PROJEKT

Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia

# Podklad pre V4

## Návrh a implementácia procesu pre threat intelligence

Prepojené s pracovným balíkom KPB2 – Návrh SOCaaS služby

# Obsah

**1. Návrh a implementácia procesu pre threat intelligence ..... 3**
**2. Preskúmanie dostupných nástrojov a platforiem pre Threat Intelligence ..... 4**
2.1. ThreatConnect ..... 4
2.2. Recorded Future ..... 5
2.3. Anomali ThreatStream ..... 6
2.4. Porovnanie vybraných riešení ..... 6
**3. Výber vhodného nástroj pre SOC centrum ..... 8**
3.1. Testovacie nasadenie Modul Threat Intel ako súčasť Filebeat agenta ..... 8
**Zoznam zdrojov ..... 10**

# 1. NÁVRH A IMPLEMENTÁCIA PROCESU PRE THREAT INTELLIGENCE

Pojem Threat Intelligence, ktorý je v posledných rokoch neoddeliteľnou súčasťou kybernetickej bezpečnosti, v ktorej má aj zaužívanú skratku CTI (Cyber Threat Intelligence). Podľa spoločnosti Gartner: „*Threat Intelligence predstavuje znalosti podložené dôkazmi, zahŕňajúce kontext, mechanizmy, indikátory, dôsledky a praktické odporúčania týkajúce sa existujúcich alebo novovznikajúcich rizík ohrozujúcich aktíva. Tieto informácie pomáhajú pri rozhodovaní o vhodnej reakcii na dané hrozby.*“

CTI by malo pomôcť získať odpovede na nasledujúce otázky:

- Kto predstavuje hrozbu pre našu organizáciu a akými metódami môže vykonať útok?
- Ako ovplyvňujú vektory útokov bezpečnosť našej organizácie?
- Na čo by mal dohliadať náš SOC tím?
- Ako môžeme znížiť riziko kybernetického útoku na našu organizáciu?

CTI sú informácie, ktoré pomáhajú organizáciám lepšie pochopiť hrozby a prijať vhodné opatrenia na ich zmiernenie, pričom sa rozdeľujú do troch kategórií:

1. Strategické CTI
2. Operačné CTI
3. Taktické CTI

**Strategické CTI**
Poskytuje široký pohľad na vývoj kybernetických hrozieb v čase, identifikáciu motivácií útočníkov a ich historické vzorce správania. Pomáha odpovedať na otázky „Kto?“ a „Prečo?“ tým, že analyzuje atribúciu útokov, trendy v aktivitách hrozieb a ich vzťah k geopolitickým konfliktom. Zahŕňa mapovanie útokov na globálne udalosti, štatistické prehľady o porušeniach bezpečnosti, zmeny v TTP (taktiky, techniky a procedúry) útočníkov a analýzu sektorovo špecifických hrozieb. Umožňuje posúdiť technologické, dodávateľské reťazce a identifikovať kľúčové oblasti ohrozenia organizácie a prijať lepšie strategické rozhodnutia o kybernetickej bezpečnosti a investíciách do nej.

**Operačný CTI**
Poskytuje odpovede na otázky „Ako?“ a „Kde?“ tým, že analyzuje metodiky útočníkov (TTP) a identifikuje ich aktivity v rôznych prostrediach. Zahŕňa stručné písomné správy o hrozbách, profily obetí a útočných skupín a konkrétne detaily útokov, ako sú nástroje, komunikačné kanály a techniky pretrvávania v systémoch. Pomáha analytikom pochopiť spôsob útoku a miesto jeho realizácie, čím podporuje lepšie reakcie na incidenty a proaktívne vyhľadávanie neznámych hrozieb. Dáva kontext pre vyšetrenie kybernetických útokov a zlepšenie obranných stratégií.

**Taktické CTI** sa zameriava na identifikáciu a analýzu IOC. Slúži primárne na automatizovanú detekciu hrozieb v rámci systémov. Môže byť taktiež využitý na obohatenie bezpečnostných upozornení, napríklad v systémoch SIEM na poskytnutie väčšieho kontextu pre rozhodnutie, ktoré hrozby môžeme bezpečne ignorovať, a pri ktorých je potrebné detailnejšie preskúmanie a aplikovanie komplexnejších bezpečnostných opatrení. A teda môže týmto spôsobom napomáhať pri analýze incidentu analytikom nájsť špecifické artefakty a lepšie ho zdokumentovať. Pre zhrnutie, taktické CTI môže obsahovať napríklad hash súborov, IP adresy, URL adresy a IOC.

Pre lepšie pochopenie rozdielov, sme ich porovnali v prehľadnej tabuľke Tab. 1 nižšie.

Tab. 1 - Kategórie Threat Intelligence

| Typ | Zodpovedá otázky | Zameranie | Výstupné dáta |
|---|---|---|---|
| **Strategický** | Kto? Prečo? | Netechnické | Rozsiahle písomné správy, mapovanie útokov a kampaní na konflikty a ďalšie |
| **Operačný** | Ako? Kde? | Zmiešané | Stručné písomné správy, profily obetí a skupín, popis TTP a ďalšie |
| **Taktický** | Čo? | Technické | Strojovo čitateľné indikátory ako IP adresy, domény, IOC (Indicators of compromise) a signatúry |
| Dáta boli získane z oficiálneho webu spoločnosti Anomali [25]. | | | |

Z tabuľky Tab. 1 vyššie nám vyplýva, že pre prostredie, kde chceme implementovať technické opatrenia pre zabezpečenie IT infraštruktúry pred kybernetickými hrozbami, je potrebný taktický Threat Intelligence, ktorý je ako jediný aj reálne prakticky aplikovateľný v našom prípade.

# 2. PRESKÚMANIE DOSTUPNÝCH NÁSTROJOV A PLATFORIEM PRE THREAT INTELLIGENCE

V tejto časti preskúmame dostupné možnosti pre implementáciu Taktického CTI. Riešení pre CTI existuje samozrejme mnoho, ale nie je v možnostiach tejto diplomovej práce preskúmať úplne všetky, a preto sa zameriame na vybrané riešenia v zadaní práce.

## 2.1. ThreatConnect

Threat Intelligence Platform (TIP) od ThreatConnect umožňuje organizáciám zhromažďovať, obohacovať a analyzovať všetky zdroje na jednej platforme, čím umožňuje prioritizáciu a reakciu na najkritickejšie hrozby. Platforma využíva silu AI a automatizácie na zjednodušenie a zrýchlenie detekcie a reakcie na hrozby, čím zvyšuje efektivitu. Tento nástroj teda inými slovami pokrýva všetky tri typy CTI, teda strategický, operatívny a taktický. Keďže nás však primárne zaujíma taktický CTI, zameriame sa iba na vybrané funkcie tohto nástroja, ktoré sú relevantné pre túto oblasť, a ktoré by podľa nášho názoru mohli byť užitočné v akademickom prostredí.

**Funkcionalita:**

1. **Jednotný zdroj threat intelligence**
   Umožňuje automatizované zhromažďovanie, normalizáciu a obohacovanie rôznych zdrojov dát. Týmto spôsobom sa eliminuje potreba manuálneho spracovania a zjednocovania dát z rôznych zdrojov, čo šetrí čas a zvyšuje efektivitu. Platforma podporuje integráciu s rôznymi zdrojmi, vrátane komerčných, open source,

komunitných a interných zdrojov, čím zabezpečuje komplexný a aktuálny prehľad o hrozbách.

2. **Automatizácia práce analytikov**
   Táto funkcionalita zahŕňa:
   – **Automatizované playbooky**
     Umožňujú rýchlu automatizáciu vlastných procesov pomocou jednoduchého drag-and-drop rozhrania, čím sa znižuje potreba programátorských zručností.
   – **AI a automatizácia**
     Collective Analytics Layer (CAL) Automated Threat Library (ATL) zhromažďuje a analyzuje viac ako 60 autoritatívnych zdrojov otvorených informácií. Automatická detekcia taktík a techník MITRE ATT&CK, CVE, indikátorov a AI-generovaných súhrnov šetrí analytikom hodiny manuálnej práce denne.
   – **Automatizované obohacovanie dát**
     Využíva tretie strany ako VirusTotal, Shodan, DomainTools a URLScan.io na automatické obohacovanie dát, čím poskytuje analytikom akčné informácie bez potreby manuálneho zásahu.

3. **Vizualizácia threat intelligence**
   Pomáha analytikom efektívne skúmať správanie útočníkov, identifikovať taktiky a techniky, a zlepšiť tímovú spoluprácu pomocou MITRE ATT&CK frameworku. Zameriava sa však na taktickú úroveň CTI, kde umožňuje rýchlu detekciu a reakciu na konkrétne hrozby.

## 2.2. Recorded Future

Umožňuje organizáciám identifikovať, vyšetrovať a prioritizovať kybernetické hrozby. Platforma využíva pokročilé analytické nástroje a automatizáciu na zjednodušenie a zrýchlenie detekcie a reakcie na hrozby, čím zvyšuje efektivitu. Tento nástroj taktiež pokrýva už spomínané všetky tri kategórie CTI. Rovnako ako pri predchádzajúcom nástroji, tak aj pri tomto si uvedieme len funkcie relevantné k taktickému CTI a k využitiu v akademickom prostredí.

**Funkcionalita:**

1. **Posilnenie opatrení na elimináciu hrozieb**
   Poskytuje podrobný kontext potrebný na prijatie účinných opatrení. To zahŕňa IOC, prispôsobiteľný sandbox na testovanie a takzvané „hunting packages“, ktoré pomáhajú analytikom pri aktívnom vyhľadávaní hrozieb. Každý balík je zameraný na konkrétneho aktéra hrozby, malvérovú kampaň alebo škodlivý softvér. Tieto balíky obsahujú YARA a SNORT pravidlá, ktoré umožňujú ich jednoduchú implementáciu do bezpečnostných riešení. Jedná sa teda aj o proaktívny prístup k hrozbám.
2. **Vizualizácia threat intelligence**
   Umožňuje rýchlejšie a s väčšou istotou reagovať na upozornenia, ktoré sú pre organizáciu relevantné.

Funkcionalita tohto nástroja je na oficiálnom webe prezentovaná veľmi špecificky, a jej interpretácia je v porovnaní s predchádzajúcim nástrojom menej prehľadná a náročnejšia na porozumenie.

## 2.3. Anomali ThreatStream

„Poskytuje prístup k najväčšiemu globálnemu úložisku starostlivo vybraných informácií o hrozbách. Táto platforma umožňuje obohatenie, kontextualizáciu a detekciu známych a novovznikajúcich hrozieb, prispôsobených danej organizácii“. Tento nástroj tiež pokrýva všetky tri typy CTI. V súlade s predchádzajúcimi nástrojmi sa aj pri Anomali ThreatStream zameriame na funkcie relevantné pre taktické CTI a jeho využitie v akademickom prostredí.

**Funkcionalita:**

1. **Rozsiahle integrácie**
   Prístup k rozsiahlemu ekosystému tretích strán, vrátane zdrojov informácií o hrozbách, obohacovacích dát a nástrojov, bez duplicitných alebo zastaraných dát.
2. **Orchestrácia informácií o hrozbách**
   Umožňujú automatizované zdieľanie bezpečnostných dát naprieč firewallmi, SIEM systémami, proxy servermi, DNS, endpoint protection platforms (EPP) a ďalšími riešeniami.

## 2.4. Porovnanie vybraných riešení

Všetky vybrané riešenia vyzerajú zaujímavo a zbierajú informácie o hrozbách z rôznych komerčných aj bezplatných zdrojov a normalizujú ich na jednotný formát. Tieto komerčné zdroje sa pri jednotlivých nástrojoch môžu líšiť, ale v podstate ide iba o to, aké partnerstvá má uzavreté daná spoločnosť, ktorá stojí za vývojom nástroja. Okrem toho dokáže každý z týchto nástrojov tieto dáta pekne vizualizovať a vykresľovať rôzne grafy. Každý si však informácie o funkcionalite nástroja interpretuje vlastným spôsobom, čo aj komplikuje neskoršie porovnanie jednotlivých nástrojov a zorientovaní sa v rozdieloch medzi nimi, pokiaľ neberieme do úvahy cenu. Skutočný rozdiel teda zrejme spočíva iba v dodatočnej funkcionalite.

Recorded Future obsahuje dodatočne funkciu integrovaného prispôsobiteľného sandbox testovacieho prostredia, a už spomínané takzvané „hunting packages“, v ktorých vidíme významný potenciál pri reakcií na hrozby. Tieto dve funkcionality môžu byť dôvodom, prečo sa tento nástroj nachádza na prvej priečke v hodnotení Gartner v kategórií Threat Intelligence produktov, aspoň v čase tohto projektu.

Anomali ThreatStream obsahuje podobnú funkcionalitu, ktorú však popisujú mierne odlišným spôsobom. Vzhľadom na to, že tieto nástroje nebolo možné prakticky vyskúšať, rozdiely medzi ich funkcionalitou je ťažké hodnotiť. ThreatConnect uvedené funkcionality neuvádza, ale poskytuje automatizované playbooky a integráciu AI do procesov automatizácie, ktoré môžu byť v praxi taktiež veľmi prínosné.

Finálne na základe funkcionality, hodnotenia Gartner, ako aj zákazníkov, ktorí sa spoliehajú na toto riešenie, ako napríklad Microsoft, Amazon a Cisco, by sme zvolili jednoznačne nástroj Recorded Future, pretože ich „hunting packages“ môžu byť silným nástrojom pre implementácie do praxe. V tabuľke Tab. 2 nižšie sme porovnali nástroje z pohľadu ceny, a či tieto nástroje obsahujú aspoň obmedzenú bezplatnú verziu.

Tab. 2 - Porovnanie vybraných riešení pre Threat Intelligence

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

Ako môžeme vidieť v tabuľke Tab. 2 vyššie, všetky nástroje obsahujú aj taktický CTI, teda spĺňajú naše potreby, ale cena je k dispozícii len na vyžiadanie, čo naznačuje, že ani z ďaleka nebude nízka, a teda pre rozpočet menšej organizácie určite nie prívetivá. Bezplatnú alternatívu z týchto nástrojov ponúkala v minulosti spoločnosť Anomali, a aktuálne ponúka len spoločnosť ThreatConnect.
Bezplatný nástroj s názvom STAXX od Anomoli má samozrejme obmedzenú funkcionalitu a umožňuje sťahovať dáta z rôznych bezplatných zdrojov o hrozbách pomocou STIX/TAXII, ktoré je možné v ňom nakonfigurovať. Umožňuje samozrejme nakonfigurovať aj komerčné zdroje o hrozbách, avšak tu už končí v tejto chvíli jeho bezplatnosť. Okrem získania dát o hrozbách si ich v tomto nástroji vieme vizualizovať a manuálne prehľadávať, čo nám pri aktuálnych možnostiach komerčných nástrojov príde dosť neefektívne, navyše mu končí oficiálna podpora a nebude už dostávať aktualizácie, preto sme uviedli, že spoločnosť Anomali aktuálne už neponúka bezplatné riešenie.

Čo sa týka bezplatného riešenia od spoločnosti ThreatConnect s názvom Polarity Community Edition, ktoré má v porovnaní s jeho platenou verziou, samozrejme obmedzenú funkcionalitu, ale v porovnaní s Anomali STAXX prináša ešte aj v dnešnej dobe pridanú hodnotu. Funkcia tohto nástroja s názvom Focus spočíva v možnosti definovať konkrétnu oblasť obrazovky, ktorá nás zaujíma, ako napríklad MD5 hash súboru alebo bezpečnostné upozornenie. Pomocou kurzora počítačovej myši si používateľ označí požadovanú oblasť, ktorá je následne zachytená formou snímky obrazovky. Táto snímka slúži ako podklad pre automatizované vyhľadávanie dodatočných údajov o hrozbách. Jedná sa o zaujímavú funkcionalitu, avšak stále je tu nutná manuálna práca analytika, ktorý prehliada dáta, napríklad zo SIEM systému, a z nášho pohľadu je tu malá miera automatizácie. Ako sme si uviedli na začiatku prvej kapitoly, taktický CTI primárne slúži na automatizovanú detekciu hrozieb, čo z pohľadu tejto definície nie je úplne pri takomto riešení dosiahnuté.

# 3. VÝBER VHODNÉHO NÁSTROJ PRE SOC CENTRUM

Pred výberom konkrétneho riešenia je nevyhnutné pochopiť mechanizmy fungovania dostupných nástrojov na spracovanie CTI a analyzovať procesy, ktoré sa na pozadí odohrávajú. V prípade bezplatných variantov sú informácie o hrozbách získavané automaticky z voľne dostupných zdrojov, následne normalizované a sprístupnené na manuálnu analýzu, či vizualizáciu. Výnimkou je nástroj Polarity Community Edition, ktorý umožňuje poloautomatizované prehľadávanie týchto údajov.
Platené riešenia samozrejme poskytujú výrazne vyšší stupeň automatizácie. Platené nástroje navyše zahŕňajú aj komerčné zdroje hrozieb, čím rozširujú dostupné údaje a väčšinou obsahujú integrácie so systémami, ako napríklad SIEM alebo firewall, ktoré vedia tieto údaje ďalej využiť pri automatizovanej detekcii hrozieb. Avšak v menších organizáciách je dôležité minimalizovať náklady na technologické riešenia, a v takomto prípade máme k dispozícií iba bezplatné zdroje hrozieb, a taktiež je tu absencia pokročilých funkcionalít.
Dôležitou požiadavkou pre tento projekt bolo vyhnúť sa spoplatneným nástrojom. Bohužiaľ, z vybraných riešení spĺňa túto požiadavku len ThreatConnect a jeho riešenie Polarity Community Edition, ktoré však úplne nespĺňa požiadavku na plne automatizovaný proces.

## 3.1. Testovacie nasadenie Modul Threat Intel ako súčasť Filebeat agenta

S cieľom centralizovaného spracovania a vizualizácie údajov o hrozbách bola navrhnutá implementácia prostredníctvom modulu Threat Intel, ktorý je súčasťou agenta Filebeat. Tento modul umožňuje automatizované získavanie údajov z rôznych dostupných zdrojov vrátane bezplatných, pričom je zabezpečená ich okamžitá aplikácia v podobe bezpečnostných upozornení. Medzi spracovávané CTI dáta patria napríklad IP adresy, URL adresy a hashe súborov.

Modul zároveň poskytuje možnosť obohacovania už existujúcich údajov a ich následnej kontextualizácie, čím je umožnené lepšie porozumenie súvislostiam identifikovaných hrozieb. Vzhľadom na schopnosť takéhoto riešenia pracovať nad širokou škálou dátovej prevádzky, bolo vyhodnotené ako vhodné miesto pre implementáciu CTI procesu.
Implementácia Threat Intel modulu v prostredí ELK zabezpečuje plynulú integráciu CTI, eliminuje potrebu dodatočnej normalizácie údajov a umožňuje ich efektívnu vizualizáciu. Keďže Kibana je už súčasťou infraštruktúry, vizualizácia údajov o hrozbách môže byť realizovaná priamo v nej, čím sa proces zjednodušuje a eliminuje sa potreba používania ďalších webových rozhraní.
Keďže väčšina prevádzky je v dnešnej dobe prenášaná šifrovane, tak bez využitia funkcie SSL inšpekcie je náročné odhaliť škodlivú prevádzku, a teda napríklad hash súborov vieme porovnávať iba s tými, ktoré sa prenášajú nešifrovanou prevádzkou alebo boli získané zo zariadení, kde máme nasadených auditbeat agentov.

Modul Threat Intel umožňuje zbierať dáta o hrozbách z nasledujúcich zdrojov:

- **Abuse.ch**: Poskytuje komunitné informácie o hrozbách, zamerané na boj proti malvéru a botnetom. Jeho kľúčovým partnerom je **Spamhaus**, ktorý poskytuje podporu a spoluprácu pri prevádzke. Na tomto projekte spolupracuje 15 000 špecializovaných výskumníkov.
- **Malware Bazaar:** Platforma od abuse.ch a Spamhaus, ktorá je určená na zdieľanie vzoriek malvéru s komunitou infosec, antivírusovými dodávateľmi a poskytovateľmi informácií o hrozbách .
- **MISP:** Malware Information Sharing Platform (MISP) je open source platforma na zdieľanie informácií o hrozbách, spolu založená s Európskou úniou. Umožňuje organizáciám zbierať, ukladať, distribuovať a zdieľať IOC. Podporuje automatizáciu, vizualizáciu dát a integráciu s nástrojmi.
- **AlientVault OTX:** Open Threat Exchange (OTX) je komunitne riadená platforma na zdieľanie informácií o hrozbách. Poskytuje prístup k viac ako 20 miliónom IOC denne, ku ktorým prispieva viac ako 200 000 účastníkov z celého sveta .
- **Anomali Limo:** Bezplatný zdroj o hrozbách, ktorý využíva už nepodporovaný nástroj STAXX od Anomali.
- **Anomali ThreatStream:** Jedná sa o integráciu s týmto plateným nástrojom.
- **ThreatQuotient:** Rovnako ako v predchádzajúcom bode, je to integrácia s plateným nástrojom.

# ZOZNAM ZDROJOV

1. **Gartner, Inc.,** *Definition: Threat Intelligence.* [online]. 10.4.2025. Dostupné na internete: <https://www.gartner.com/en/documents/2487216>
2. **Anomali Inc.,** *What is threat intelligence?.* [online]. 10.4.2025. Dostupné na internete: <https://www.anomali.com/resources/what-is-threat-intelligence>
3. **ThreatConnect,** *TI Ops: An Evolved Threat Intelligence Platform.* [online]. 10.4.2025. Dostupné na internete: <https://threatconnect.com/threat-intelligence-platform/?>
4. **ThreatConnect,** *Unified Threat Library.* [online]. 10.4.2025. Dostupné na internete: <https://threatconnect.com/solutions/unified-threat-library/>
5. **ThreatConnect,** *Unleash Efficiency Through Automation.* [online]. 10.4.2025. Dostupné na internete: <https://threatconnect.com/solutions/automation/?>
6. **ThreatConnect,** *Understand the Attacker and Take Action.* [online]. 10.4.2025. Dostupné na internete: <https://threatconnect.com/solutions/attck-visualizer/?>
7. **Recorded Future, Inc.,** *Identify, investigate, and prioritize cyber threats.* [online]. 10.4.2025. Dostupné na internete: <https://www.recordedfuture.com/products/threat-intelligence>
8. **Recorded Future, Inc.,** *Special Delivery: Recorded Future Hunting Packages.* [online]. 10.4.2025. Dostupné na internete: <https://www.recordedfuture.com/blog/threat-hunting-packages>
9. **Anomali Inc.,** *Harness the Power of Global Threat Intelligence.* [online]. 10.4.2025. Dostupné na internete: <https://www.anomali.com/products/threatstream>
10. **Anomali Inc.,** *STAXX - Your Free STIX/TAXII Solution.* [online]. 10.4.2025. Dostupné na internete: <https://www.anomali.com/resources/staxx>
11. **ThreatConnect,** *Get Started with Polarity Community Edition.* [online]. 10.4.2025. Dostupné na internete: <https://threatconnect.com/polarity-community-edition>
12. **Abuse.ch,** *FIGHTING MALWARE AND BOTNETS.* [online]. 11.4.2025. Dostupné na internete: <https://abuse.ch/>
13. **Abuse.ch,** *MalwareBazaar.* [online]. 11.4.2025. Dostupné na internete: <https://bazaar.abuse.ch/>
14. **MISP project,** *Open Source Threat Intelligence and Sharing Platform.* [online]. 11.4.2025. Dostupné na internete: <https://www.misp-project.org/>
15. **LevelBlue, Inc.,** *The World's First Truly Open Threat Intelligence Community.* [online]. 11.4.2025. Dostupné na internete: <https://otx.alienvault.com/>
16. **Elasticsearch B.V.,** *Threat Intel module.* [online]. 11.4.2025. Dostupné na internete: <https://www.elastic.co/docs/reference/beats/filebeat/filebeat-module-threatintel>
17. **Anomali,** *Download STAXX 3.4.* [online]. 11.4.2025. Dostupné na internete: <https://www.anomali.com/resources/staxx/download-staxx>