



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



KOMPETENČNÉ CENTRUM
KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Spravodajstvo o hrozbách (CTI)

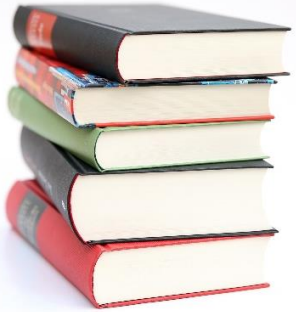
Moderné technológie, bezpečnosť cloudu a IoT (Blok VII)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, <https://kc.uniza.sk/>

Jana.Uramova@fri.uniza.sk



Obsah

- CTI (Cyber Threat Intelligence) ako spravodajská služba o kybernetických bezpečnostných hrozbách
- Možnosti pre zber, analýzu a využívanie informácií o kybernetických hrozbách s cieľom zlepšiť bezpečnostné opatrenia a reakcie na incidenty
- CTI platformy ktoré pomáhajú predvídať, identifikovať a reagovať na potenciálne hrozby tým, že poskytujú aktuálne a relevantné informácie o taktikách, technikách a postupoch útočníkov



Úvod

Cyber Threat Intelligence

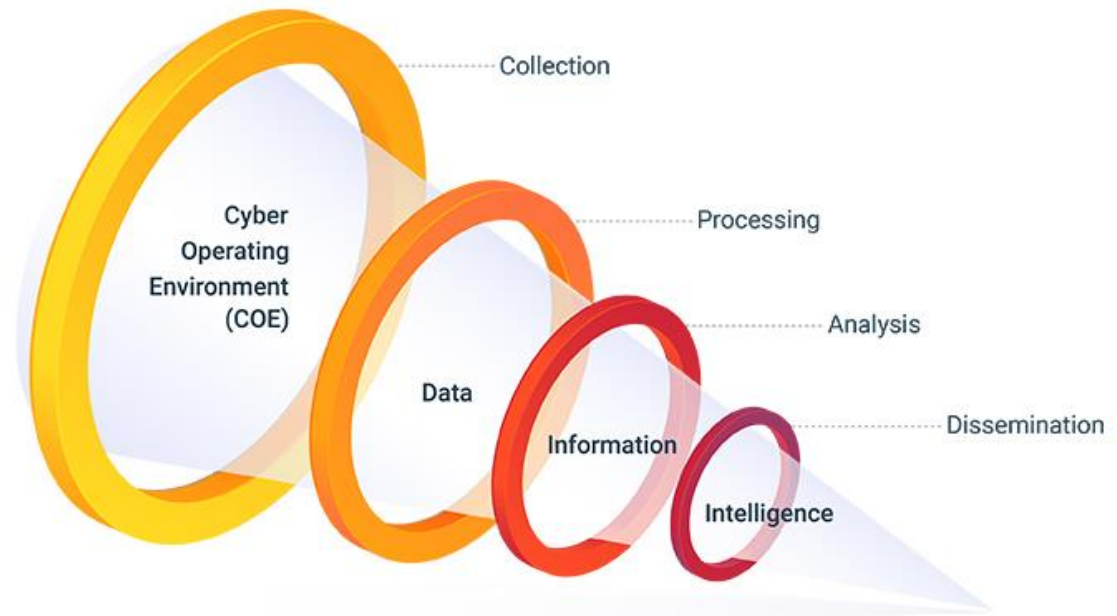
- **CTI (Cyber Threat Intelligence)** je proces zberu, analýzy a interpretácie informácií o kybernetických hrozbách s cieľom pochopiť, kto útočí, ako útočí, prečo útočí a aký dopad môže mať útok na organizáciu.
- **Na čo sa CTI používa:**
 - zlepšenie detekcie v SIEM/EDR
 - rýchlejšia reakcia na incidenty (Incident Response)
 - threat hunting a proaktívne vyhľadávanie hrozieb
 - prioritizácia zraniteľností podľa aktuálneho ohrozenia
 - tvorba bezpečnostných politík a plánovanie investícií
 - posilnenie celkovej kybernetickej odolnosti organizácie



CTI v SOC

- **CTI (Cyber Threat Intelligence)** zásadne zvyšuje efektivitu SOC tím, že poskytuje **kontext** a **význam** k technickým udalostiam, ktoré by inak vyzerali ako bežný šum
- **1. Obohacovanie alertov**
 - CTI pridáva význam ku každému záznamu v SIEM/EDR
 - SOC ihneď vidí, či IP, doména alebo hash patrí:
 - známej APT skupine
 - aktívnej kampani
 - malvéru alebo botnetu
 - Znižuje počet falošných poplachov a zrýchľuje analýzu
- **2. Prioritizácia incidentov**
 - SOC dáva najväčšiu prioritu incidentom spojeným s reálnou hrozbou
 - CTI umožňuje zoradiť incidenty podľa rizika, nie podľa času
- **3. Zlepšenie detekcie (Detection Engineering)**
 - CTI poskytuje TTP techniky z MITRE ATT&CK a i.
 - SOC z nich tvorí nové detekčné pravidlá a korelačné scenáre
 - Zlepšuje pokrytie obrany a odhaľovanie pokročilých útokov

Relationship of Data, Information, and Intelligence



CTI v SOC

4. Threat Hunting

- CTI umožňuje SOC-u loviť hrozby ešte predtým, než spôsobia incident:
 - hunting podľa IOC (IP, hash, doména)
 - hunting podľa TTP útočníkov
 - preverovanie stôp aktívnych kampaní v logoch

5. Rýchlejšia reakcia na incidenty (IR)

- CTI poskytuje odporúčania, analýzy malvéru a predchádzajúce prípady útokov
- SOC okamžite/rýchlejšie rozpozná útočníka alebo kampaň
- Znižuje čas potrebný na izoláciu a blokovanie útoku

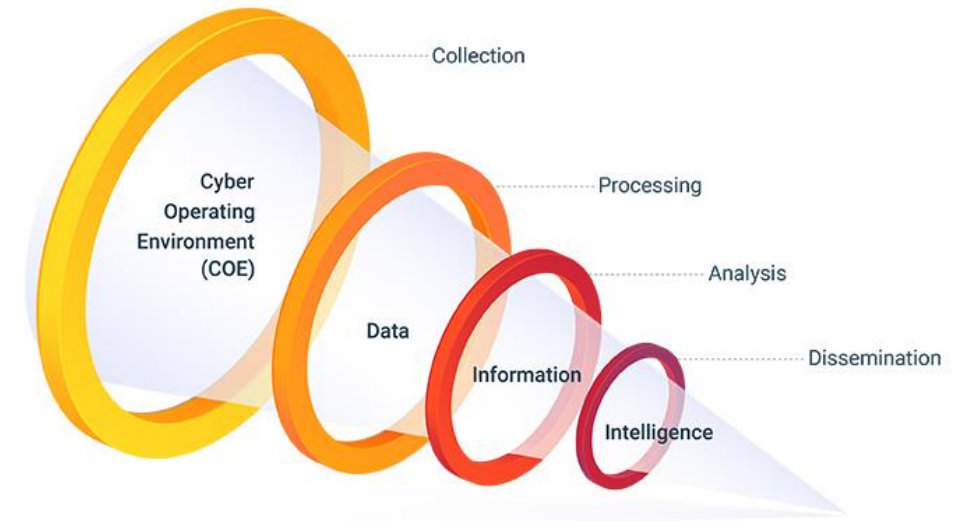
6. Identifikácia aktérov a ich správania

- SOC vie, *kto* útočí, *prečo*, *aký má cieľ* a *aké techniky použije ďalej*
- Umožňuje predvídať ďalšie kroky útočníka

7. Proaktívna obrana

- CTI poskytuje IOC, ktoré možno blokovať ešte predtým, než sú zaznamenané v logoch
- SOC môže zaviesť mitigácie vopred, nie až po útoku

Relationship of Data, Information, and Intelligence





Typy CTI

Threat Intelligence

1. Strategické CTI

„Kto“ a „Prečo“

2. Operačné CTI

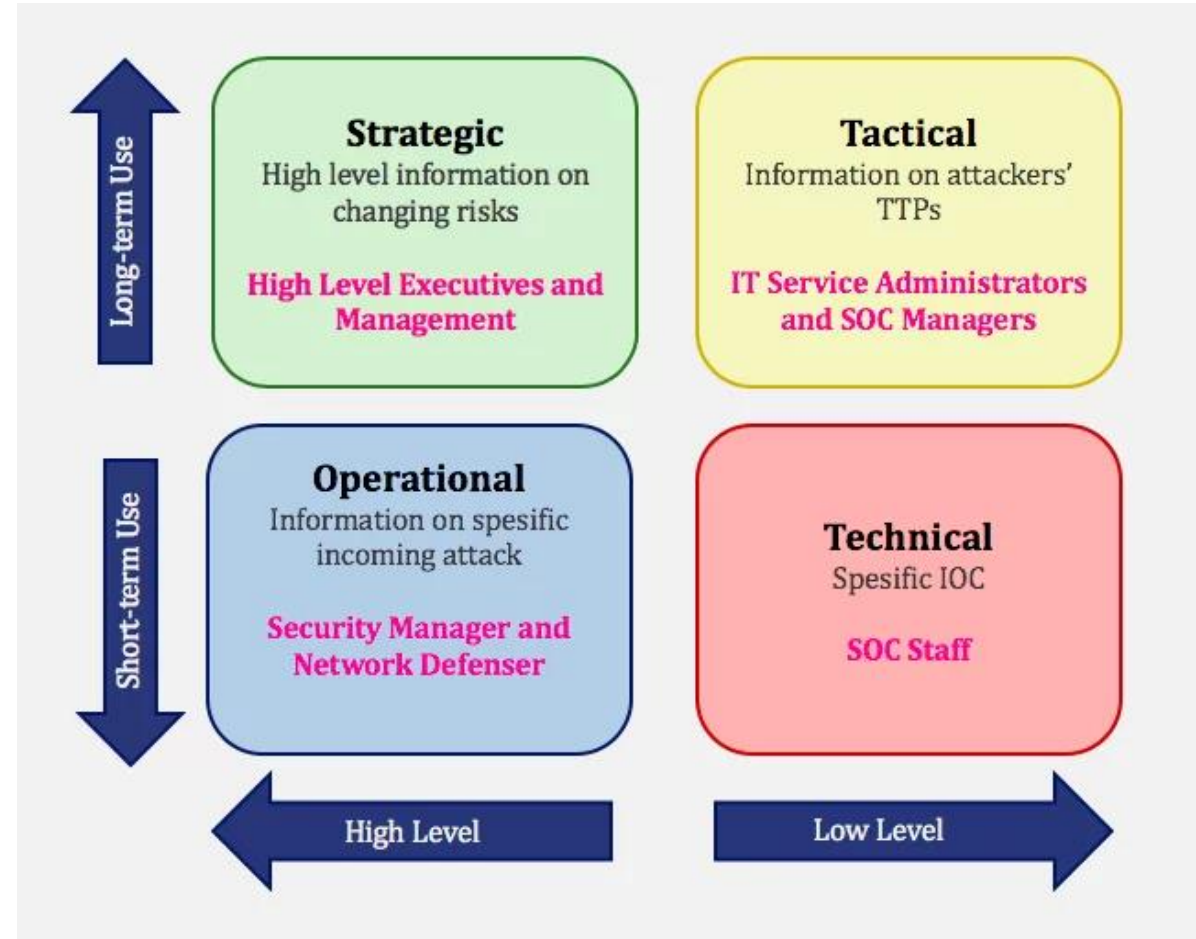
„Kedy?“ a „Kde?“ a „Ako prebieha útok?“

3. Taktické CTI

„Ako útočník postupuje?“

4. Technické CTI

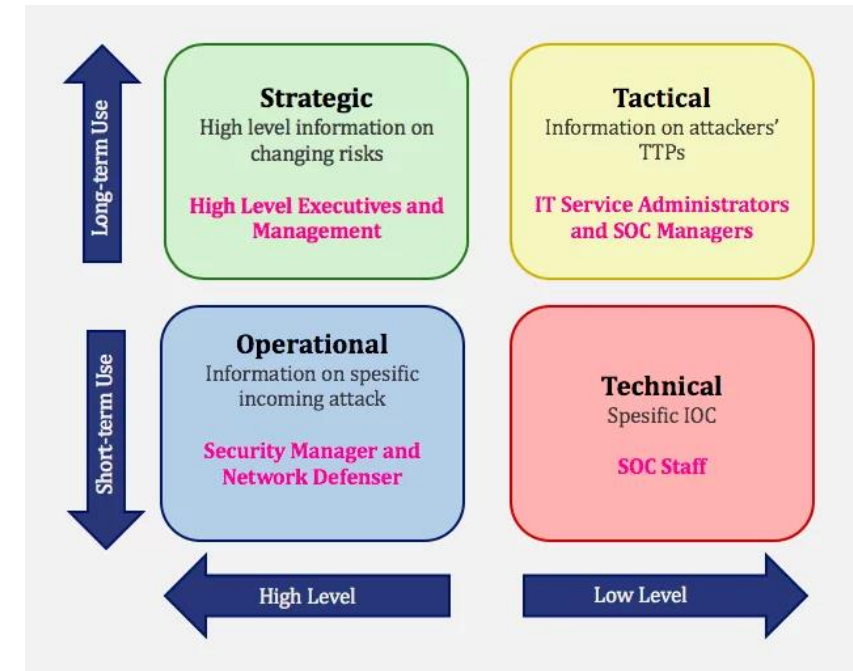
„Čo vidíme?“



Strategické CTI



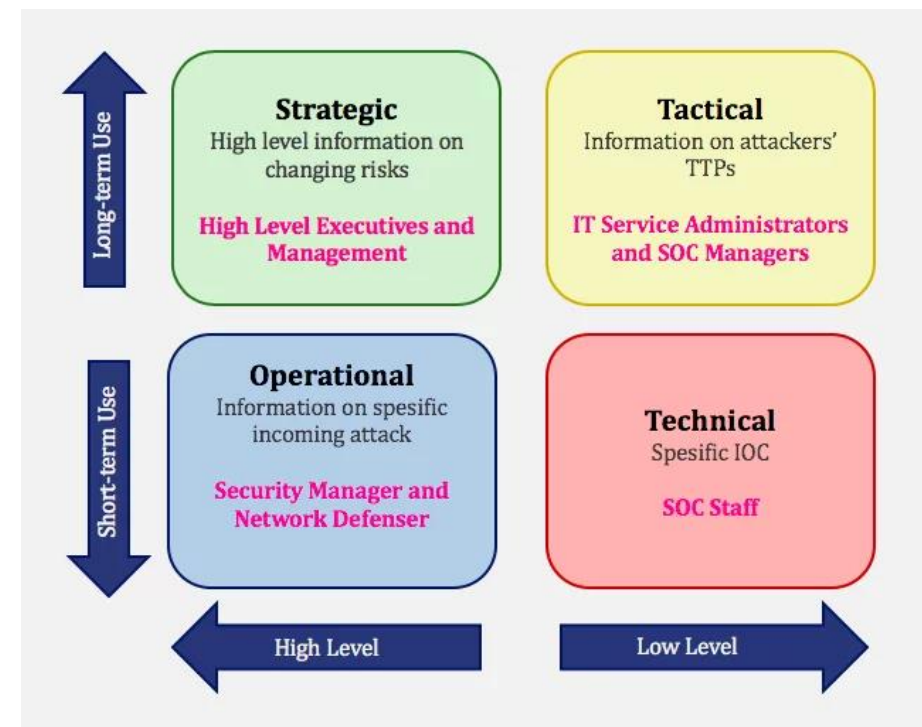
- **Zabezpečuje dlhodobý prehľad hrozieb a trendov**
 - poskytuje vysokoúrovňové a kontextové informácie, ktoré pomáhajú vedeniu organizácie robiť rozhodnutia o bezpečnostných investíciách, prioritách a dlhodobých stratégiách.
- **Kto ho využíva:**
 - manažment organizácie
 - vedenie bezpečnosti (CISO, CSO)
 - rozhodovacie orgány, štátna správa
- **Zameranie:**
 - geopolitické súvislosti a aktivity štátnych/organizovaných skupín
 - dlhodobé kampane APT aktérov a ich motivácie
 - analýza trendov v malvérovom ekosystéme a zločineckých skupinách
 - riziká pre kritické sektory (energetika, zdravotníctvo, verejná správa)
- **Časový horizont:**
 - mesiace až roky
- **Výstupy:**
 - strategické bezpečnostné reporty
 - odporúčania pre rozpočet, modernizáciu, legislatívu a politiku KB
 - hodnotenie dopadov nových technológií (AI, IoT, cloud)
- **Cieľ:**
 - podporiť dlhodobé strategické rozhodovanie a zlepšiť odolnosť organizácie.



Operačné CTI



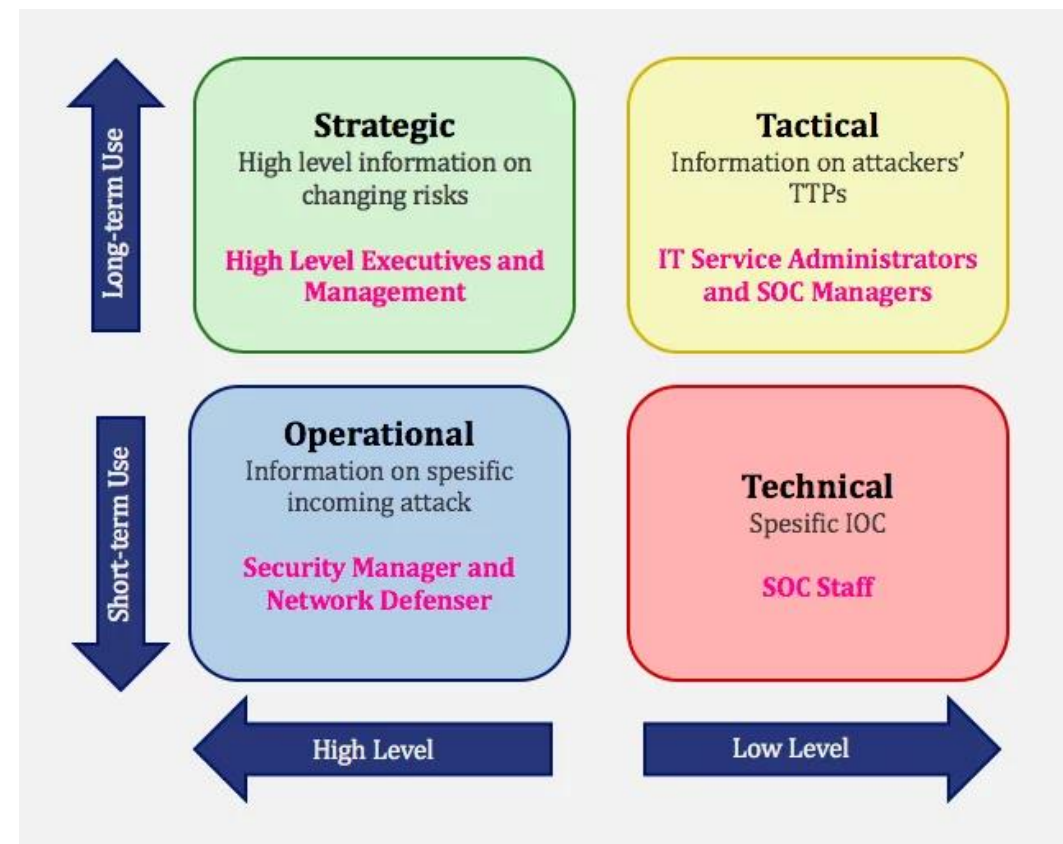
- **Pehľad prebiehajúcich kampaní a aktérov**
 - zameriava sa na to, čo sa deje práve teraz – poskytuje aktuálny obraz o prebiehajúcich hrozbách, kampaniach a útočnických technikách.
- **Kto ho využíva:**
 - Analytici SOC L2/L3
 - Incident Response tímy
 - Threat hunters
 - Manažéri bezpečnosti
- **Zameranie:**
 - identifikácia aktívnych phishingových, ransomware alebo APT kampaní
 - informácie o používaných exploitoch, nástrojoch a zraniteľnostiach
 - analýza útočníkov: motivácia, cieľové sektory, postupy
 - sledovanie novej infraštruktúry útočníkov (C2 servery, domény)
- **Časový horizont:**
 - dni až týždne
- **Výstupy:**
 - odporúčania pre IR
 - IOC/TTP pre SOC
 - situačné správy o prebiehajúcich útokoch
 - informácie pre patch management (aké CVE sú aktívne zneužívané)
- **Cieľ:**
 - umožniť rýchle pochopenie aktuálnej hrozby, zrýchliť reakciu na incident a zlepšiť pripravenosť SOC.



Taktické CTI



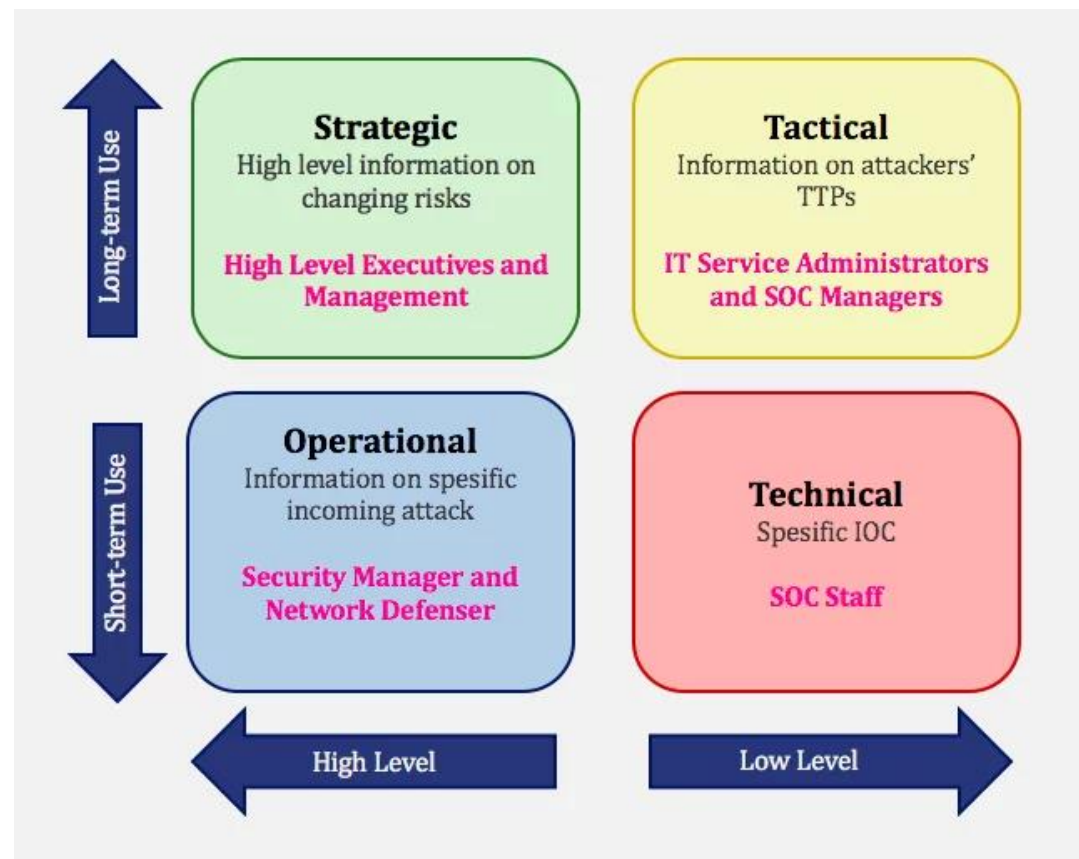
- **Zameranie na TTP (Tactics, Techniques and Procedures) útočníkov**
 - Taktické CTI poskytuje detailný pohľad na konkrétne taktiky, techniky a postupy (TTP), ktoré útočníci používajú.
 - Najčastejšie vychádza z MITRE ATT&CK.
- **Kto ho využíva:**
 - SOC analytici
 - bezpečnostní inžinieri
 - tvorcovia detekčných pravidiel (SIEM, EDR)
 - red team / threat hunting tímy
- **Zameranie:**
 - ako útočník postupuje po zneužití zraniteľnosti
 - techniky laterálneho pohybu, privilege escalation, credential dumping
 - aké logy a udalosti zachytia jednotlivé techniky
 - odporúčania na detekciu a mitigáciu
 - analýza behaviorálnych vzorcov útočníkov
- **Časový horizont:**
 - hodiny až dni
- **Výstupy:**
 - nové korelačné pravidlá a detekčné scenáre
 - mapovanie bezpečnostného pokrytia podľa ATT&CK
 - playbooky pre SOC/IR
 - odporúčania pre hardening a monitoring
- **Cieľ:**
 - zlepšiť detekciu, viditeľnosť a odhalenie aktivít útočníkov ešte pred incidentom.





Technické CTI

- **Nízkoúrovňové a rýchlo sa meniace informácie – technické indikátory**
 - obsahuje detailné a krátkodobé technické indikátory, ktoré sa využívajú v automatizovaných systémoch.
- **Kto ho využíva:**
 - SIEM/EDR systémy
 - firewall/IDS/IPS nástroje
 - SOC L1 analytici
 - automatizačné nástroje a CTI platformy (MISP, OTX, ThreatStream...)
- **Zameranie:**
 - IOC (Indicators of Compromise):
 - škodlivé IP adresy, domény, URL
 - hash-e súborov (MD5/SHA256)
 - JA3 TLS fingerpriny
 - e-mailové indikátory (odchádzajúce adresy, spam vzory)
 - technické indikátory z malvéru (C2 adresy, mutexy, registry)
 - pravidlá pre YARA, Snort/Suricata, Sigma
- **Časový horizont:**
 - minúty až dni (krátka životnosť)
- **Výstupy:**
 - automatizované blokovanie v perimetrovej ochrane
 - alerting v SIEM
 - Obohacovanie udalostí počas analýzy
 - IOC feedy pre zoznamy blokovania
- **Cieľ:**
 - Okamžite reagovať na identifikované hrozby a minimalizovať čas medzi detekciou a mitigáciou.

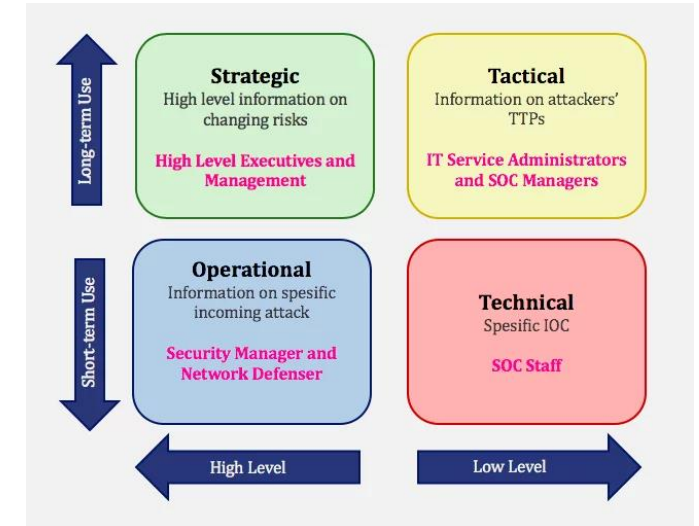




Databázy využívané v CTI nástrojoch

Kategorizácia CTI databáz

- CTI databázy a znalostné bázy možno rozdeliť do štyroch hlavných kategórií podľa typu informácií, ktoré poskytujú:
 - Databázy taktík a techník (TTP)**
 - popisujú správanie útočníkov, techniky, postupy, t.j. dlhodobé, behaviorálne informácie
 - Príklady : MITRE ATT&CK, CAPEC, MAEC
 - Databázy zraniteľností a slabín**
 - poskytujú informácie o konkrétnych technických slabínach a ich zneužitelnosti.
 - Príklady: CWE, CVE, NVD
 - Malvérové databázy**
 - Zaoberá sa vzorkami malvéru, technickými indikátormi, analýzou jeho správania
 - Príklady: MalwareBazaar, VirusTotal, ANY.RUN, Hybrid Analysis
 - IOC databázy**
 - Zaoberá sa krátkodobými indikátormi kompromitácie pre detekciu v reálnom čase.
 - Príklady: MISP, OTX, ThreatFox, Feodo Tracker, URLhaus
 - Databázy/platformy poskytujúce strategické informácie (trendy, aktérov, kampane, geopolitické súvislosti)



Reporty a platformy poskytujúce strategické informácie

Prečo strategické CTI „nemá databázy“ ako iné typy CTI?

- Pretože:
 - Strategická CTI sa rýchlo vyvíja, hodnotí **zámer, motiváciu a geopolitický kontext**, nie technické parametre
 - Nedá sa pevne štruktúrovať ako „hash – IP – doména“
 - Ide o **správy, analýzy, mierové a vojenské aktivity, ekonomické ukazovatele, trendy kampaní**
- Tieto platformy poskytujú strategické informácie: trendy, aktérov, kampane, geopolitické súvislosti:
 - **1. ENISA Threat Landscape (ETL)**
 - Európska agentúra pre kybernetickú bezpečnosť
 - Strategické prehľady, trendy, budúce hrozby
 - ročné správy + pravidelné analytické výstupy
 - **2. Verizon DBIR (Data Breach Investigations Report)**
 - Najpoužívanejší strategicko-operatívny report
 - Štatistiky útokov, motivácie, trendy v sektoroch
 - **3. Mandiant / Google Cloud Threat Intelligence Reports**
 - Analýzy APT skupín, geopolitické kampane, ekonomická motivácia
 - Strategické odporúčania a predikcie
 - **4. CrowdStrike Global Threat Report**
 - Ročný strategický prehľad aktérov, trendov a kampaní
 - Zamerané na národné štáty, kyberšpionáž a ransomware
 - **5. Recorded Future – Intelligence Cloud**
 - Jedna z mála platforiem, ktorá má *reálnu CTI databázu*
 - Strategické, operačné aj technické CTI v jednom
 - AI-analýzy trendov, geopolitické hrozby
 - **6. Microsoft Digital Defense Report**
 - Strategická úroveň – štátni aktéri, trendy, budúce riziká
 - **7. IBM X-Force Threat Intelligence Index**
 - Strategické trendy, ekonomické dopady, predikcie

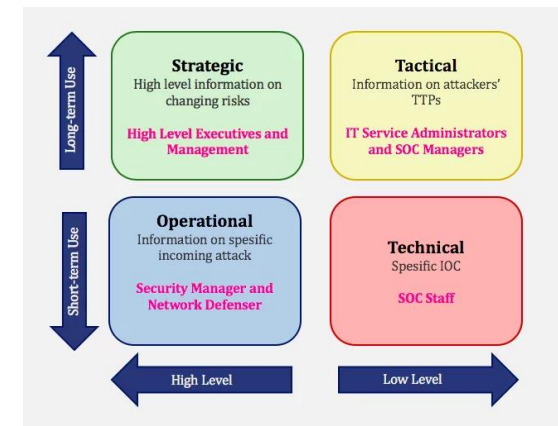


Databázy hrozieb a TTP

Pre zdieľanie informácií o hrozbách (útoky, malvér, ...)

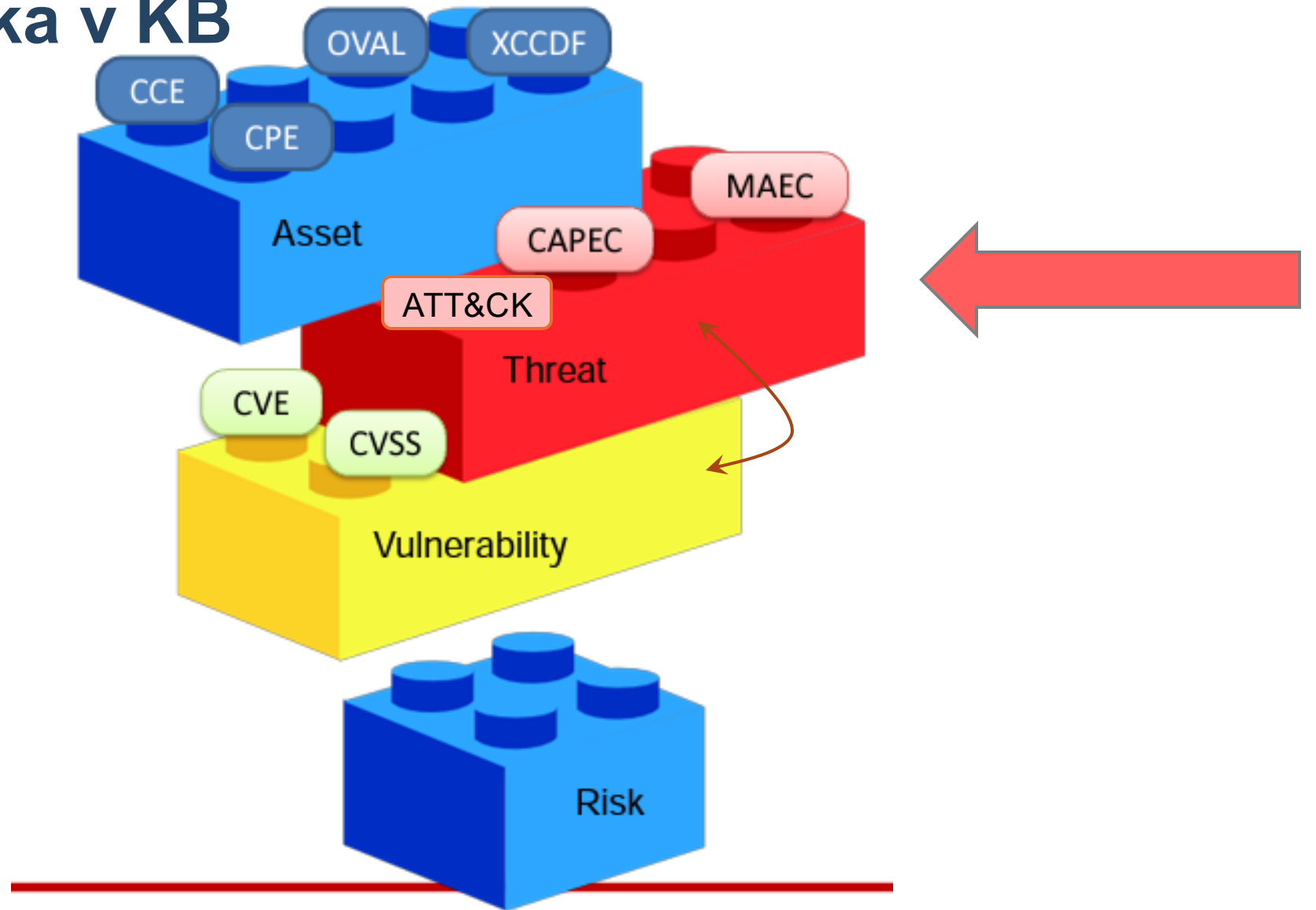
Ako popísať vzory útočných vektorov?

Aké štandardy a nástroje sú dostupné pre popis hrozieb?



Známa skladačka v KB

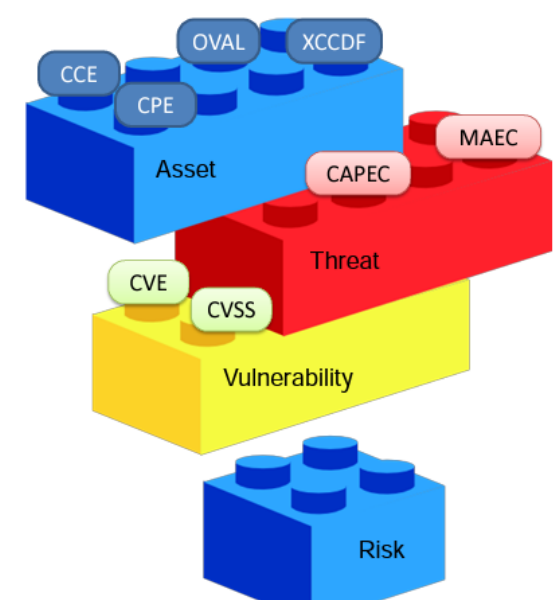
- Zameriame sa na hrozby
- Vulnerability a Threat by mali mať opačné poradie



Common Attack Pattern Enumeration and Classification

CAPEC

- Zdieľaný štandard indexovania pre bežné vzory útokov používané pri zneužitíach alebo malvéri
 - Databáza *útokových vzorov* – opisuje **spôsoby, ako môže útočník zaútočiť**, napr. „SQL Injection“, „Privilege Escalation“ alebo „Phishing“
 - Popis na vyjadrenie útočných vektorov
- Penetration Testing Management Platforms
 - využívajú CAPEC na mapovanie do Attack Chains, ktoré môžu byť tiež prepojené s rámcom MITRE ATT&CK
 - Aby poskytli úplný obraz
- Celkový počet vzorov útokov: 559 (zoznam ver. 3.9)
- Slúži pre threat modeling, vzdelávanie, penetračné testovanie alebo integráciu do TI platforiem.



Príklady známych vzorov útokov:

- HTTP Response Splitting ([CAPEC-34](#))
- Session Fixation ([CAPEC-61](#))
- Cross Site Request Forgery ([CAPEC-62](#))
- SQL Injection ([CAPEC-66](#))
- Cross-Site Scripting ([CAPEC-63](#))
- Buffer Overflow ([CAPEC-100](#))
- Clickjacking ([CAPEC-103](#))
- Relative Path Traversal ([CAPEC-139](#))
- XML Attribute Blowup ([CAPEC-229](#))

<https://capec.mitre.org/community/usage.html>

Integrácie CAPEC



Hlavné typy nástrojov, ktoré CAPEC využívajú:

1. Threat Modeling Tools

- **Microsoft Threat Modeling Tool** – integruje CAPEC attack patterns na podporu analýzy a identifikácie hrozieb.
- **OWASP Threat Dragon** – pri modelovaní útokov môže využiť CAPEC vzory pre kategorizáciu útokov.
- **IriusRisk** – komerčný nástroj pre threat modeling, podporuje CAPEC pre identifikáciu a klasifikáciu hrozieb.

2. Penetračné testovanie / Red Team Tools

- Niektoré komerčné penetračné testovacie platformy alebo simulátory útokov (napr. **Core Impact**, **Immunity Canvas**) odkazujú na CAPEC attack patterns pri generovaní testovacích scenárov.

3. Security Education & Research Tools

- CAPEC je často integrovaný do vzdelávacích platforiem a laboratórií, napr. MITRE ATT&CK + CAPEC pre výučbu identifikácie a prevencie útokov.
- Rôzne akademické nástroje využívajú CAPEC ako referenčný zdroj útokových vzorov pri štúdiu kybernetickej bezpečnosti.

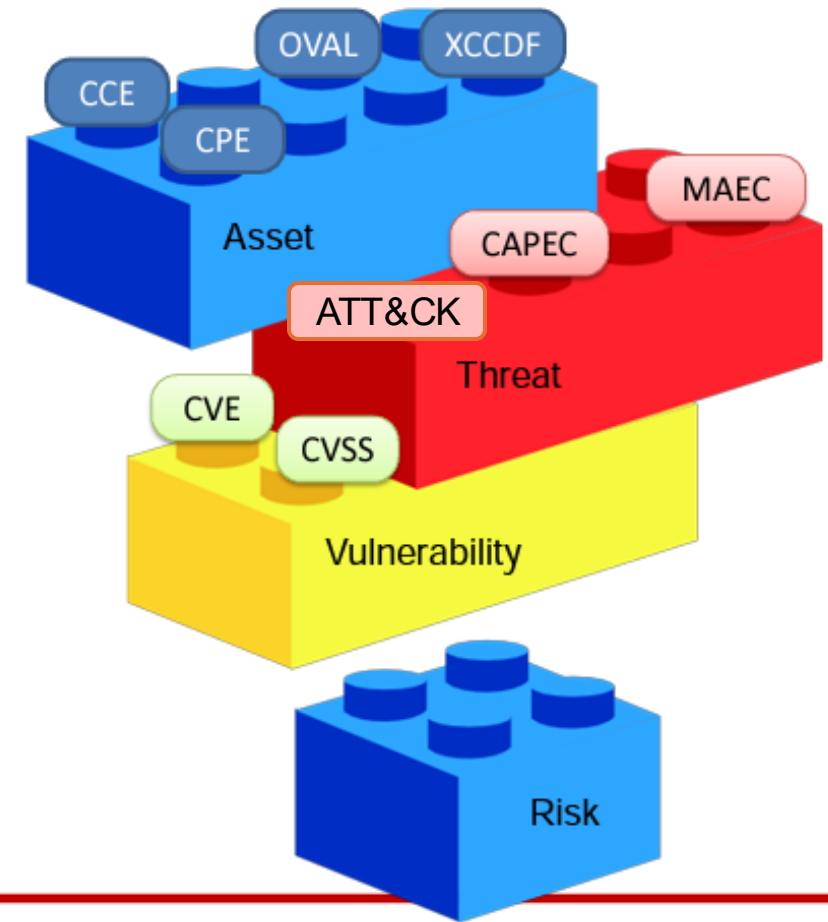
4. Vulnerability Management / Threat Intelligence Platforms

- Niektoré TI platformy a SIEM nástroje môžu importovať CAPEC attack patterns na mapovanie incidentov alebo klasifikáciu útokov podľa známych vzorov.

Štandard MAEC™



- komunitou vyvinutý štruktúrovaný jazyk
 - na kódovanie a zdieľanie verných informácií o **malvéri** na základe atribútov:
 - správania
 - artefaktov
 - vzťahov medzi vzorkami malvéru, ...
- **Výhody:**
 - Eliminácia nejednoznačnosti a nepresnosti v popisoch malvéru
 - Znížená duplicita úsilia o analýzu škodlivého softvéru
 - Vylepšené všeobecné povedomie o malvéri
 - Znížená celková doba odozvy na hrozby škodlivého softvéru
- Intergráciu MAEC majú rôzni dodávateľia sandboxov, EDR/CTI riešení a analytických nástrojov
- Reportovací modul Cuckoo Sandbox 2.x vytvára výstup MAEC 5.0



<https://maecproject.github.io/about-maec/>

Globálne dostupná znalostná báza o taktikách a technikách protivníka

MITRE ATT&CK (v17 – Október 2025)



- je celosvetovo dostupná vedomostná báza protivníkových taktík a techník založená na skutočnom pozorovaní
 - používa sa ako základ pre vývoj špecifických modelov hrozieb a metodológií
 - v súkromnom sektore
 - vo vládnom sektore
 - v komunite produktov a služieb kybernetickej bezpečnosti
- Aktuálna verzia **MITRE ATT&CK** je **v17.1** — platná od **22. apríla 2025**
 - ATT&CK sa priebežne aktualizuje (major-releases spravidla dvakrát ročne)

Globálne dostupná znalostná báza o taktikách a technikách protivníka

MITRE ATT&CK (v18.1 – 28.október 2025)

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 11 techniques	Execution 16 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defense Evasion 45 techniques	Credential Access 17 techniques	Discovery 33 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Active Scanning (2)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (12)	BITS Jobs	Access Token Manipulation (6)	Access Token Manipulation (6)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	Account Manipulation (7)	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (6)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (2)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts (6)	Debugger Evasion	Forced Authentication	Cloud Service Discovery	Remote Services (8)	Clipboard Data	Data Obfuscation (2)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Exploitation for Client Execution	Compromise Host Software Binary	Create or Modify System Process (5)	Decfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Storage Object Discovery	Replication Through Removable Media	Data from Cloud Storage	Dynamic Resolution (2)	Exfiltration Over Physical Medium (1)	Email Bombing
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Input Injection	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Container and Resource Discovery	Software Deployment Tools	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (2)	Inter-Process Communication (2)	Create or Modify System Process (5)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Modify Authentication Process (9)	Fallback Evasion	Taint Shared Content	Data from Information Repositories (5)	Hide Infrastructure	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)	Valid Accounts (4)	Trusted Relationship	Native API	Event Triggered Execution (17)	Escape to Host	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Device Driver Discovery	Use Alternate Authentication Material (4)	Data from Local System	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites	WiFi Networks	Valid Accounts (4)	Scheduled Task/Job (5)	Exclusive Control	Event Triggered Execution (17)	Email Spoofing	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels	Network Denial of Service (2)	Inhibit System Recovery
			Serverless Execution	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (2)	Network Sniffing	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol	Resource Hijacking (4)	Service Stop
			Shared Modules	Hijack Execution Flow (12)	Exploitation for Privilege Escalation	Execution Guardrails (2)	OS Credential Dumping (8)	Group Policy Discovery		Data Staged (2)	Non-Standard Port	System Shutdown/Reboot	
			Software Deployment Tools	Implant Internal Image	Hijack Execution Flow (12)	File and Directory Permissions Modification (2)	Steal Application Access Token	Log Enumeration		Email Collection (3)	Protocol Tunneling		
			System Services (2)	Modify Authentication Process (9)	Process Injection (12)	Hide Artifacts (14)	Steal or Forge Authentication Certificates	Network Service Discovery			Proxy (1)		
			User Execution (4)	Scheduled Task/Job (5)	Scheduled Task/Job (5)	Hijack Execution Flow (12)	Steal or Forge Kerberos Tickets (5)	Network Share Discovery					
			Windows Management Instrumentation	Modify Registry	Valid Accounts (4)	Impair Defenses (11)	Steal Web Session Cookie	Network Sniffing					
				Office Application Startup (6)		Indicator Removal (10)	Unsecured Credentials (2)	Password Policy Discovery					
				Power Settings		Indirect Command Execution		Peripheral Device Discovery					
				Pre-OS Boot (5)		Masquerading (11)		Permission Groups Discovery (2)					
				Scheduled Task/Job (5)		Modify Authentication Process (9)		Process Discovery					
				Server Software Component (6)		Modify Cloud Compute Infrastructure (6)		Query Registry					
				Software Extensions (2)		Modify Cloud Resource Hierarchy		Remote System Discovery					
				Traffic Signaling (2)		Modify System Image (2)		Software Discovery (1)					
				Valid Accounts (4)		Network Boundary Bridging (1)		System Information Discovery					
						Obfuscated Files or Information (17)		System Location Discovery (1)					
						Plist File Modification		System Network Configuration Discovery (2)					
						Pre-OS Boot (5)		System Network Connections Discovery					
						Process Injection (12)		System Owner/User Discovery					
						Reflective Code Loading		System Service Discovery					
						Rogue Domain Controller		System Time Discovery					
						Rootkit		Virtual Machine Discovery					
						Subvert Trust Controls (6)		Virtualization/Sandbox Evasion (3)					
						System Binary Proxy Execution (14)							
						System Script Proxy Execution (2)							
						Template Injection							
						Traffic Signaling (2)							
						Trusted Developer Utilities Proxy Execution (3)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Virtualization/Sandbox Evasion (3)							
						XSL Script Processing							

- 14 taktík
- 216 techník
- 475 sub-technik
- 176 skupín (threat actor entities)
- 910 softvérových nástrojov (pre realizáciu útokov)
- 55 kampaní (série útokov alebo operácií, ktoré sú spojené s určitou skupinou alebo hrozbou)
- 44 mitigácií (pre techniky)
- 691 detekčných stratégií
- 37 dátových zdrojov (Např. logy, sieťový traffic, udalosti z antivírusu, ..)

- Až 3 matice:
- Enterprise
 - Mobile
 - ICSS

Pomáhajú SIEM/EDR nástrojom vyhodnocovať, či sa nejaká technika deje v systéme.



CAPEC and ATT&CK by MITRE

CAPEC

- Zameriava sa na **bezpečnosť aplikácií**
- Vypočítava zneužitia proti zraniteľným systémom
 - popisuje spoločné **atribúty a techniky**
 - SQL Injection, XSS, Session Fixation, Clickjacking
- Zahŕňa social engineering / supply chain
- Súvisí s Common Weakness Enumeration (CWE)

ATT&CK

- Zameriava sa na **obranu siete**
- Založené na spravodajstve o hrozbách (threat intelligence) a výskume red tímu
- Poskytuje kontextové pochopenie škodlivého správania
 - opisuje operačné fázy v životnom cykle protivníka, pred a po zneužití (napr. Persistence, Lateral Movement, Exfiltration)
 - podrobne popisuje špecifické taktiky, techniky a postupy (**TTP**), ktoré používajú útočníci pri pokročilých a perzistentných hrozbách (**APT**)
 - na realizáciu svojich zámerov pri zacielení, kompromitovaní a fungovaní v sieti svojej obeť
- Podporuje testovanie a analýzu možností obrany

CAPEC and ATT&CK by MITRE

Ako spolu súvisia...

- Mnohé vzory útokov vymenované CAPEC sú využívané protivníkmi prostredníctvom špecifických techník popísaných ATT&CK.
 - Toto umožňuje kontextové pochopenie vzorov útokov v rámci operačného životného cyklu protivníka
- Vzory útokov CAPEC a súvisiace techniky ATT&CK sa medzi sebou (v prípadoch keď je to možné a vhodné) na seba odkazujú (cross referencing)

Použite CAPEC na:

- Modelovanie hrozieb aplikácií
- Školenie a vzdelávanie vývojárov
- Penetračné testovanie

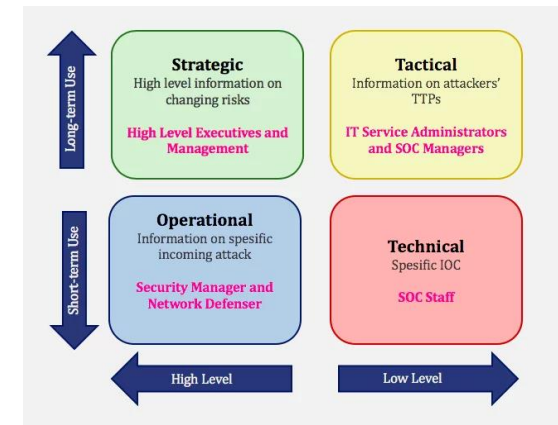
Použite ATT&CK na:

- Porovnanie obranných schopností počítačovej siete
- Obranu proti Advanced Persistent Threat (pokročilej pretrvávajúcej hrozbe)
- Hľadanie nových hrozieb (Hunting..)
- Zlepšenie spravodajstva o hrozbách
- Cvičenia emulácie protivníka



Databázy zraniteľností a slabín

CWE, CVE, CVSS



CWE and CVE

Common Weakness Enumeration

- Katalóg slabín v softvéri
- Napr.:
 - CWE-79 – Cross-Site Scripting
 - CWE-89 – SQL Injection
 - CWE-787 – Out-of-Bounds Write
- Použitie:
 - vývoj bezpečného kódu
 - SDLC
 - hodnotenie zraniteľností

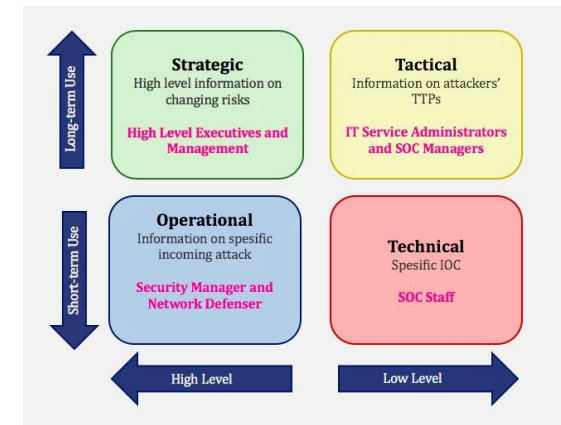
Common Vulnerabilities and Exposures

- Zoznam všetkých známych zraniteľností
- Každá zraniteľnosť má identifikátor napríklad:
 - **CVE-2023-23397** (Outlook zero-click exploit)
 - **CVE-2017-0144** (EternalBlue)
- Použitie:
 - patch management
 - risk assessment
 - threat modeling



Malvérové databázy

MalwareBazaar (abuse.ch), VirusTotal
AnyRun, Hybrid Analysis



Malware databázy

- **úložiská vzoriek a informácií o malvéri**
- Malvérové databázy zhromažďujú vzorky škodlivého kódu, jeho technické artefakty, analýzy správania a reputačné informácie. Používajú sa na výskum, detekciu a spracovanie incidentov.
- Malvérové databázy sa odlišujú od IOC databáz tým, že obsahujú **skutočné vzorky malvéru a ich analýzy**, nie len indikátory kompromitácie. Ich cieľom je *výskum a pochopenie správania malvéru*, kým IOC databázy sú primárne určené na *detekciu a blokovanie hrozieb*.














Malware databázy

- **MalwareBazaar (abuse.ch)**
 - Hashe a vzorky škodlivých súborov.
- **VirusTotal**
 - multiscanner + threat intel od vendorov
- **AnyRun, Hybrid Analysis**
 - dynamická analýza malvéru (sandboxy)

Link: <https://bazaar.abuse.ch/>

MalwareBazaar (abuse.ch)

- **Typ:** Open source *databáza a nástroj na distribúciu vzoriek malvéru*
- **Obsah:**
 - vzorky škodlivých súborov (.exe, .dll, skripty, dokumenty)
 - SHA256/MD5 hash-e, názvy kampaní
 - analýzy statického správania
 - informácie o C2 infraštruktúre (riadiaca a komunikačná infraštruktúra útočníka, ktorá slúži na ovládanie kompromitovaných zariadení a malvéru)
- **Využitie:**
 - výskum, identifikácia a porovnávanie malvéru
 - obohatenie TI platforiem (MISP, OpenCTI)

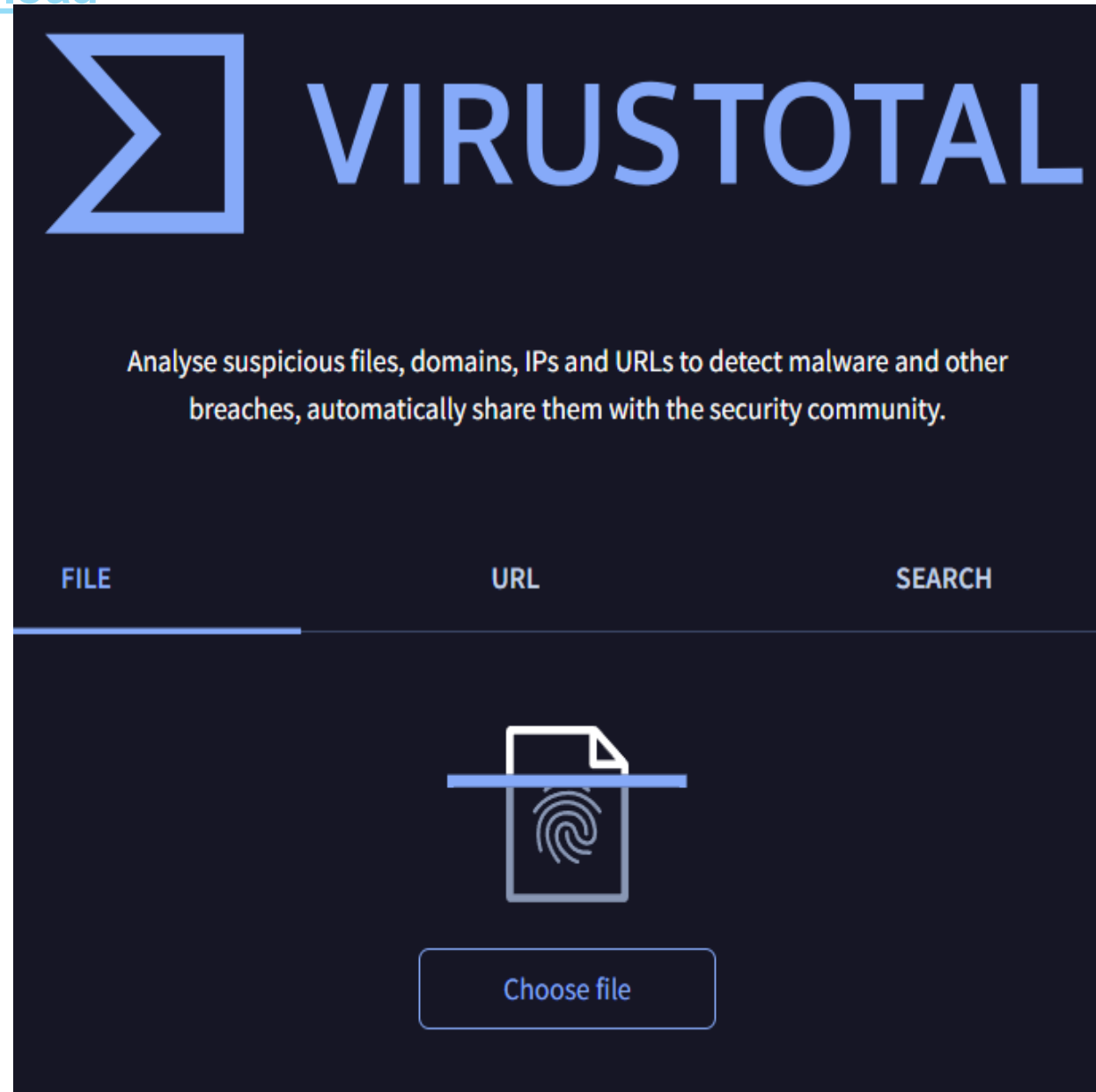
Date (UTC) ↑↓	SHA256 hash ↑↓	Type ↑↓	Signature ↑↓	Tags
2026-02-02 15:51	342b5e56a768327e1cd5...	 exe		 
2026-02-02 15:50	7b40e010ae6556b159ea...	 apk		
2026-02-02 15:50	a81b801522a1c72be91a...	 apk		
2026-02-02 15:50	d566c64a41faf573349cf2...	 apk		
2026-02-02 15:50	3616fd6004678159e531f...	 apk		
2026-02-02 15:50	2f451d9cfda5d91b2063a...	 apk		
2026-02-02 15:50	f99486a60b7f8ae9ba5cf9...	 apk		
2026-02-02 15:50	77c54058a2bb45219e6e...	 apk		
2026-02-02 15:50	5cb94ba3236bd4fa89ba...	 apk		
2026-02-02 15:50	807d8ffb7975d52538603...	 apk		

ABUSE | ch

Link: <https://www.virustotal.com/gui/home/upload>

VirusTotal

- **Verzia:** Poskytuje free aj platenú verziu
- **Obmedzenia Free verzie:**
 - Obmedzený počet dotazov
 - Manuálna správa
- **Typ:** *cloudový multiscanner a TI platforma*
- **Obsah:**
 - viac ako 70 AV enginov, sandbox výsledky
 - hash-e, metadáta, statická a dynamická analýza
 - sieťová komunikácia a extrahované indikátory
- **Využitie:**
 - rýchle overenie súborov/URL
 - hľadanie prepojení medzi vzorkami (VT Graph)
 - feedy IOC a reputačné informácie



Link: <https://any.run/>

ANY.RUN

- **Verzia:** Poskytuje free aj platenú verziu
 - **Obmedzenia Free verzie:**
 - Obmedzený počet analýz
 - Manuálna správa
 - **Typ:** *interaktívny cloud sandbox*
- Obsah:**
- detailné dynamické analýzy (procesy, registry, sieť)
 - vizualizácie C2 komunikácie
 - extrakcia IOC
- Využitie:**
- behaviorálna analýza malvéru
 - výskum nových kampaní



Start your analysis

Interact with Windows, Linux, and Android OS directly and immediately see the feedback from your actions.

Deep interactive investigation in full environment



Submit File / Email

Detonate an object to observe its malicious activity



Submit URL

Investigate malicious and phishing activity and inspect downloaded files

Power your SOC with ANY.RUN solutions



TI Feeds



Prevent attacks with actionable IOC streams and automate detection in SIEM, SOAR, and TIP



TI Lookup

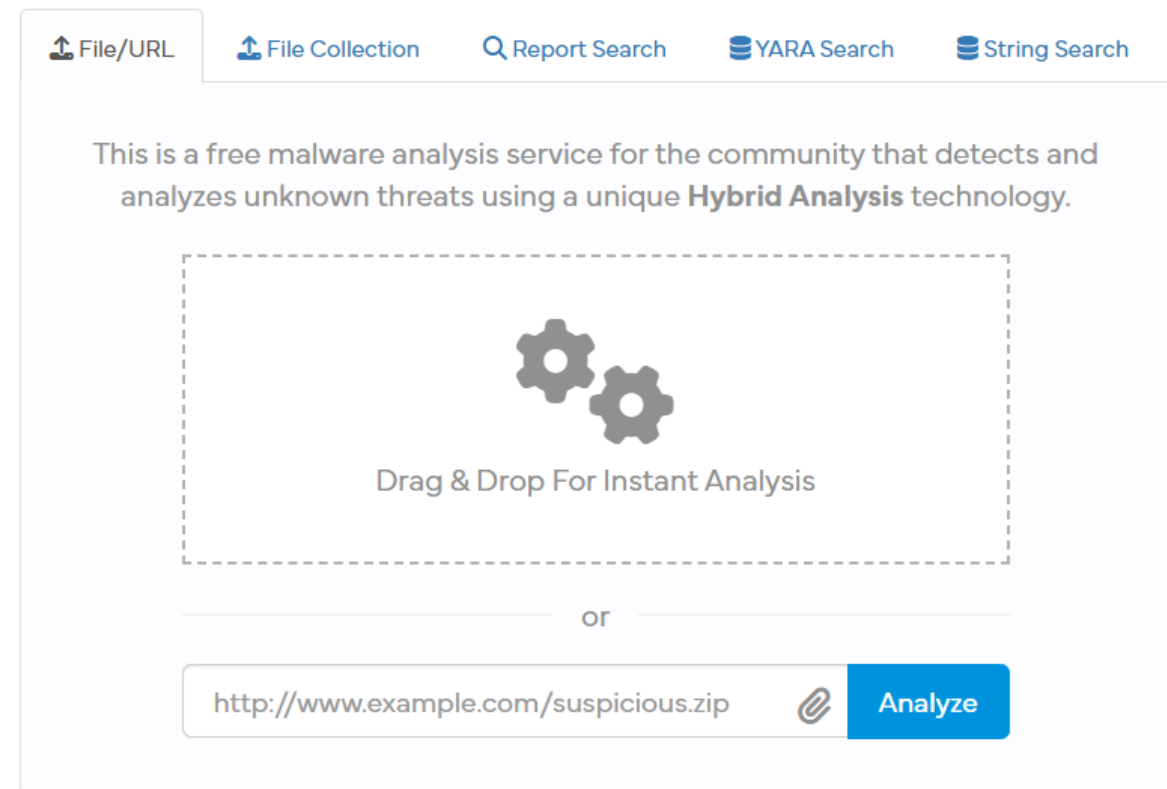


Enrich investigations and respond faster with IOCs, IOBs, and IOAs from live attack data

Link : <https://hybrid-analysis.com/>

Hybrid Analysis (CrowdStrike Falcon Sandbox)

- **Verzia:** Poskytuje free aj platenú verziu
- **Obmedzenia Free verzie:**
 - Obmedzený počet analýz
 - Prístup len verejným dáta
- **Typ:** *sandbox + databáza analýz*
Obsah:
 - automatické správy o správaní malvéru
 - extrahované IOC, YARA pravidlá
 - reputačné skóre Falcon ML**Využitie:**
 - porovnávanie vzoriek
 - získavanie signatúr a IOC pre SOC/IR





IOC databázy

AlienVault OTX

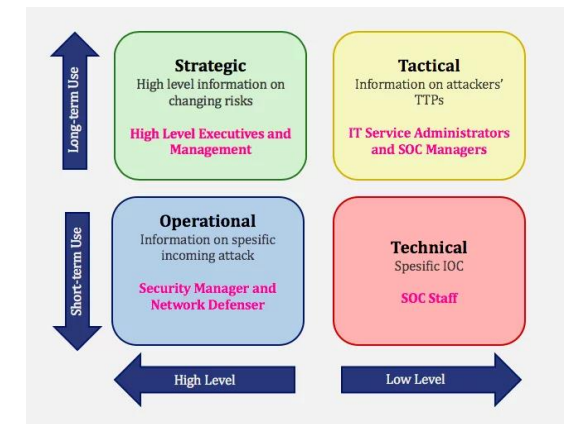
MISP

ThreatFox

Feodo Tracker

URLHaus

Spamhaus DBL/SBL/XBL



IOC databázy

- **úložiská indikátorov kompromitácie**
- IOC databázy zhromažďujú informácie použiteľné na detekciu útočníkov v infraštruktúre. Neobsahujú vzorky malvéru, ale indikátory, *ktoré po sebe malvér alebo útočník zanechá.*
- IOC databázy sú kľúčové pre **detekciu a okamžitú reakciu** – poskytujú krátkodobé, ale veľmi presné indikátory, ktoré sa dajú priamo aplikovať do SIEM, EDR, firewall a IDS/IPS. Neobsahujú detailné analýzy malvéru, ale rýchle, akčné dáta pre SOC.

IOC databázy

- **AlienVault OTX**
- **MISP**
- **ThreatFox**
- **Feodo Tracker**
- **URLHaus**
- **Spamhaus DBL/SBL/XBL**

Link : <https://otx.alienvault.com/>

AlienVault OTX (Open Threat Exchange)

- **Verzia:** Poskytuje free aj platenú verziu
- **Obmedzenia Free verzie:**
 - Obmedzený počet dotazov
 - Manuálna správa
 - Prístup k základným zdrojom
- **Typ:** TI platforma a databáza IOC
- **Obsah:**
 - IP/domény URL spojené s kampaniami
 - hash-e malvéru
 - informácie od komunity (Pulses)
- **Využitie:**
 - obohatenie alertov v SIEM
 - sledovanie hrozieb v reálnom čase
 - integrácia s MISP, Elastic, Suricata

We've found 94,865,369 indicators

<http://196.251.107.130/cfedbcab777558b8.php>

Type: URL

<http://158.94.210.74/4d4b240c75954580.php>

Type: URL

retrodayaengineering.icu

Type: Domain



OPEN THREAT EXCHANGE

Link : <https://threatfox.abuse.ch/>

ThreatFox (abuse.ch)

- **Verzia:** *Open source*
- **Typ:** *IOC databáza zameraná na malvér*

Obsah:

- škodlivé IP, domény, URL
- typ malvéru (Emotet, QakBot, AgentTesla atď.)
- časová platnosť IOC







Využitie:

- automatické blocklisty pre firewall/SIEM
- feedy pre TI platformy

abusech/**ThreatFox**

ABUSE | ch

Open IOC sharing platform

Date (UTC) ↑↓	IOC	↑↓	Malware	↑↓
2026-02-02 16:00	45.32.218.131:4444		 AsyncRAT	
2026-02-02 16:00	158.94.211.31:80		 Sliver	
2026-02-02 16:00	85.122.114.230:2404		 Remcos	
2026-02-02 15:55	47.76.86.151:23156		 ValleyRAT	
2026-02-02 14:33	109.107.168.147:80		 Unknown RAT	
2026-02-02 14:33	http://109.107.168.147/ws/client		 Unknown RAT	

Link : <https://urlhaus.abuse.ch/>

URLhaus (abuse.ch)

- **Verzia:** Open source
- **Typ:** databáza škodlivých URL

Obsah:

- škodlivé download URL
- malvér distribučné servery
- metadata (hosting, čas objavenia)

Využitie:

- ochrana webového perimetra
- automatické prispôsobenie URL filtrácie

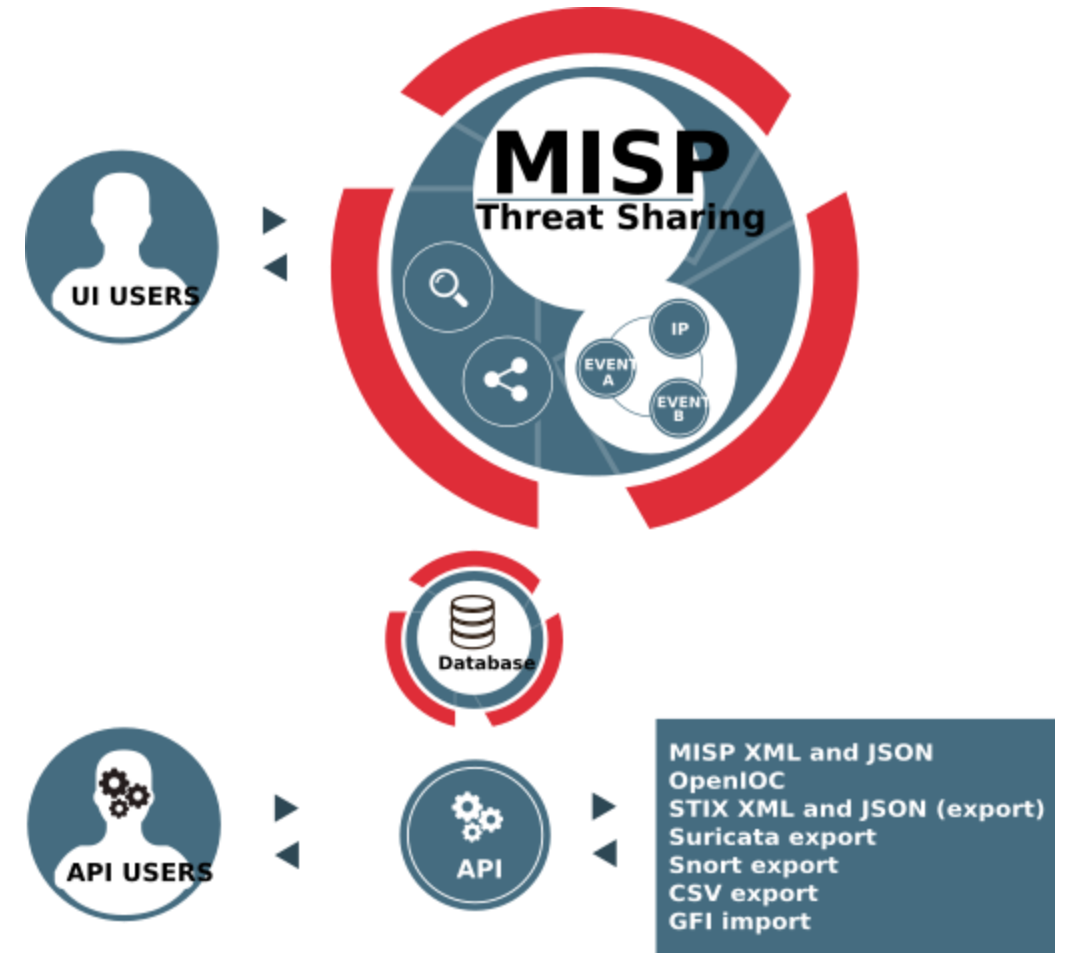
URLhaus

by ABUSE | ch

Dateadded (UTC)	Malware URL	Status
2026-02-02 15:54:08	http://27.215.123.69:48813/i	Online
2026-02-02 15:40:10	http://175.165.82.70:56547/bin.sh	Online
2026-02-02 15:35:10	http://42.227.187.160:48273/i	Online
2026-02-02 15:33:10	http://110.37.76.11:39925/bin.sh	Online
2026-02-02 15:31:09	http://110.37.66.198:34486/i	Online
2026-02-02 15:30:09	http://125.43.230.147:44334/i	Online
2026-02-02 15:18:08	http://130.12.180.43/files/7782139129/4utgF9B.exe	Online
2026-02-02 15:12:10	http://115.50.105.222:37579/i	Online
2026-02-02 15:07:18	http://115.55.49.236:33460/i	Online
2026-02-02 15:04:24	http://222.139.72.108:45682/bin.sh	Online
2026-02-02 15:03:16	http://110.37.89.129:44639/i	Online
2026-02-02 15:03:15	http://125.45.67.251:39487/i	Online

MISP - Malware Information Sharing Platform

- open source platforma na zdieľanie IOC pre novoobjavené hrozby
- MISP je podporovaná EÚ
 - CIRCL vedie vývoj MISP
 - Computer Incident Response Center Luxembourg
- je široko používaný
 - vládnymi inštitúciami
 - národnými CERTs
 - súkromnými spoločnosťami,
 - finančným sektorom
 - a ďalšími organizáciami po celom svete.
- MISP umožňuje automatizované zdieľanie IOCs medzi ľuďmi a strojmi pomocou STIX a iných export formátov
 - Zdieľanie a import dát:
 - Generovaním **Snort/Suricata/Bro/Zeek IDS pravidiel**
 - pomocou **STIX, OpenIOC, text alebo csv** exportov



<https://www.misp-project.org/features/>

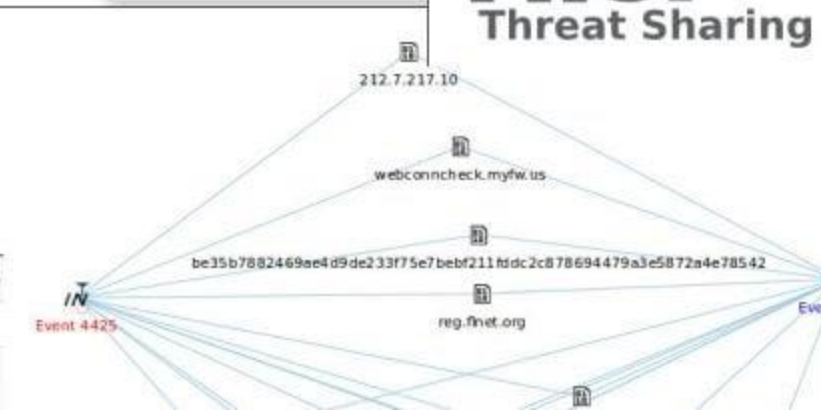
MISP - Malware Information Sharing Platform

OSINT - CVE-2015-2545: overview of current threats

Event ID	3865
Uuid	57460863-76dc-4272-8116-4ea302de0b81
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulsunoy@circl.lu
Tags	ftp:white circl:osint-feed Type:OSINT estimative-language:likelihood-probability~"very-likely"
Date	2016-05-25
Threat Level	Medium
Analysis	Completed
Distribution	All communities
Info	OSINT - CVE-2015-2545: overview of current threats
Published	Yes
Sightings	0 (0)

Related Events

2016-05-27 (3883)	Org: CIRCL
2016-05-23 (3844)	Date: 2016-05-23
2016-05-06 (3826)	Info: OSINT - Operation Ke3chang Resurfaces With New TidePool Malware



Expanded	Events	Tag	Action
Likelihood or probability: Almost no chance - remote - 01-05%	0	estimative-language:likelihood-probability~"almost-no-chance"	
Likelihood or probability: Very unlikely - highly improbable - 05-20%	0	estimative-language:likelihood-probability~"very-unlikely"	

Malicious activities

Event ID: 10878
 Uuid: 5aec700c-0eb8-468...
 Org: CIRCL
 Owner org: CIRCL
 Contributors: alexandre.dulaunoy
 Email: alexandre.dulaunoy@circl.lu
 Tags: [tag icon]
 Date: 2018-05-04
 Threat Level: Low
 Analysis: Initial
 Distribution: All communities
 Info: Malicious activities
 Published: No
 #Attributes: 2
 Last change: 2018/05/04 02:38:12
 Extended by:
 Sightings: 0 (0)
 Activity: [activity icon]



Threat Level: Low
 Analysis: Initial

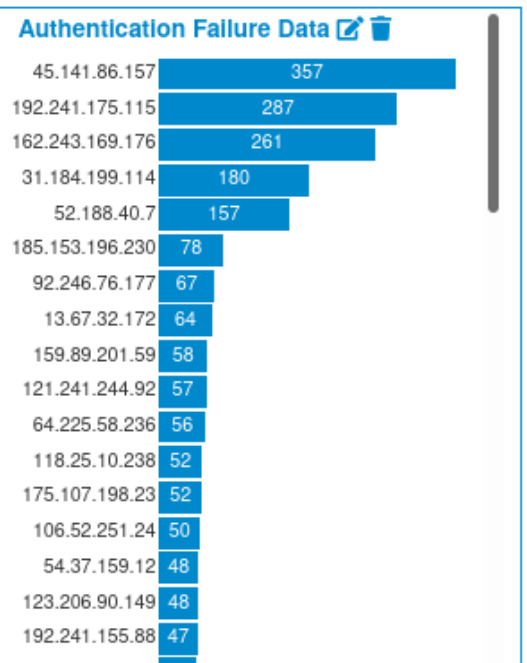
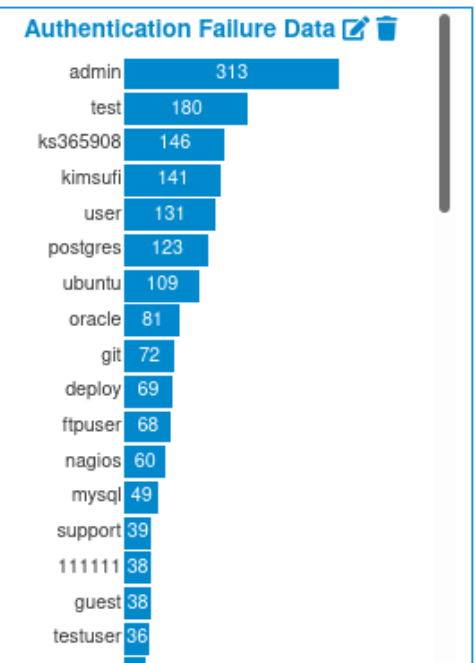
Event Info: Ransomware found on a production server

Extends event: 5ad8687b-De10-4a8b-a157-46a5950d210f

Matched event
 Id: 10728
 Analysis: Completed
 Threat level: Low
 Tags:
 - circ:osint-feed ttp:white
 - malware_classification:malware-category="Ransomware"
 - osint:source-type="blog-post"
 - misp-galaxy:ransomware="CSGO Ransomware"
 - misp-galaxy:ransomware="MC Ransomware"
 Info: OSINT - Minecraft & CS:GO Ransomware Stir For Media Attention

estimative-language:confidence-in-analytic-judgment="high"
 High

- View Dashboard
- Add Widget
- Import Config JSON
- Export Config JSON
- Save Dashboard Config
- List Dashboard Templates



Achievements of my organization

Achievements Unlocked!

- Event**: Congratulations, you have shared your first event!
- Sharing Definition**: You have been using tags, good job!
- Taxonomy**: Taxonomies have been used in your events.
- Galaxy**: Galaxies have no secrets for you in this Threat Sharing universe.

Next on your list:

Cyber Threat
Intelligence
(CTI)



Zdieľanie informácií o hrozbách (CTI)

CTI transport & modeling standard

Štandardy/formáty, ktoré slúžia na *reprezentáciu všetkých typov CTI*
— technického, operačného, taktického aj strategického

Ministerstvo pre vnútornú bezpečnosť USA

U.S. – Department of Homeland Security (DHS)

<https://www.dhs.gov/operational-and-support-components>

- je určené ako Sektorová agentúra pre riadenie rizík pre sektor kritických služieb, ktorý poskytuje služby v oblasti prevencie, pripravenosti, reakcie a obnovy počas každodenných operácií aj reakcie na incident
- operačné a podporné zložky, ktoré v súčasnosti tvoria DHS:



U.S. Immigration and Customs Enforcement

United States Immigration and Customs Enforcement (ICE)



United States Secret Service (USSS)

USSS safeguards the



Transportation Security Administration (TSA)



U.S. Citizenship and Immigration Services (USCIS)



United States Coast Guard (USCG)




United States Customs and Border Protection (CBP)




Management Directorate



Science and Technology Directorate (S&T)




Countering Weapons of Mass Destruction Office (CWMD)




Cybersecurity and Infrastructure Security Agency (CISA)



Federal Emergency Management Agency (FEMA)



Federal Law Enforcement Training Center (FLETC)



Office of Intelligence and Analysis



Office of Operations Coordination (OPS)



Ombudsman Offices

Threat Intelligence Services

Automated Indicator Sharing



Homeland
Security



CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY



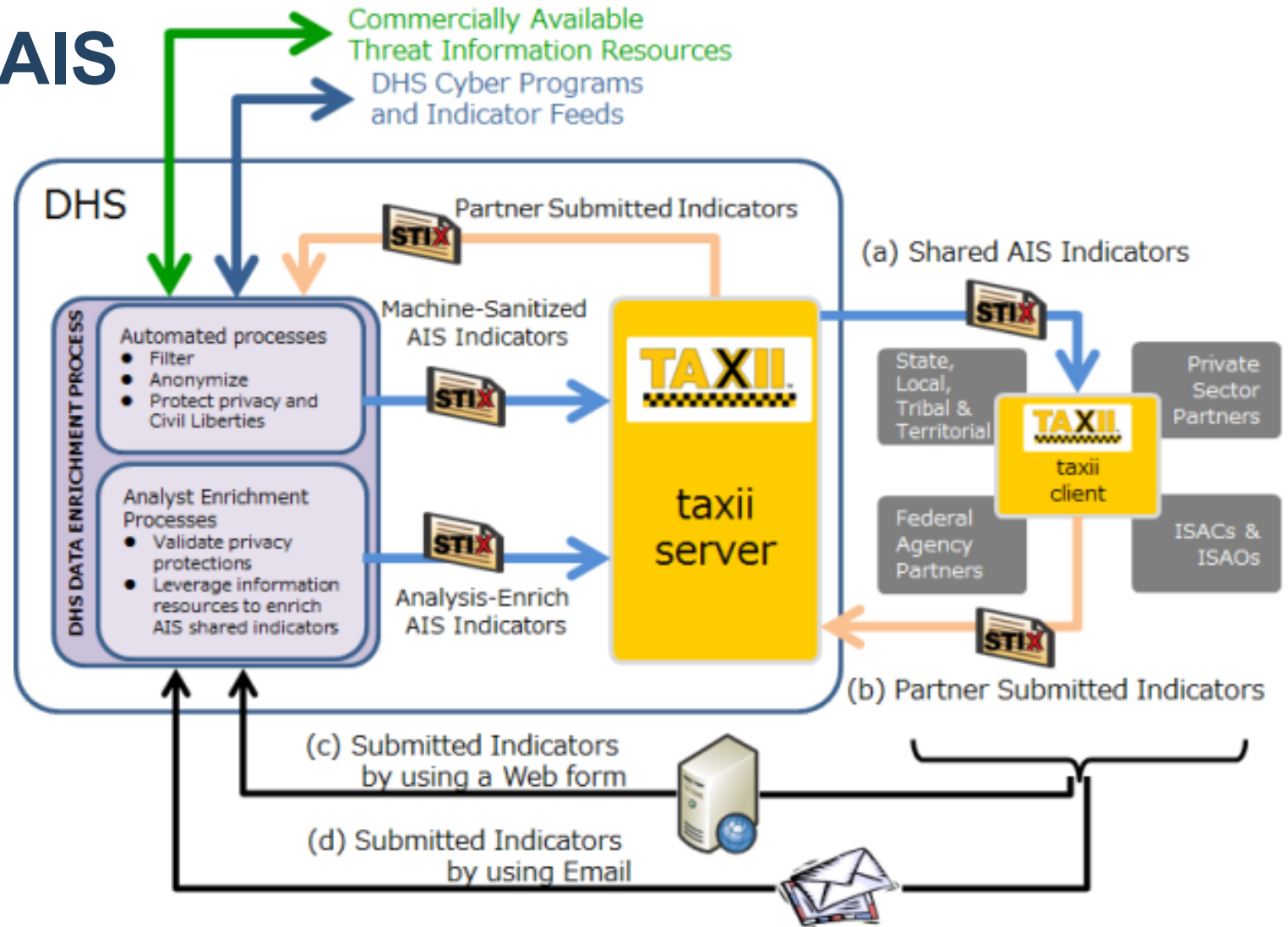
- The Automated Indicator Sharing (AIS) je bezplatná služba, ktorú ponúka U.S DHS – by CISA
- AIS umožňuje **výmenu** indikátorov **kybernetických hrozieb** v reálnom čase medzi
 - U.S. Federal Government
 - a privátnym sektorom
- AIS vytvára **ekosystém**, keď je rozpoznaná hrozba
- Neskôr sa okamžite **zdieľa** s komunitou, aby im pomohla chrániť ich siete pred danou hrozbou
- Čo sa zdieľa:
 - CTIs - cyber threat indicators
 - DM - defensive measures
- Ako sa zdieľa:
 - Pomocou protokolov:
 - Na popis – STIX
 - Na prenos - TAXII

<https://www.cisa.gov/ais>

Automated Indicator Sharing

Open Standards for AIS

- AIS používa otvorené štandardy:
 - STIX™
Structured Threat Information Expression for CTIs and DMs information
 - dátový model na popis
 - TAXII™
Trusted Automated Exchange of CTIs for machine-to-machine communications
 - protokol aplikačnej vrstvy, ktorý umožňuje komunikáciu CTIs cez HTTPS
 - má podporu pre STIX
- CISA rešpektuje súkromie v organizácií
 - AIS pri odosielaní podaní, ich automaticky anonymizuje
 - identita predkladateľa sa nezverejňuje bez jeho predchádzajúceho výslovného súhlasu



<https://www.hitachi.com/hirt/publications/hirt-pub17007/index.html>

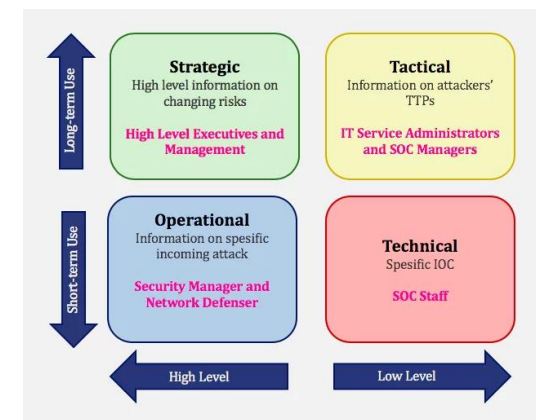
Štruktúra STIX 2.0

- A. STIX Domain Objects (SDO) → popisujú hrozby, útočníkov, kampane, zraniteľnosti...
- B. STIX Relationship Objects → prepájajú objekty (vzťahy)
- C. STIX Cyber-Observable Obj. → popisujú konkrétne technické artefakty (hash, IP, súbor,...)



A) STIX Domain Objects (SDOs)

Objekty, ktoré opisujú svet hrozieb, aktérov a udalostí:

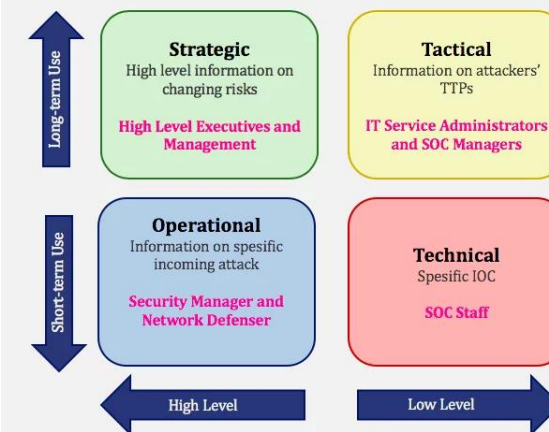


Objekt	Popis
Attack Pattern	Vzor útoku – popisuje techniky, ktoré útočník používa (napr. z MITRE ATT&CK).
Campaign	Súbor súvisiacich útokov zameraných na rovnaké ciele alebo s rovnakým cieľom.
Course of Action	Opatrenie alebo odporúčanie, ako zmierniť alebo zabrániť útoku.
Grouping	Zoskupenie viacerých objektov STIX, ktoré patria k sebe (napr. incident + indikátory).
Identity	Popisuje organizáciu, osobu, OSINT identitu alebo APT skupinu (napr. firma, výskumný tím, vláda).
Incident	(Novinka v STIX 2.1) Reálna bezpečnostná udalosť, ktorá sa stala.
Indicator	Indikátor kompromitácie (IOC) – napr. hash, IP, URL spojená s hrozbou.
Infrastructure	Popisuje infraštruktúru útočníka – servery, C2 siete, domény, botnety.
Intrusion Set	Kolekcia kampaní, útokov a techník patriacich jednej skupine útočníkov.
Location	Geografické miesto (napr. krajina, mesto, región, IP geolokácia).

A) STIX Domain Objects (SDOs), pokrač.

Objekty, ktoré opisujú svet hrozieb, aktérov a udalostí:

Objekt	Popis
Malware	Softvér vytvorený s cieľom poškodiť alebo zneužiť systémy.
Malware Analysis	Výsledok alebo popis analýzy malvéru (sandbox, statická analýza atď.).
Note	Ľubovoľné poznámky, komentáre alebo hodnotenia analytika.
Observed Data	Popis reálne pozorovaných údajov (napr. log z IDS, hash z detekcie).
Opinion	Vyjadrenie názoru analytika (napr. „myslím, že tento malware súvisí s APT29“).
Report	Súhrn viacerých objektov do správy (napr. mesačný CTI report hrozieb, report incidentu).
Threat Actor	Osoba alebo skupina, ktorá realizuje útoky.
Tool	Legitímny alebo škodlivý softvér používaný v útoku (napr. Mimikatz, nmap).
Vulnerability	Slabina v softvéri alebo systéme, ktorú útočník môže využiť.



B) STIX Relationship Objects (SROs)

- Objekty, ktoré prepájajú iné STIX objekty:

Objekt

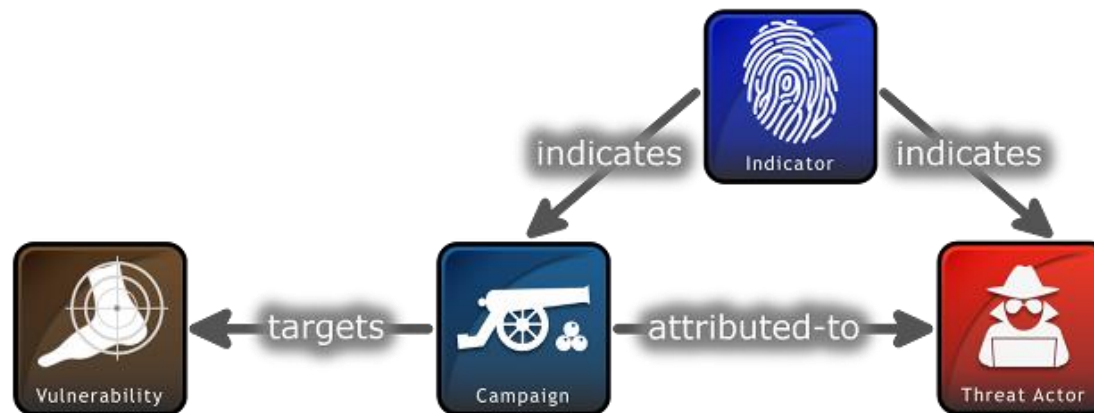
Popis

Relationship

Všeobecné prepojenie medzi dvoma objektmi (napr. „malware uses infrastructure“).

Sighting

Informácia, že konkrétny objekt (napr. IOC) bol pozorovaný v reálnom svete.



C) STIX Cyber-Observable Objects (SCOs)

- Objekty, ktoré opisujú **konkrétne technické artefakty** – sú to „CybOX“ objekty integrované priamo do STIX 2.x:
- Opisuje „čo sa stalo“ alebo „čo vidíme“
- **Účel:**
 - Umožniť, aby rôzne nástroje (IDS, SIEM, EDR, ...) hovorili rovnakým jazykom pri popise udalostí
 - aby sa observable dalo automaticky spracovať a porovnávať medzi systémami

Objekt	Popis
Artifact	Dátový artefakt – súbor, obrázok, dokument, base64 obsah.
Autonomous System	Informácie o AS (Autonomous System Number).
Directory	Adresár v súborovom systéme.
Domain Name	Doménové meno.
Email Address	E-mailová adresa (napr. je zaznamenaný e-mail z konkrétnej adresy).
Email Message	Celý e-mail – hlavičky, telo, prílohy.
File	Súbor (názov, hash, veľkosť, a iné, napr. súbor malware.exe s konkrétnym hashom)
IPv4 Address	IPv4 adresa (napr. ktorá komunikuje s malvérom, ...)
IPv6 Address	IPv6 adresa (napr. ktorá komunikuje s malvérom, ...)

C) STIX Cyber-Observable Objects (SCOs)

Objekty, ktoré opisujú **konkrétne technické artefakty** – sú to „CybOX“ objekty integrované priamo do STIX 2.x:

Objekt

MAC Address

Mutex

Network Traffic

Process

Software

URL

User Account

Windows Registry Key

X.509 Certificate

Popis

MAC adresa.

Synchronizačný objekt v systéme (typický pri malware).

Popis sieťovej komunikácie (TCP, UDP, porty, spojenie, napr. aplikačné protokoly ukazujú komunikáciu na určitých portoch).

Proces bežiaci v OS (názov, PID, parent process, atď.).

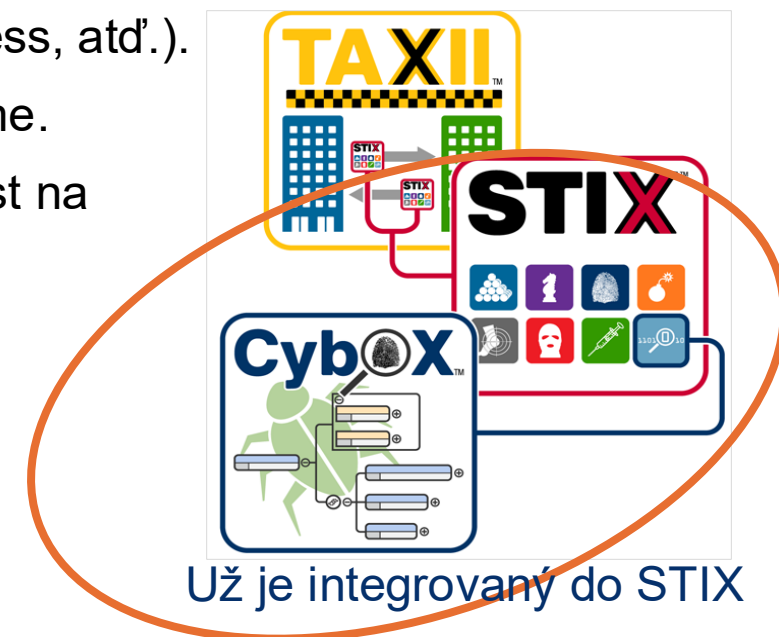
Softvér alebo aplikácia nainštalovaná v systéme.

Uniform Resource Locator (napr. HTTP request na podozrivú doménu).

Používateľské konto.

Kľúč alebo hodnota v registroch Windows (napr. zmena v registroch).

Certifikát X.509.

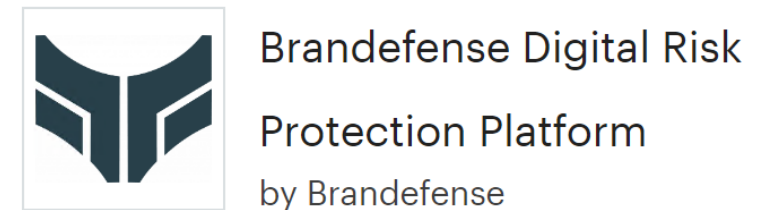




Komerčné nástroje pre CTI

Threat Intelligence Platforms

- A Threat Intelligence Platform (TIP) centralizuje zber údajov o hrozbách z mnohých zdrojov a formátov.
- **Typy threat Intelligence dát:**
 - Indicators of Compromise (IOC)
 - Tactics Techniques and Procedures (TTP)
 - Informácie o reputácii internetových cieľov alebo domén
- Organizácie môžu prispieť k CTI **zdieľaním** svojich údajov o narušeníach cez internet, zvyčajne prostredníctvom automatizácie
- Honeypots - simulované siete alebo servery, ktoré sú navrhnuté tak, aby prilákali útočníkov.
 - Informácie súvisiace s útokmi získané z honeypotov sa môžu zdieľať s predplatiteľmi CTI platformy.



<https://www.gartner.com/reviews/market/security-threat-intelligence-services>

Threat Intelligence

Porovnanie riešení:

- ThreatConnect (Polarity CE)
- Recorded Future
- Anomali ThreatStream

	ThreatConnect	Recorded Future	Anomali ThreatStream
Bezplatná verzia	✓	✗	✗
Cena	?	?	?
Pokrytie taktického CTI	✓	✓	✓
? Cena dostupná len na požiadanie.			

ThreatConnect

- ThreatConnect je komplexná CTI platforma, ktorá kombinuje threat intelligence, orchestráciu, automatizáciu a workflow. Verzia **Polarity Community Edition (CE)** je ľahší modul využívaný na dopĺňanie TI kontextu priamo počas práce analytika.
- **Kľúčové vlastnosti ThreatConnect / Polarity CE:**
 - podpora STIX/TAXII a integrácie s SIEM/EDR nástrojmi
 - schopnosť prepájať IOC, kampane a aktérov
 - automatické enrichmenty pri reálnom vyhodnocovaní alertov
 - možnosť tvorby playbookov (orchestrace)
 - orientované na výkon analytikov SOC/IR – šetrí čas pri vyhľadávaní kontextu



Recorded Future

- Recorded Future patrí medzi najrozsiahlejšie a najpokročilejšie Threat Intelligence riešenia na trhu. Využíva kombináciu strojového učenia, OSINT, dark web monitoringu a vlastných TI zdrojov na poskytovanie detailných informácií o aktéroch, kampaniach, malvéri a hrozbách v reálnom čase.
- **Kľúčové vlastnosti Recorded Future:**
 - obrovská databáza CTI informácií vrátane OSINT, dark web, leak stránok a sociálnych sietí
 - Risk Scoring – automatické hodnotenie rizikovosti IOC pomocou ML
 - detailné profily aktérov, TTP, kampaní a malvérových rodín
 - monitoring únikov dát, ransomware skupín a ilegálnych fór
 - prediktívne analýzy a upozornenia na nadchádzajúce kampane
 - podpora STIX/TAXII a prepojenie s SIEM/EDR
 - vhodné pre pokročilých CTI analytikov, threat hunting a strategické plánovanie



Anomali ThreatStream

- Anomali ThreatStream sa zameriava na spracovanie, normalizáciu a distribúciu veľkých objemov IOC feedov. Platforma integruje stovky zdrojov TI, automatizuje analýzu IOC a poskytuje jednotnú databázu pre SOC, IR a TI tímy.
- **Kľúčové vlastnosti Anomali ThreatStream:**
 - silné spracovanie IOC – normalizácia, scoring a deduplikácia
 - automatizované preberanie feedov z desiatok komerčných aj open-source zdrojov
 - machine learning na extrakciu IOC z textov, logov a neznačkových dát
 - korelácia IOC s aktérmi, kampaňami a hrozbami
 - integrácia s SIEM, EDR a firewall riešeniami pre rýchle blokovanie IOC
 - schopnosť fungovať ako centrálna platforma pre Threat Intelligence operácie
 - vhodné pre SOC L2/L3, threat hunting a IR tímy



Porovnanie Recorded Future s ThreatConnect

Výhody

- Jedna z najlepších hĺbkových databáz CTI na trhu – obsahuje OSINT, dark web monitoring, geopolitické dáta, ransomware leaksites, paste stránky
- **Strojové učenie** na odhad rizikovosti IOC (Risk Score)
- **Prediktívne modelovanie** – upozornenia na budúce kampane, zvyšujúcu sa aktivitu skupín
- **Najlepšie pokrytie globálnych hrozieb a APT aktérov** (oveľa širšie ako ThreatConnect CE)

Nevýhody

- **Nedáva taký kontext počas práce ako Polarity CE**
- Komplexné moduly sú **drahé** – pre univerzitu alebo malé SOC nevhodné
- Menej zamerané na **workflow orchestration**
- Vyžaduje špecializovaný tréning a onboarding

Porovnanie Anomali ThreatStream s ThreatConnect

Výhody

- Široký TI ekosystém so stovkami feedov a integrácií
- Veľmi dobré spracovanie IOC a automatické normalizovanie feedov
- **Machine Learning na extrakciu IOC z textu a webových zdrojov**
- Silné nástroje na scoring IOC a koreláciu medzi feedmi

Nevýhody

- Menej prepojené workflow ako v ThreatConnect (hlavne v CE aj enterprise verzii)
- Knowledge graph je slabší než vo ThreatConnect alebo OpenCTI
- Dashboardy sú menej intuitívne

Threat Intelligence Services

Cisco Talos

- Talos je jedným z najväčších **komerčných threat intelligence tímov** na svete, a pozostáva zo špičkových výskumníkov, analytikov a inžinierov.
- Cieľom je **pomôcť chrániť** podnikových používateľov, údaje a infraštruktúru pred aktívnymi útočníkmi.
- Tím zhromažďuje informácie o aktívnych, existujúcich a vznikajúcich hrozbách a následne poskytuje svojim predplatiteľom komplexnú ochranu pred týmito útokmi a malvérom.
- Produkty Cisco Security môžu využívať Talos threat intelligence v reálnom čase a poskytovať rýchle a účinné bezpečnostné riešenia.
- Cisco Talos tiež poskytuje bezplatný softvér, služby, zdroje a údaje a spravuje súbory pravidiel na detekciu bezpečnostných incidentov pre niekoľko nástrojov na bezpečnosť sietí:
 - Snort.org
 - ClamAV
 - SpamCop



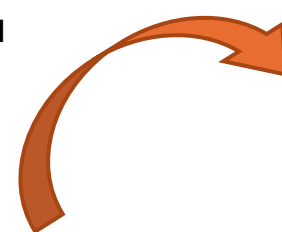
FireEye >> Trellix

- FireEye je ďalšia bezpečnostná spoločnosť, ktorá ponúka služby na pomoc podnikom pri zabezpečení ich sietí.
- Využíva trojstranný (three-pronged) prístup, ktorý kombinuje bezpečnostné informácie, odborné znalosti v oblasti bezpečnosti, a technológie.
- Ponúka SIEM a SOAR s Helix Security Platform, ktorá využíva behaviorálnu analýzu a pokročilú detekciu hrozieb a je podporovaná celosvetovou threat intelligence sieťou FireEye Mandiant.

Január 19, 2022:

- McAfee Enterprise a FireEye sa spájajú a vzniká Trellix
 - nový biznis poskytujúci organizáciám **rozšírenú detekciu a reakciu** (XDR) so zameraním na urýchlenie technologických inovácií prostredníctvom **strojového učenia a automatizácie**
 - Trellix XDR ekosystém je navrhnutý tak, aby **urýchlil účinnosť bezpečnostných operácií** tým, že zákazníkom poskytuje možnosť využívať viac ako 600 pôvodných a otvorených bezpečnostných technológií.

https://www.trellix.com/en-us/about/newsroom/news/news-detail.html?news_id=3e247ede-b638-4bb4-bd13-00b94a623e01



Featured FireEye Products



Helix Security Platform

Applies threat intelligence, automation, and case management.



Endpoint Security

Comprehensive endpoint defense to stop breaches in their tracks.



Email Security

Detects and blocks every kind of unwanted email, especially advanced attacks.



Cloud Security

Controls the cloud with our holistic cyber security approach.



Trellix XDR Platform



Endpoint Security

Secure your organization with proactive endpoint detection, response, and prevention.

[Explore Endpoint Products →](#)



SecOps and Analytics

Conduct streamlined, efficient SecOps (Security Operations) and Analytics from a holistic foundation.

[Explore SecOps Products →](#)



Data Protection

Keep your information safe with a single integrated suite.

[Explore Data Protection Products →](#)



Network Detection and Response

Protect networks, servers, and data centers with a living, learning solution.

[Explore Network Products →](#)



Email Security

Keep your email infrastructure and users safe—whether on-premises or in the cloud.

[Explore Email Products →](#)



Cloud Security

Unlock unparalleled protection and productivity across your organization.

[Explore Cloud Products →](#)

FireEye >> Trellix (Pokr.)

FireEye Security System:

- The FireEye Security System blokuje útoky cez webové a e-mailové vektory hrozieb a latentný malvér, ktorý sa nachádza na zdieľaných úložiskách.
- Dokáže blokovat' pokročilý malvér, ktorý ľahko obchádza tradičné obranné mechanizmy založené na signatúrach a ohrozuje väčšinu podnikových sietí.
- Rieši všetky fázy životného cyklu útoku pomocou signature-less engine, ktorý využíva stavovú analýzu útokov na odhalenie zero-day hrozieb.



Príklad nasadenia

Threat Intelligence

Výber vhodného nástroj pre FRI:

- Integrácia do SIEM ELK
- Modul Threat Intel ako súčasť Filebeat agenta
 - Vizualizácia – Kibana
 - Alerty na základe CTI
 - VM



kibana

Alerts TECHNICAL PREVIEW Rule count 2 Disabled 0 Snoozed 0 Errors 0 [Manage Rules](#)

Search alerts (e.g. kibana.alert.evaluation.threshold > 75) Last 24 hours

Status active 1 Rule Group Tags

Columns 11 Sort fields 1 4 alerts Fields Updated now

Actions	Alert Status	Feature	Last updated	Started	Rule category	Rule
...	Active	Stack management	May 30, 2024 @ 15:20:50.530	May 30, 2024 @ 15:20:50.530	Index threshold	kibana sites - low by
...	Active	Stack management	May 30, 2024 @ 15:20:50.530	May 30, 2024 @ 15:20:50.530	Index threshold	kibana sites - low by
...	Active	Stack management	May 30, 2024 @ 15:20:50.530	May 30, 2024 @ 15:20:50.530	Index threshold	kibana sites - low by
...	Active	Stack management	May 30, 2024 @ 15:20:50.530	May 30, 2024 @ 15:20:50.530	Index threshold	kibana sites - low by

Threat Intelligence

Výber vhodného nástroj pre FRI:

- Zdroje CTI:
 - Abuse.ch
 - Malware Bazaar
 - MISP
 - AlientVault OTX
 - Anomali Limo
 - Anomali ThreatStream (Platený)
 - Threat Quotient (Platený)

ABUSE | ch



Threat Intelligence

Výber vhodného nástroj pre FRI:

- Použité zdroje CTI:
 - Abuse.ch
 - abuseurl
 - abusemalware
 - AlientVault OTX
 - otx

URLhaus
from ABUSE^{ch} |  SPAMHAUS

ABUSE | ch



OPEN THREAT EXCHANGE
ALIEN VAULT

Integrácia CTI do monitoringu

LibreNMS

The screenshot displays the LibreNMS web interface. At the top, there is a navigation bar with icons for Overview, Devices, Maps, Services, Ports, Health, Wireless, Apps, Routing, Alerts, and a Global Search box. Below this, a device card for 'threat-intel' is highlighted with a red border. To the right of the device card are three small bar charts for Storage Usage, Memory Usage, and Processor Usage. A secondary navigation bar below the device card includes icons for Overview, Graphs, Health, Ports, Routing, Inventory, Logs, Alerts, Alert Stats, Latency, and Notes. The main content area is split into two panels. The left panel shows the details for the device 'Linux threat-intel 5.15.0-136-generic #147-Ubuntu SMP Sat Mar 15 15:53:30 UTC 2025 x86_64'. The right panel shows a 'Processors' graph for 'Intel Xeon E5-2690 0 @ 2.90GHz x4' with a 1% usage indicator.

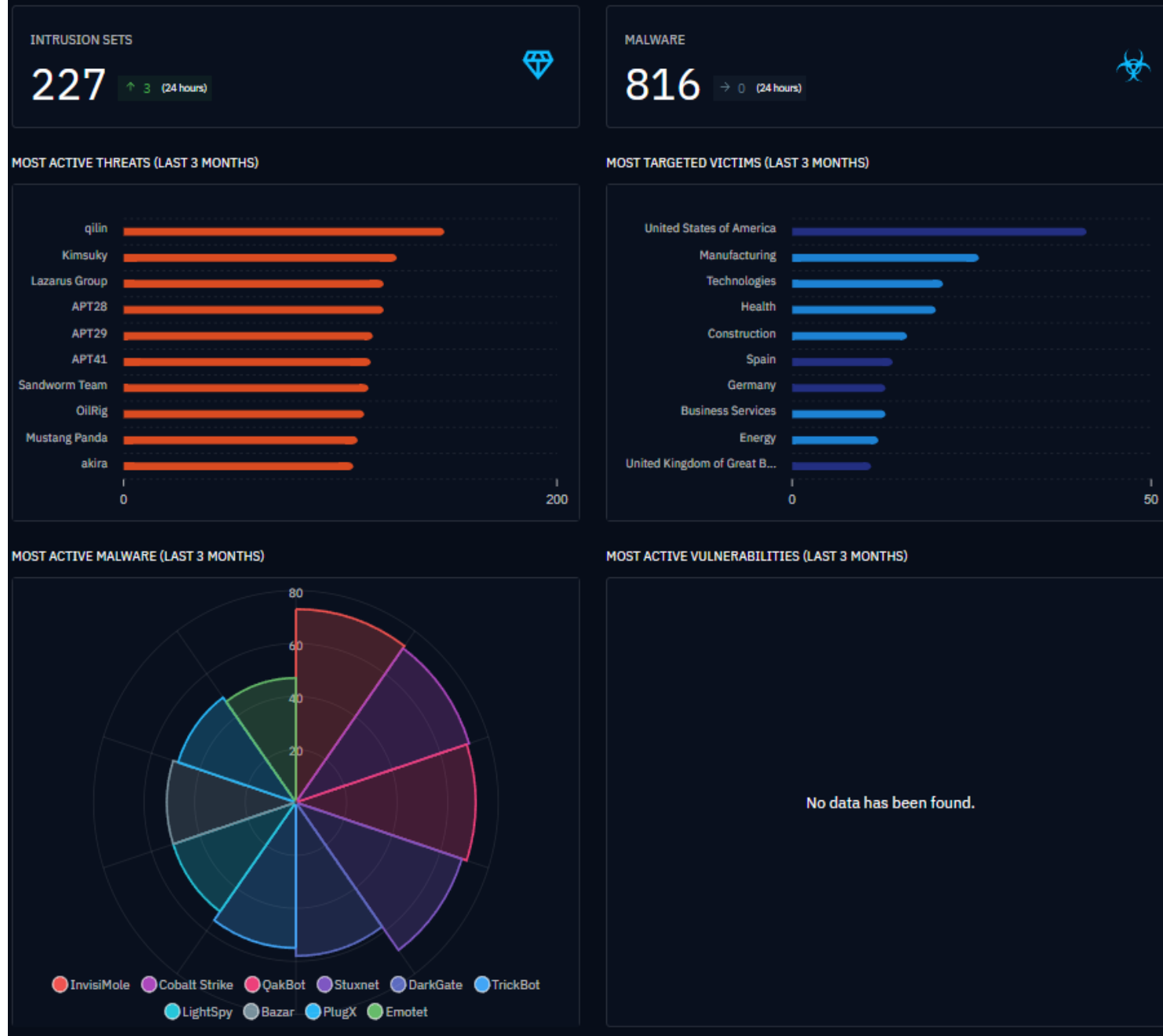
System Name	threat-intel
Resolved IP	[REDACTED]
Hardware	Generic x86 64-bit
Operating System	Linux 5.15.0-136-generic
Object ID	.1.3.6.1.4.1.8072.3.2.10
Contact	[REDACTED]
Device Added	1 week 2 days 4 hours 1 minute 1 second ago
Last Discovered	3 hours 45 minutes 36 seconds ago
Uptime	1 week 6 days 4 hours 45 minutes 46 seconds
Location	[REDACTED]
Lat / Lng	N/A

Processors

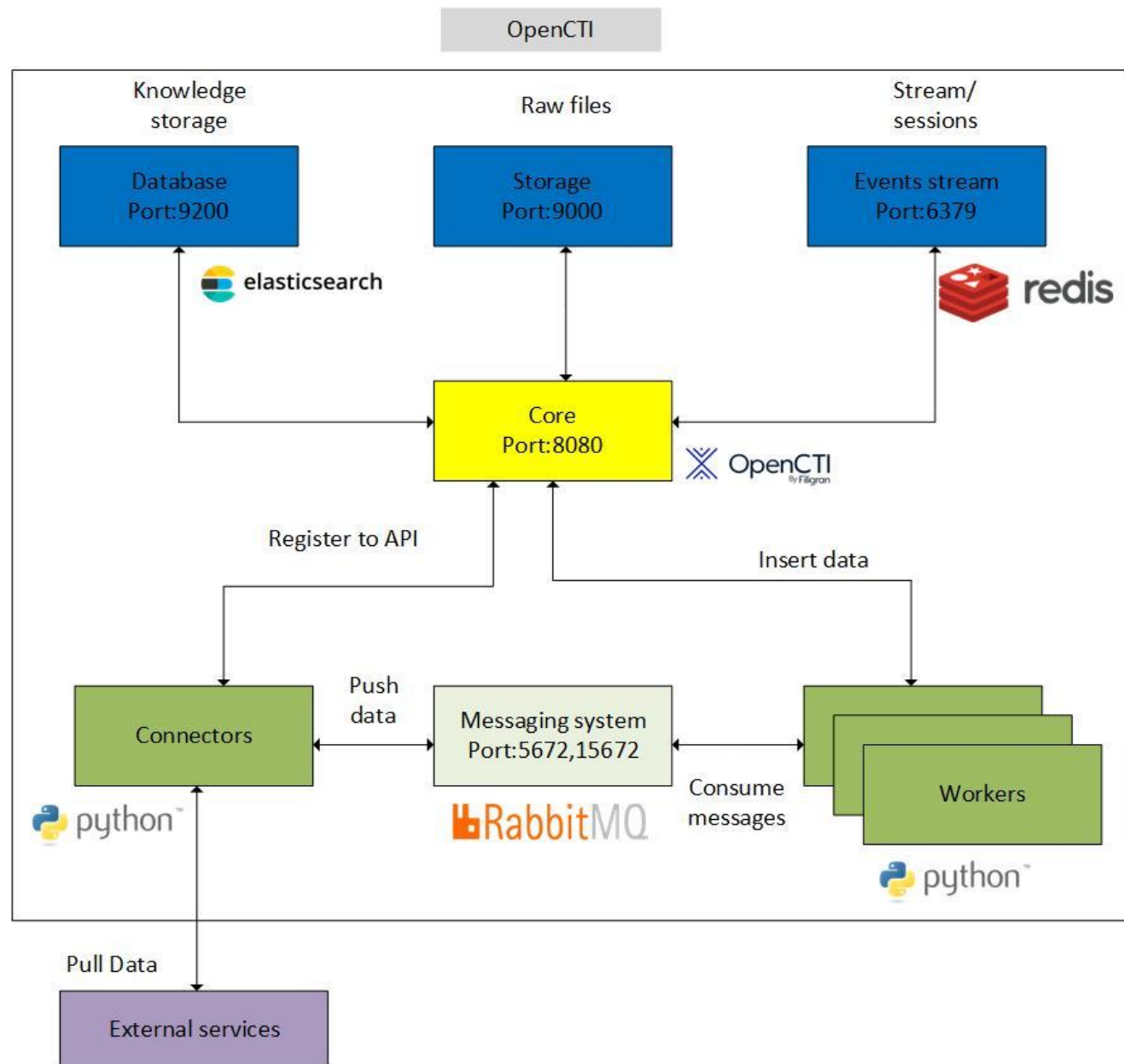
Intel Xeon E5-2690 0 @ 2.90GHz x4 1%

OpenCTI

- Open-source platforma, ktorá umožňuje centrálnu správu všetkých 4 typov CTI.
- Umožňuje zber, koreláciu a vizualizáciu dát o kybernetických hrozbách z interných aj externých zdrojov
- Pracuje s formátom STIX aj TAXII čo umožňuje jednoduchšiu prácu s jednotlivými zdrojmi CTI.
- Podporuje integráciu s viacerými databázami(abuse.ch, MISP, AlienVault OTX).



OpenCTI architektúra



Prepojenie s databázou ransomwarelive

dragonforce has published a new victim: Esposito Bros. Construction Ltd

UPDATE

OVERVIEW KNOWLEDGE CONTENT ENTITIES OBSERVABLES DATA

AI INSIGHTS ADD SECURITY COVERAGE

ENTITY DETAILS

Description

Esposito Bros. Construction Ltd. is a leading construction company based in Bolton, Ontario, recognized as one of the top bridge contractors. With over four decades of experience, the firm specializes in managing complex projects involving bridges, roads, demolition, and underground infrastructure. Their commitment to safety and innovation ensures that they provide exceptional construction...

Report types

RANSOMWARE-REPORT

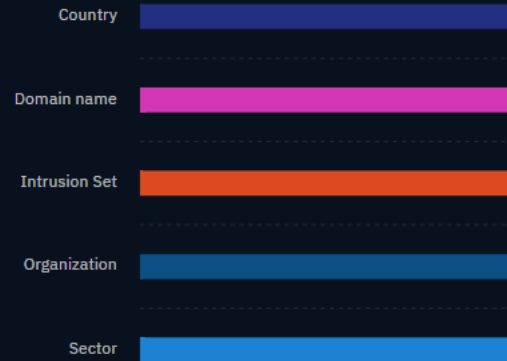
Publication date

February 6, 2026 at 2:12:51 AM

Correlated containers

No correlated containers has been found.

Entities distribution



BASIC INFORMATION

Marking

NONE

Author

RANSOMWARE.LIVE

Reliability (of author)

A - Completely rel...

Confidence level

1 - Confirmed b...

Distribution of opinions



Original creation date

February 6, 2026 at 2:12:51 AM

Processing status

NEW

Assignees

-

Participants

-

Revoked

NO

Labels

-

Platform creation date

February 6, 2026 at 11:15:16 AM

Creators

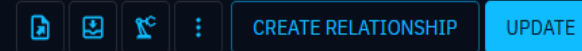
ADMIN

Standard STIX ID

report--5754d08d-c6c4-5e3c-854b-15bd9bba7189

Prepojenie s databázou URLHaus

http://130.12.180.43/files/8360091208/VD4ZhoY.exe



OVERVIEW KNOWLEDGE CONTENT ANALYSES SIGHTINGS DATA HISTORY

DETAILS

Indicator pattern

```
[url:value = 'http://130.12.180.43/files/8360091208/VD4ZhoY.exe']
```

Valid from

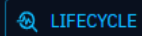
FEBRUARY 6, 2026 AT 11:09:06 AM

Valid until

MARCH 7, 2026 AT 4:51:56 PM

Score ?

80 / 100



Detection

NO

Description

Threat: malware_download - Reporter: Bitsight - Status: online

Kill chain phases

-

Indicator types

-

Main observable type

URL

Platforms

-

Based on +

URL http://130.12.180.43/files/8360091208/VD4ZhoY.exe Feb 6, 2026

BASIC INFORMATION

Marking

TLP:CLEAR

Author

ABUSE.CH

Reliability (of author)

Unknown

Confidence level

1 - Confirmed b...

Distribution of opinions ?



Pattern type

stix

Processing status

DISABLED

Revoked

NO

Labels +

-

Platform creation date

February 6, 2026 at 11:15:48 AM

Creators

ADMIN

Standard STIX ID ?

indicator--22b9560a-8236-5fdd-80fe-1e1882e59894

Original creation date

February 6, 2026 at 11:09:06 AM

Modification date

February 6, 2026 at 11:15:49 AM

Prepojenie s databázou Mitre Att&ck

3PARA RAT +

CREATE RELATIONSHIP UPDATE

OVERVIEW KNOWLEDGE CONTENT ANALYSES DATA HISTORY

AI INSIGHTS

DETAILS

Is family
YES

Description
3PARA RAT is a remote access tool (RAT) programmed in C++ that has been used by Putter Panda. (Citation: CrowdStrike Putter Panda)

Architecture execution env.
Unknown

Implementation languages
Unknown

Malware types
-

First seen
-

Last seen
-

Kill chain phases
-

Capabilities
Unknown

BASIC INFORMATION

Marking
Copyright 201...

Author
THE MITRE CORPORATION

Reliability (of author)
Unknown

Confidence level
2 - Probably True

Distribution of opinions

Processing status
DISABLED

Revoked
NO

Labels
+

Platform creation date
January 4, 2026 at 9:34:20 PM

Creators
[C] MITRE ATT&CK

Standard STIX ID
malware--13a5b23d-6cce-5d82-bde5-bd365846f206

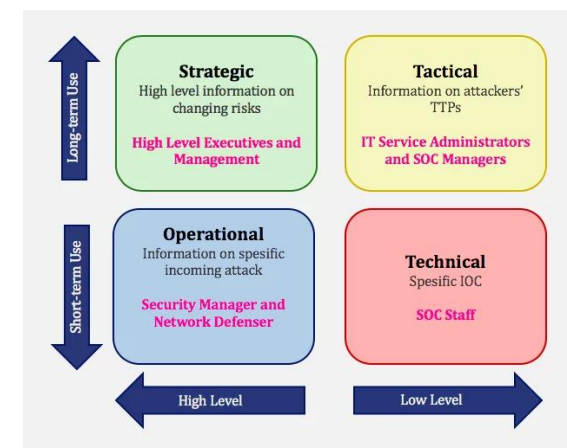
Original creation date
May 31, 2017 at 11:32:44 PM

Modification date
February 6, 2026 at 11:25:37 AM



Informačné zdroje pre špecialistov KB

Strategické CTI



Network Intelligence Communities

- Na účinnú ochranu siete musia byť odborníci na bezpečnosť neustále informovaní o hrozbách a zraniteľnostiach.
- Existuje mnoho bezpečnostných organizácií, ktoré poskytujú sieťové informácie, zdroje, semináre a konferencie na pomoc bezpečnostným profesionálom.
- Ak chce odborník na bezpečnosť siete zostať efektívny, musí:
 - **Keep abreast of the latest threats** – Zahŕňa odber real-time noviniek týkajúcich sa hrozieb, pravidelné sledovanie webových stránok súvisiacich s bezpečnosťou, sledovanie bezpečnostných blogov a podcastov a ďalšie.
 - **Continue to upgrade skills** – Zahŕňa účasť na školeniach, seminároch a konferenciách týkajúcich sa bezpečnosti.
- **Poznámka:** Bezpečnosť sietí je veľmi náročná na učenie a vyžaduje si záväzok neustáleho profesionálneho rozvoja.

Network Intelligence Communities (Pokr.)

V tabuľke sú uvedené dôležité organizácie týkajúce sa bezpečnosti siete.

Organizácia	Popis
SysAdmin, Audit, Network, Security (SANS)	<p>Zdroje inštitútu SANS sú zväčša bezplatné na požiadanie a zahŕňajú:</p> <ul style="list-style-type: none">• The Internet Storm Center – populárny systém „včasného varovania“• NewsBites – týždenný prehľad spravodajských článkov o počítačovej bezpečnosti• @RISK - Týždenný prehľad novoobjavených vektorov útokov, zraniteľností s aktívnymi exploitmi a vysvetlenia fungovania nedávnych útokov• Flash security alerts• Reading Room – viac ako 1,200 ocenených, originálnych výskumných článkov <p>SANS tiež vyvíja bezpečnostné kurzy</p>
Mitre	<p>Spoločnosť Mitre Corporation spravuje zoznam Common Vulnerabilities and Exposures (CVE), ktorý používajú významné bezpečnostné organizácie</p>

Network Intelligence Communities (Pokr.)

Organizácia	Popis
Forum of Incident Response and Security Teams (FIRST)	Je to bezpečnostná organizácia, ktorá združuje rôzne tímy pre reakciu na počítačové bezpečnostné incidenty z vládných, komerčných a vzdelávacích organizácií s cieľom podporiť spoluprácu a koordináciu pri výmene informácií, prevencii incidentov a rýchlej reakcii .
SecurityNewsWire	Bezpečnostný spravodajský portál, ktorý zhromažďuje najnovšie aktuálne správy týkajúce sa výstrah, exploitov a zraniteľností .
International Information Systems Security Certification Consortium (ISC) ²	Poskytuje vendor neutral vzdelávacie produkty a kariérne služby pre viac ako 75 000 profesionálov vo viac ako 135 krajinách.
Center for Internet Security (CIS) ..MS-ISAC	Je to ústredný bod pre prevenciu, ochranu, reakciu a obnovu kybernetických hrozieb pre štátne, miestne, kmeňové a územné samosprávy (SLTT) prostredníctvom Multi-State Information Sharing and Analysis Center (MS-ISAC) . MS-ISAC ponúka 24x7 výstrahy a odporúčania týkajúce sa kybernetických hrozieb, identifikáciu zraniteľností a zmierňovanie a reakciu na incidenty.

Cisco Cybersecurity Reports

- Zdroje, ktoré pomáhajú odborníkom na bezpečnosť udržať si prehľad o najnovších hrozbách
 - the Cisco **Annual** Cybersecurity Report
 - the **Mid-Year** Cybersecurity Report.
- Tieto správy poskytujú **aktuálne** informácie o stave
 - bezpečnostnej pripravenosti
 - odbornú analýzu top zraniteľností
 - faktory, ktoré stoja za prudkým nárastom útokov využívajúcich adware, spam a pod.
- Analytici v oblasti kybernetickej bezpečnosti by si mali tieto reporty predplatiť a prečítať, aby sa dozvedeli:
 - ako sa útočníci zameriavajú na ich siete,
 - a aké **opatrenia možno prijať na zmiernenie** týchto útokov.

Ukážka reportu z r. 2018:

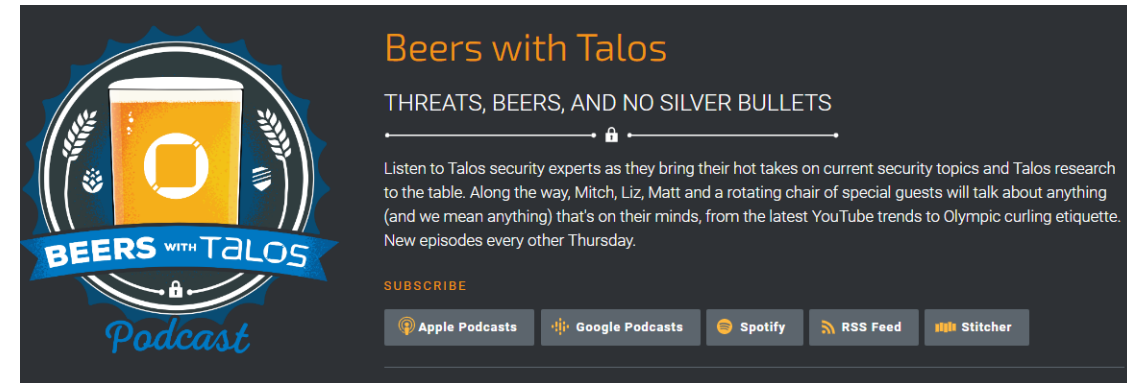
Table of contents

Executive summary	3
Part I: The attack landscape	6
The evolution of malware	6
Encrypted malicious web traffic	9
Email threats	14
Sandbox evasion tactics	22
Abuse of cloud services and other legitimate resources.....	24
IoT and DDoS attacks.....	31
Vulnerabilities and patching	38
Part II: The defender landscape	46
The cost of attacks	46
Challenges and obstacles	47
Complexity created by vendors in orchestration	48
Impact: Public scrutiny from breaches, higher risk of losses	50
Services: Addressing people and policies, as well as technology.....	53
Expectations: Investing in technology and training	54
Conclusion	57
About Cisco	60
Appendix	65

Security Blogs and Podcasts

- Blogy a podcasty tiež poskytujú
 - poradenstvo
 - výskum
 - odporúčané techniky na zmiernenie následkov
- Cisco poskytuje blogy na témy súvisiace s bezpečnosťou od viacerých odborníkov z odvetvia a od skupiny Cisco Talos Group.
- Cisco Talos ponúka sériu viac ako 80 podcastov, ktoré si môžete prehrať z internetu alebo stiahnuť do Vášho zariadenia.

<https://www.talosintelligence.com/podcasts>

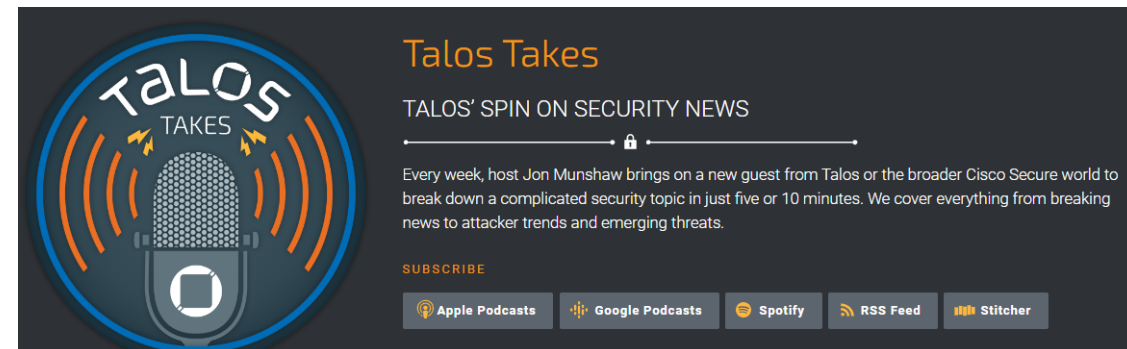


[Im a skiddie, and you can too!](#)

[The intricacies of cyber conflict in Ukraine](#)

[A\(nother\) new host approaches!](#)

....



[The best \(and free\) ways to improve your cybersecurity skills](#)

[The basics of threat hunting](#)

[Tips for kickstarting your cybersecurity career](#)

[The latest on Lockbit 3.0 drama and the rest of the ransomware landscape](#)



Otvorená reflexia

- **Čo je hlavným cieľom STIX v oblasti CTI?**
 - a) Automatizované blokovanie IP adries
 - b) Štandardizovať spôsob reprezentácie hrozieb a IOC
 - c) Detekcia malvéru v reálnom čase
 - d) Monitorovanie sieťovej prevádzky
- **Ktoré tvrdenie najlepšie popisuje CAPEC?**
 - a) Zoznam známych zraniteľností v softvéri
 - b) Databáza občianskych kybernetických incidentov
 - c) Katalóg útokových vzorov, ktorý popisuje spôsob vykonania útoku
 - d) Nástroj na patch management
- **Ktorý typ CTI sa zameriava na dlhodobé trendy, geopolitiku a strategické rozhodovanie?**
 - a) Technické CTI
 - b) Taktické CTI
 - c) Operačné CTI
 - d) Strategické CTI
- **Ktorý z nasledujúcich rámcov obsahuje taktiky, techniky a postupy (TTP) útočníkov?**
 - a) CWE
 - b) MITRE ATT&CK
 - c) CVE
 - d) CAPEC
- **Ktorá platforma slúži na zdieľanie indikátorov kompromitácie (IOC) a je široko využívaná CERT tímami a vládnyimi organizáciami?**
 - a) Shodan
 - b) OpenVAS
 - c) MISP
 - d) Nessus



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



KOMPETENČNÉ CENTRUM
KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Spravodajstvo o hrozbách (CTI)

Moderné technológie, bezpečnosť cloudu a IoT (Blok VII)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, <https://kc.uniza.sk/>

Jana.Uramova@fri.uniza.sk