombinování

- Klíčová vlastnost Navigatoru: nad vrstvami lze provádět jednoduché aritmetické operace
- Typický pracovní postup v rámci threat-informed defense:
  - Vrstva a – model hrozeb, tedy relevance technik (např. model od MPO)
  - Vrstva b – model pokrytí prostředí stávajícími preventivními opatřeními
  - Vrstva c – pokrytí prostředí detekčními scénáři v SIEM či EDR
- Nová vrstva „a - b - c“ ukáže mezery v pokrytí vážené relevancí hrozby (a případně efektivitou bezpečnostních opatření)
- Od modelu hrozeb se tak dostáváme k prioritizovanému seznamu bezpečnostních potřeb na úrovni TTP
  - Vrstvy je vhodné verzovat – model hrozeb ani modely opatření nesmí být statické

NETTLES CONSULTING

Cvičení 1: Interpretace modelu hrozeb (nejen) v kontextu analýzy rizik

- Zadání:
  - Otevřete celkový model hrozeb v ATT&CK Navigatoru
  - Zorientujte se ve skórování a určete které (sub-)techniky mají nejvyšší relevanci
  - Vyberte 5 nejvýše hodnocených technik a projděte si jejich popis na attack.mitre.org
- Otázky k diskusi:
  - Odpovídá relevance technik prioritním hrozbám z vaší analýzy rizik, nebo vaší představě o hrozbách pro vaši organizaci?
  - Které techniky byste na základě vlastní zkušenosti považovali za podstatnější a proč?
  - Které taktiky jsou v modelu zastoupeny nejsilněji a co to o hrozbách vypovídá?

NETTLES CONSULTING

Cvičení 2: Přizpůsobení modelu vlastní organizaci

- Model od MPO je univerzální výchozí bod – rozsah zájmového prostředí ani jeho specifika za nás nikdo nevymezí
- Zadání:
  - Vytvořte dodatečnou vrstvu mapující TTP související s riziky relevantními pro vaší organizaci
  - Na základě jednoduché OSINT analýzy (čtěte „pokud nevíte, zeptejte se Googlu“) vytvořte dodatečnou vrstvu mapující TTP související s alespoň 3 skupinami škodlivých aktérů relevantními pro vaší organizaci
  - Vytvořte specifický model hrozeb pro vaší organizaci ze všech dostupných dílčích modelů a dvou výše zmíněných modelů specifických pro vaší organizaci
    - Zajistěte, aby tento model obsahoval skóry v rozsahu 0-100

NETTLES CONSULTING

Cvičení 3: Mapování stávajících opatření

- Zadání:
  - Vytvořte novou vrstvu a vyberte v ní s pomocí mechanismu Search and Multiselect všechna preventivní opatření (Mitigations), která ve své organizaci máte zavedena alespoň na části infrastruktury a souvisejícím technikám nastavte skóre na 1
  - S pomocí mechanismu Search and Multiselect následně vyberte jen ta preventivní opatření (Mitigations), která ve své organizaci máte zavedena **plošně a plně** a souvisejícím technikám nastavte skóre na 2

NETTLES CONSULTING

Cvičení 4: Identifikace mezer a prioritizace

- Zadání:
  - Vytvořte novou vrstvu vhodnou kombinací vrstvy modelu hrozeb a vrstvy pokrytí (např. „a - (b*10)“ nebo „a - (b*25)“ apod.)
    - Výsledkem bude vrstva u níž jsou nejprioritnější techniky s vysokou relevancí a nízkým pokrytím – tedy významné mezery
  - Vyberte 5 nejvýznamnějších technik a pro každou formulujte:
    - Vhodné opatření pro její preventivní pokrytí (je-li preventivní pokrytí možné)
    - Jaká by byla odhadovaná náročnost implementace opatření
    - Jak byste ověřili, že daná technika by byla efektivně pokryta
- Řečnická otázka:
  - Kolik z těchto „mezer“ na úrovni TTP by odhalila běžná gap analýza podle ISO, ZoKB nebo jiné normy?

NETTLES CONSULTING

Jak na zavedení TID v reálné organizaci

NETTLES
CONSULTING

Od mezer v pokrytí k rozvoji bezpečnosti

- Výše uvedený postup je pouze vzorový a v praxi by nedával smysl – pro využití na úrovni plného TID je potřeba jít do podstatně větší hloubky a **dynamicky** rozlišovat různé typy pokrytí u různých typů systémů a prostředí organizace
  - Servery s Linuxem v DMZ jsou zcela jistě pokryté jinak, než router v OT prostředí nebo uživatelský laptop obchodníka apod.
- Identifikované „mezery“ na úrovni detekčních i preventivních opatření by v takovém případě byly vhodným vstupem pro konkrétní, technicky formulovaný požadavek na:
  - Doplnění či rekonfiguraci preventivního opatření
  - Doplnění detekčního scénáře do SIEM či EDR včetně potřebných logovacích zdrojů
  - Zavedení nebo úpravu procesu apod.
- Cílem není nikdy 100% pokrytí ATT&Cku, ale maximální pokrytí toho, co je pro nás relevantní

NETTLES CONSULTING

Jak zavést základní threat-informed defense v organizaci

- Zavedení základních TID principů nevyžaduje okamžitou transformaci systémů ani architektury – vhodný je iterativní přístup:
  1. Vytvořit základní model hrozeb z CTI vstupů a analýzy rizik (např. z modelů MPO)
  2. Vymezit rozsah a přizpůsobit model vlastnímu prostředí
  3. Namapovat existující bezpečnostní (preventivní i detekční) opatření na rámec ATT&CK
  4. Identifikovat a prioritizovat zjištěné mezery v pokrytí
  5. Postupně rozšiřovat pokrytí a granularitu a zpřesňovat modely
  6. Průběžně modely aktualizovat podle nových CTI vstupů, incidentů, výsledků testů apod.
- I hrubé rozlišení vysoce a méně relevantních technik má významnou přidanou hodnotu
  - Klíčové však je, aby výchozí model hrozeb, ani žádný model opatření nebyl statický

NETTLES CONSULTING

Limity threat-informed defense a rámce ATT&CK

- ATT&CK je relativně vyčerpávající na úrovni obecných technik chování útočníků, principiálně však nemůže pokrývat vše:
  - Nepracuje s naturogenními hrozbami (požár, povodeň, …)
  - Konceptuálně v něm chybí některé specifické aplikační scénáře
  - Nepokrývá hrozby s dopadem na vybrané „businessové“ aspekty systémů a procesů
- Kompenzace v praxi může být použití doplňkových modelů hrozeb (definovaných např. s pomocí STRIDE) pro kritické systémy
  - Nejde o nativní součást koncepce threat-informed defense, spíše racionální přístup k pokrytí potenciálních mezer
- Druhou slabinou je významná závislost na kvalitě dostupných CTI vstupů
  - Na strategické úrovni obecnější vstupy zpravidla dostačují
  - Při detailní specifikaci potřeb (např. v oblasti monitoringu) jsou jejich nedostatky významným problémem

NETTLES CONSULTING

Od Navigatoru k enterprise nástroji pro řízení TID

- Navigator je výborný pro seznámení s konceptem a pro první iterace, v běžném provozu však naráží:
  - Správa desítek vrstev formou JSON souborů, chybějící verzování a řízení přístupu
  - Omezené možnosti reportingu a sledování vývoje pokrytí v čase
  - Absence vazby na konkrétní prostředí, aktiva, opatření, analýzu rizik apod.
- Aktuálně proto vyvíjíme nástroj pro pokročilé modelování hrozeb a měření jejich pokrytí na základě rámce ATT&CK
  - Enterprise-ready platforma pro řízení threat-informed defense
  - Řada pokročilých funkcí nad rámec možností Navigatoru
- Dostupnost je plánována v průběhu příštího roku – pokud by vás takový nástroj zajímal, sledujte stránky https://threatcore.cz/

NETTLES CONSULTING

Shrnutí – co si odnést

- Generické hrozby vedou ke generickým a neprokazatelně účinným opatřením
- Threat-informed defense staví bezpečnost na znalosti reálných hrozeb
  - Nenahrazuje řízení rizik, ale propojuje ho s technickou realitou
- ATT&CK umožňuje prakticky využít CTI a je společným jazykem bezpečnostních týmů
- Model hrozeb je nutný výchozí bod – nemusíte ho však tvořit od nuly
  - MPO českým organizacím poskytuje „základ“ bezplatně – stačí napsat na kb@mpo.gov.cz
- Měření pokrytí modelu hrozeb může být rozumný přechod od stavu „splnili jsme normu“ k „umíme prokázat, že naše bezpečnostní opatření reálně pokrývají technická specifika relevantních hrozeb“
  - První, jednoduchou iteraci zvládnete s prohlížečem, Navigatorem a jedním odpolednem, pro komplexnější přístup však počítejte s potřebou větší časové investice

NETTLES CONSULTING

Je pro vás problematika modelování hrozeb s pomocí rámce ATT&CK relevantní

- Pak pro Vás máme několik specializovaných školení – mj.:
  - Modelování hrozeb prakticky
  - Taktiky, techniky a postupy škodlivých aktérů v praxi (školení zaměřené na praktické možnosti použití rámce MITRE ATT&CK)

- Všechna školení najdete na https://www.nettles.cz/security/cz/training

- Pokud s námi chcete zůstat v kontaktu a získat přístup k zajímavým informacím nebo např. slevám na vybraná školení, můžete se tamtéž přihlásit k odběru našeho newsletteru

NETTLES CONSULTING

Q&A

NETTLES CONSULTING

Děkuji Vám za pozornost!

NETTLES CONSULTING