

Cyber Threat Intelligence

Od podataka do odluke: osnove, metodologije, frejmvorci i praktična primena CTI u odbrani IKT sistema



Predavač: DarkoS
CISO @ DCT



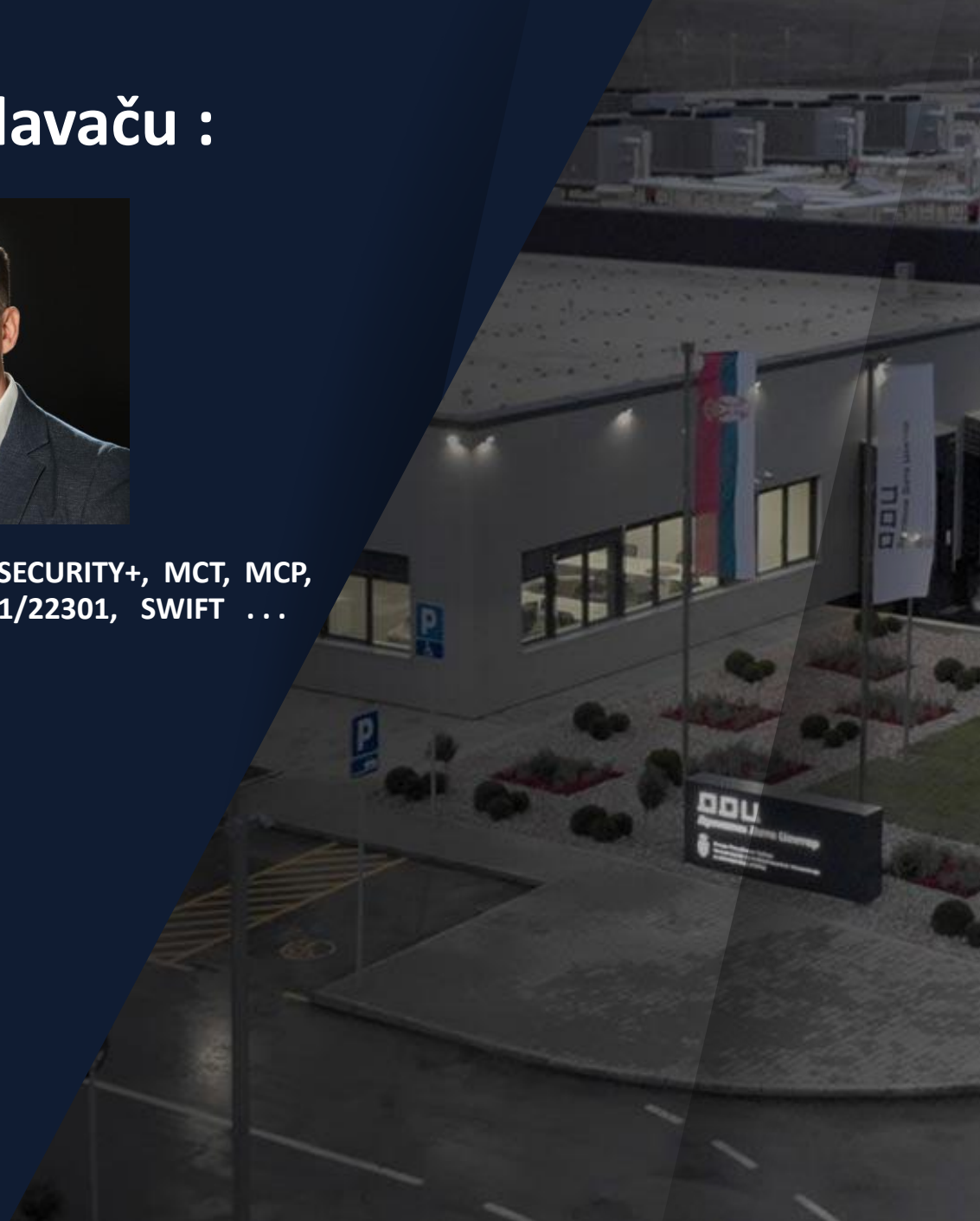
O predavaču :



CISSP, CEH, CTIA, SECURITY+, MCT, MCP,
ISO LA 27001/27701/22301, SWIFT ...



Државни Дата Центар





Data Cloud Technology d.o.o.
Kragujevac
Osnivač: Vlada Republike Srbije
Državno vlasništvo 100%

Komercijalni korisnici

Pružanje IT usluga na slobodnom tržištu uz
poštovanje principa ravnopravnosti privrednih subjekata



Државни Дата Центар

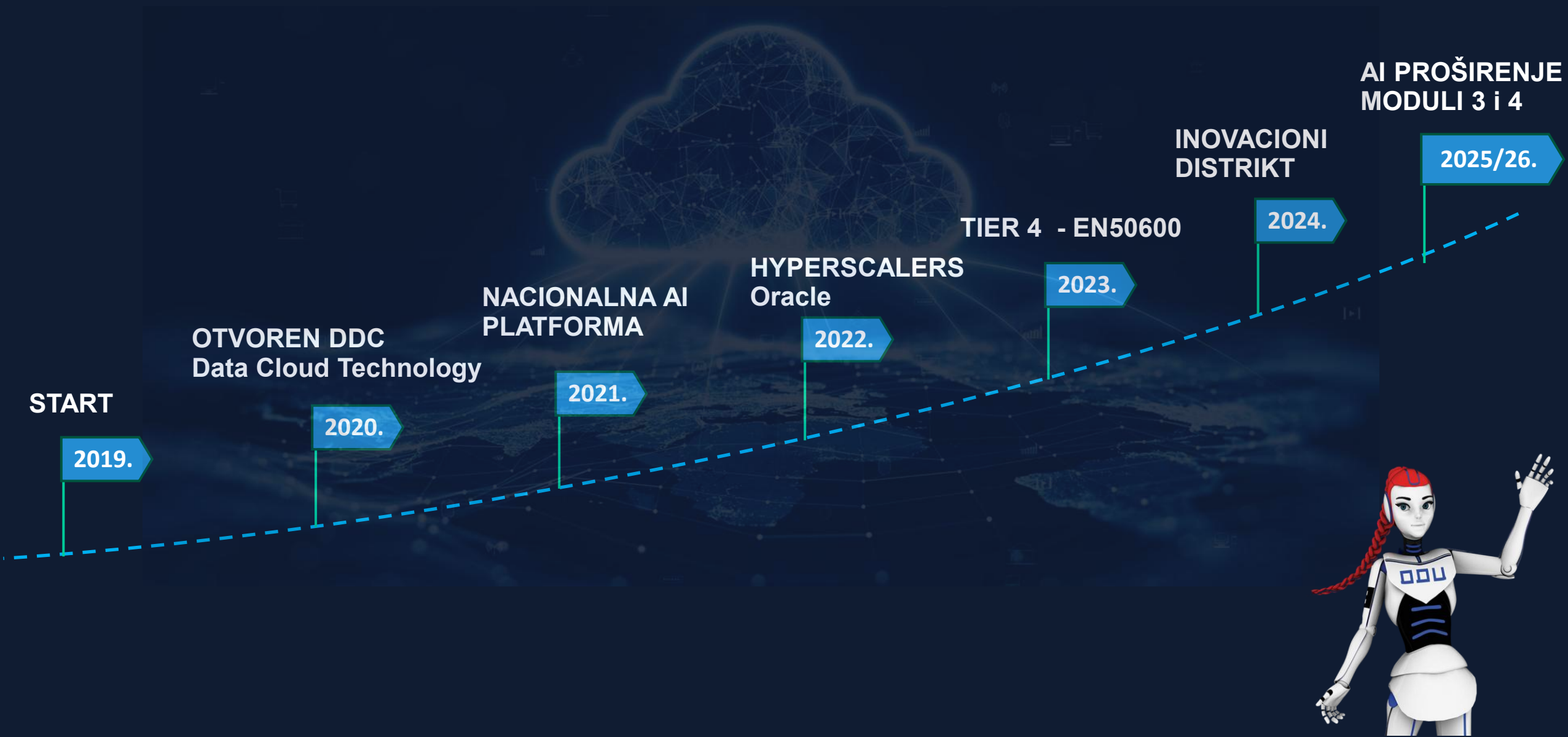


Republika Srbija
Kancelarija za informacione tehnologije
i elektronsku upravu

Državni organi

Državna uprava i institucije
Održavanje kompleksa i svih komponenti sistema 24/7/365

Timeline





KOLOKACIJA



CLOUD



**SAJBER
BEZBEDNOST**

INOVACIONI DISTRIKT



HTP
Крагујевац

SMART CITY

БИОИНФОРМАТИКА
&БИОМЕДИЦИНА

AI

СРЦЕ
ИД-а

ОБУКЕ

МЕСТО СУСРЕТА

COWORKING

ИТЕ &
еУПРАВА

КОМЕРЦИЈАЛНИ
КОРИСНИЦИ

ИНФОРМАЦИОНА
БЕЗБЕДНОСТ

ТРГ

ГЛАВНИ УЛАЗ

ДРЖАВНИ ДАТА
ЦЕНТАР

Надземно – 60 800 m²

A	23 900m ²	P+4
B	14 700m ²	P+1
C	22 200m ²	P+4

Подземно – 24 600 m²

A	9 800m ²	-
B	1 100m ²	-
C	13 700m ²	-

TOTAL – 85 400 m²

Šta ćemo obraditi danas



1 · Osnove i istorijat



3 · Metodologije i frejmvorci



5 · Standardi i zajednice



2 · Ključni koncepti i akteri



4 · Primena u odbrani



6 · Besplatni alati i resursi



01

SEKCIJA 01

Osnove i istorijat

Odakle CTI dolazi, kako ga definišemo i zašto je postao nezaobilazan deo sajber bezbednosti.



Šta uopšte znači „intelligence“?

Obaveštajni podatak (intelligence)

nije običan podatak — to je analizirana informacija koja odgovara na konkretno pitanje donosioca odluke i smanjuje neizvesnost.

Ključni test: „Šta tačno dobijamo ovim saznanjem?“

- Ako podatak ne menja nijednu odluku — nije intelligence
- Mora biti pravovremen, relevantan i upotrebljiv
- Kontekst je vredniji od sirovog indikatora



↑ svaki nivo dodaje kontekst i vrednost

Od sirovog podatka do akcije



Vrednost raste sleva nadesno: isti podatak, sve više konteksta i sve konkretnija odluka.

Kako definišemo Cyber Threat Intelligence



Gartner (klasična)

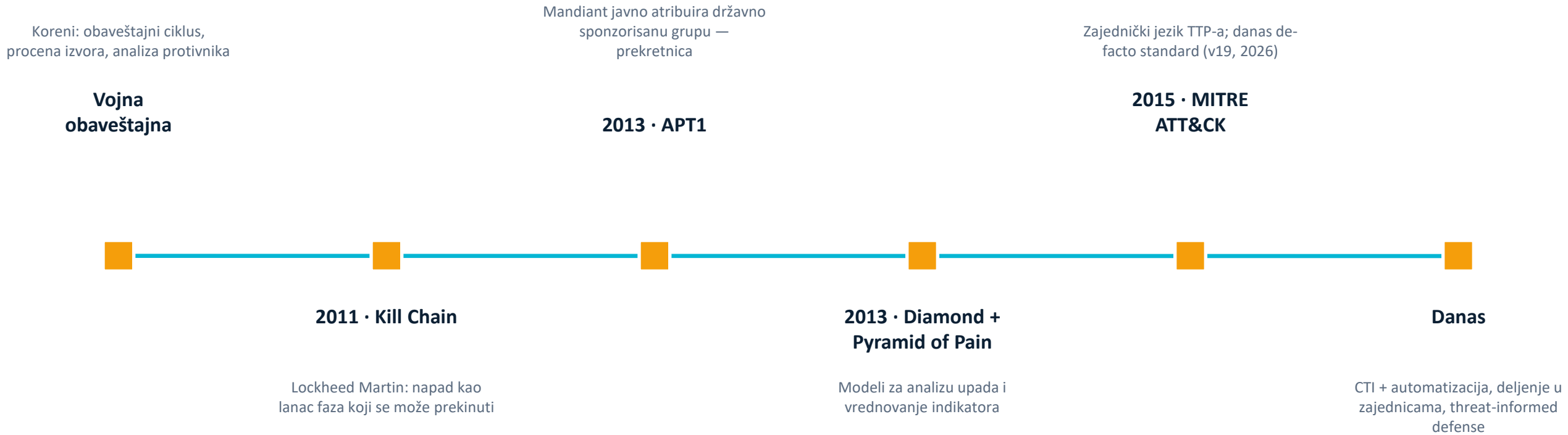
Znanje zasnovano na dokazima — uključujući kontekst, mehanizme, indikatore i akcione savete — o postojećoj ili nastajućoj pretnji, koje podržava odluke o odgovoru.



SANS (operativna)

Analizirane informacije o namerama, sposobnostima i prilikama protivnika, prikupljene i obrađene da bi branilac doneo bolju, bržu odluku.

Kratka evolucija discipline



Rani radovi APT izveštaja ...

Year	Report/event	Importance
2006	Symantec Japan reporting on APT1 infrastructure	Earliest known public reporting associated with APT1
2008	<i>An Evolving Crisis</i> / Byzantine Foothold	Early public use of the APT terminology
Jan 2010	Mandiant M-Trends 2010	Mandiant's first published APT details
2010	Operation Aurora reports	APT becomes widely known
2011	McAfee Shady RAT	Major large-scale APT campaign report
2013	Mandiant APT1	Landmark modern APT report
2013+	APT28, APT29, Turla, Lazarus etc.	Threat-actor-centric CTI becomes mainstream

Zašto organizacije ulažu u CTI



Prioritizacija

Fokus na pretnje koje su relevantne baš za vaš sektor i tehnologiju



Proaktivnost

Od reagovanja ka predviđanju: hunting i priprema pre incidenta



Deljenje

Kolektivna odbrana — ono što pogodi jednog, upozorava sve



Brzina odgovora

Poznat protivnik = brža detekcija i kraće vreme zadržavanja (dwell time)



Bolja ulaganja

Odluke o kontrolama i budžetu zasnovane na stvarnoj pretnji



Jezik za upravu

Rizik iskazan poslovno, razumljiv menadžmentu i regulatoru

Četiri nivoa CTI



Ko koristi CTI unutar organizacije



CISO / rukovodstvo

Strateške odluke, rizik, prioriteti ulaganja



Incident Response

Kontekst tokom istrage, atribucija, obim



Vulnerability mgmt

Prioritizacija zakrpa po eksploataciji u praksi



SOC / detekcija

Pravila, korelacija, obogaćivanje alarma



Threat Hunting

Hipoteze zasnovane na TTP protivnika



Anti-fraud / rizik

Prepoznavanje kampanja prevara i zloupotreba

Mitovi ...



„CTI = kupiti feed indikatora“



Feed je sirovina. Bez analize i konteksta to je samo lista koja brzo zastareva



„CTI je samo za velike SOC-ove“



I mali tim ima koristi — počinje se od besplatnih izvora i jasnih pitanja.



„Više indikatora = bolja odbrana“



Više šuma = više lažnih alarma. Cilj je relevantnost, ne količina.



„Atribucija je najvažnija“



Za odbranu su TTP i akcije važniji od imena grupe.



02

SEKCIJA 02

Ključni koncepti i akteri

Jezik struke: indikatori, ponašanje protivnika, procena i pravila deljenja.



IOC vs. IOA vs. TTP — tri pogleda na pretnju

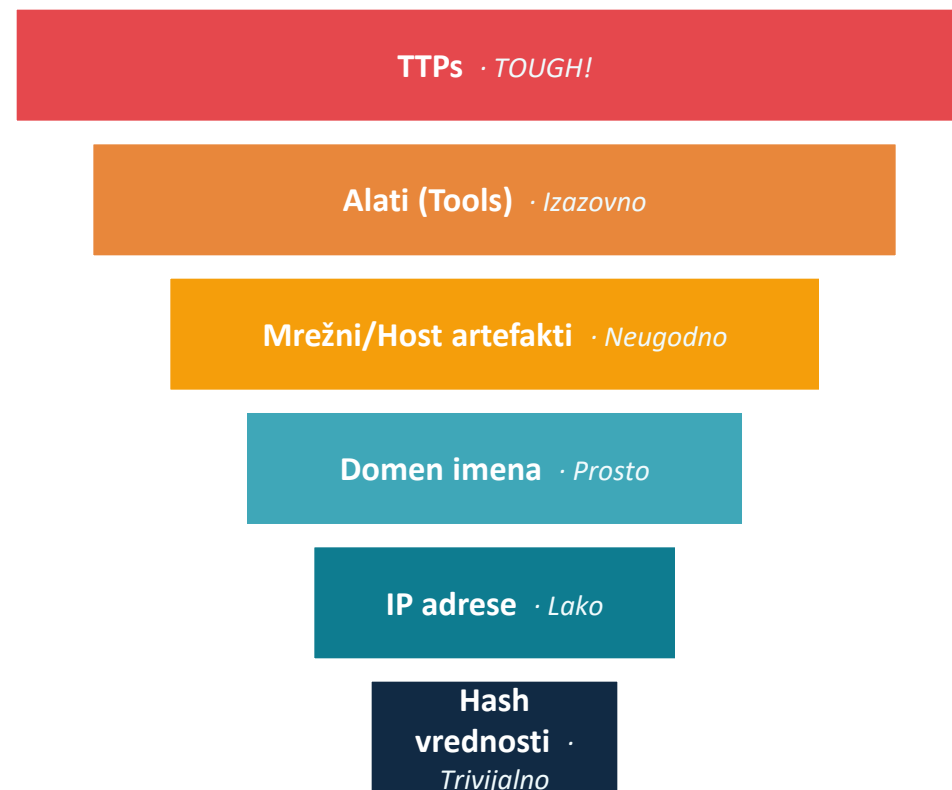
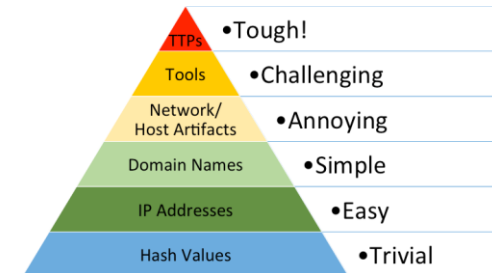
IOC	IOA	TTP
Indicator of Compromise	Indicator of Attack	Tactics, Techniques, Procedures
Artefakt koji dokazuje da se nešto dogodilo • Hash fajla • IP / domen C2 • Registry ključ • URL / mutex <i>Reaktivno · brzo zastareva</i>	Ponašanje koje ukazuje da se napad dešava • Neuobičajen proces • PowerShell + enkodiran payload • Lateral movement • Eskalacija privilegija <i>Proaktivnije · trajnije</i>	Kako protivnik radi — njegov „Modus operandi“ • Taktika: Persistence • Tehnika: Scheduled Task • Procedura: konkretan način • Vezano za ATT&CK <i>Najtrajnije · najteže za napadača</i>

Pyramid of Pain (David Bianco, 2013)

Što je indikator viši u piramidi, to je napadaču teže i skuplje da ga promeni — i vrednija je vaša detekcija.

- Hash, IP, domen: napadač ih menja trivijalno
- Mrežni/host artefakti: nešto teže
- Alati: menjanje traži trud i vreme
- TTP: menjanje znači promenu načina rada — najskuplje

→ Cilj zrelog CTI programa: detekcija na nivou TTP-a, ne samo IOC-a.



Ko su protivnici — tipologija pretećih aktera



Državno sponzorisani (APT)

Špijunaža, sabotaza; visoki resursi, strpljivi, prikriveni



Sajber-kriminal

Profit: ransomware, prevare, krađa podataka; profesionalizovani



Haktivisti

Ideologija; DDoS, defacement, curenje podataka



Insajderi

Zaposleni/partneri; namerno ili nenamerno; teški za detekciju



Script kiddies

Niska veština, gotovi alati; masovni, oportunistički napadi



Cyber-mercenari

Napad-kao-usluga; spyware i pristup na prodaju

Atribucija

Zašto je teška

- Napadači namerno ostavljaju lažne tragove (false flags)
- Alati i infrastruktura se dele i preprodaju
- Iste TTP koristi više grupa
- Politička težina — greška ima posledice

Za branioca: prvo TTP i akcije, pa tek onda ime grupe.

Nivoi pouzdanosti procene



Visoka pouzdanost



Umerena pouzdanost



Niska pouzdanost

Uvek iskazujte NIVO POUZDANOSTI uz tvrdnju. Analitičar koji ne greši — ne analizira dovoljno.

Admiralty skala: odvojite izvor od informacije

NATO/Admiralty sistem ocenjuje dve stvari nezavisno: koliko je pouzdan izvor i koliko je verodostojna sama informacija.

Pouzdanost izvora (A–F)

A	Potpuno pouzdan
B	Uglavnom pouzdan
C	Prilično pouzdan
D	Ne uvek pouzdan
E	Nepouzdan
F	Ne može se proceniti

Verodostojnost informacije (1–6)

1	Potvrđeno iz drugih izvora
2	Verovatno tačno
3	Moguće tačno
4	Sumnjivo
5	Malo verovatno
6	Ne može se proceniti

Primer: „B2“ = uglavnom pouzdan izvor, verovatno tačna informacija.

Traffic Light Protocol (TLP 2.0)

Standard koji održava FIRST — određuje kome smete da prosledite dobijenu informaciju. Poštovanje TLP-a gradi poverenje u zajednici.

TLP:RED

Samo za primaoca lično. Ne deliti dalje, ni unutar organizacije.

TLP:AMBER+STRICT

Deliti samo unutar organizacije primaoca.

TLP:AMBER

Organizacija primaoca i njeni klijenti — po principu potrebe.

TLP:GREEN

Cela zajednica / partneri, ali ne javno.

TLP:CLEAR

Bez ograničenja — može javno (uz zdravu logiku).



SEKCIJA 03

Metodologije i frejmvorci

Struktuiran način razmišljanja: obaveštajni ciklus i modeli koji nam daju zajednički jezik.



Obaveštajni ciklus



Planiranje i prikupljanje



1 · Planiranje i usmeravanje

.

- PIR – Priority Intelligence Requirements: šta nas tačno zanima
- Ko je publika i koju odluku donosi
- Definiši obim, rokove i format isporuke
- Loše pitanje → beskoristan izveštaj



2 · Prikupljanje

Izvori

- OSINT: blogovi, izveštaji, feedovi, društvene mreže
- Zajednice: MISP, ISAC, CERT/CSIRT razmena
- Interni: logovi, IR nalazi, telemetrija senzora
- Komercijalni feedovi (kada budžet dozvoli)

PIR



Šta je PIR?

Priority Intelligence Requirements — ključna pitanja na koja donosilac odluke mora da dobije odgovor. Ona USMERAVALJU ceo obaveštajni ciklus.

- Definišu ŠTA prikupljamo i analiziramo (a šta ignorišemo)
- Pretvaraju „zanimljivo“ u „relevantno“
- Vezuju CTI za poslovni rizik i konkretne odluke
- Bez PIR-a: skupljate šum i davite se u podacima

Osobine dobrog PIR-a



Konkretno

Usko, jednoznačno pitanje — ne „reci mi o pretnjama“



Vezano za odluku

Ima vlasnika i odluku koju podupire



Odgovorljivo

Može se odgovoriti iz dostupnih izvora

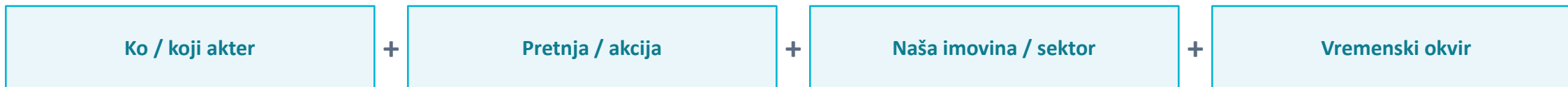


Prioritizovano i sa rokom

Rangirano po važnosti, vremenski ograničeno

Loše pitanje → beskorisan izveštaj. Dobar PIR → upotrebljiv intel koji utiče na odluku.

Kako napisati dobar PIR



Formula za oštar, akcionabilan PIR



Loše — previše široko

- „Reci mi sve o ransomware-u.“
- „Da li smo bezbedni?“
- → Nemoguće odgovoriti, ne vodi ka odluci



Dobro — konkretno i akciono

- „Koje ransomware grupe ciljaju banke u regionu i koje početne vektore koriste (naredna 2 kvartala)?“
- „Da li se CVE-2025-XXXX aktivno iskorišćava protiv naše tehnologije od aktera koji nas cilja?“



PIR · prioritetno pitanje



SIR · specifičniji zahtevi



EI / indikatori · šta tačno tražimo u podacima

Priority Intelligence Requirement
Da li postoji povećan rizik od APT napada na našu organizaciju?

Essential Elements of Information

PIR/SIR/EEI

PIR	Priority Intelligence Requirement	SIR – konkretna pitanja	EEI – šta prikupljamo
PIR-01	Koje APT grupe predstavljaju najveću pretnju našoj organizaciji?	Koje grupe ciljaju naš sektor? Koje zemlje/region?	Actor, country, sector, campaigns, motivation
PIR-02	Da li smo trenutno meta aktivne kampanje?	Da li postoji kampanja koja cilja naše sektore/tehnologije?	Campaign, victimology, dates, targeting
PIR-03	Koje TTP koriste relevantni threat actors?	Koje ATT&CK tehnike koriste?	MITRE technique/sub-technique, procedures
PIR-04	Koje ranjivosti trenutno predstavljaju najveći rizik?	Koje CVE aktivno eksploatišu naši relevantni threat actors?	CVE, CVSS, KEV, exploit availability
PIR-05	Da li su naše tehnologije direktno targetirane?	Da li napadači ciljaju M365, VPN, firewall, VMware, AWS itd.?	Product, version, exploit, campaign
PIR-06	Koja maliciozna infrastruktura je povezana sa relevantnim napadačima?	Koji C2/server/domain infrastruktura se koristi?	IP, domain, URL, ASN, certificate
PIR-07	Da li postoje indikatori kompromitacije naših sistema?	Da li se IOC pojavljuje u našoj telemetriji?	Hash, IP, domain, email, endpoint evidence
PIR-08	Koje phishing kampanje predstavljaju rizik za zaposlene?	Koji brand/department/personnel su targetirani?	Sender, domain, URL, attachment, lure
PIR-09	Da li postoji rizik od ransomware napada?	Koje grupe ciljaju naš sektor? Kako dobijaju initial access?	Actor, access broker, TTP, ransomware
PIR-10	Da li threat actors targetiraju naše dobavljače/partnere?	Koji third parties su kompromitovani?	Supplier, campaign, compromise evidence
PIR-11	Da li postoji rizik od supply-chain napada?	Koji proizvođači/platforme imaju aktivne kampanje?	Vendor, product, CVE, campaign

Obrada i analiza



3 · Obrada

- Normalizacija formata i deduplikacija
- Prevod, dekodiranje, ekstrakcija indikatora
- Obogaćivanje (enrichment): geo, WHOIS, reputacija
- Mapiranje na ATT&CK i taksonomije



4 · Analiza i produkcija

- Strukturne tehnike: ACH (analiza konkurentskih hipoteza)
- Izbegavaj pristrasnost potvrđivanja (confirmation bias)
- Zaključci + procena pouzdanosti

Diseminacija i povratna informacija



5 · Diseminacija

Pravi format za pravu publiku:

- Menadžment → kratak brief, poslovni rizik
- SOC → pravila, IOC, ATT&CK mapiranja (mašinski)
- IR/hunt → detaljni tehnički izveštaj
- Kanali: TIP, e-pošta, ticketing, dashboards



6 · Povratna informacija

Zatvaranje petlje — najčešće preskočeno:

- Da li je izveštaj promenio ijednu odluku?
- Šta je nedostajalo, šta je bilo suvišno?
- Ažuriraj PIR i izvore za sledeći ciklus
- Ciklus je petlja, ne prava linija

Cyber Kill Chain (Lockheed Martin, 2011)



Napad kao lanac od 7 faza. Prekid u BILO kojoj karici zaustavlja ceo napad — zato tražimo najraniju tačku detekcije.



← ranije = jeftinije za odbranu

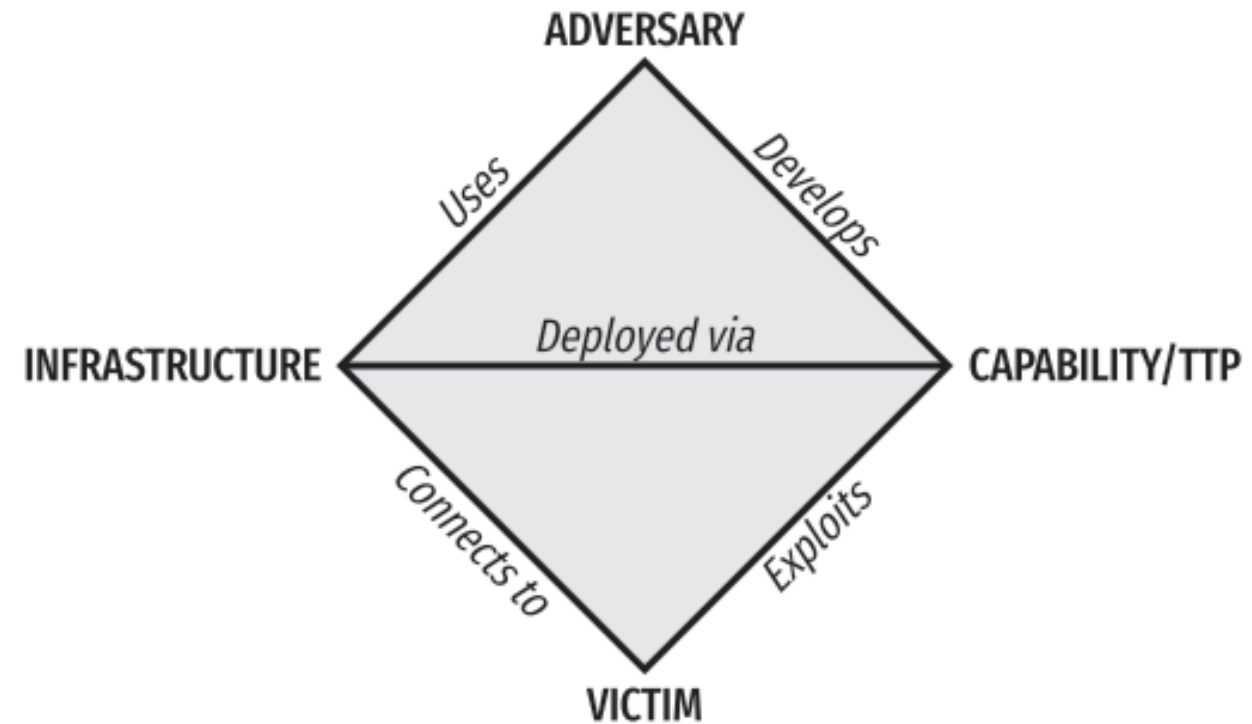
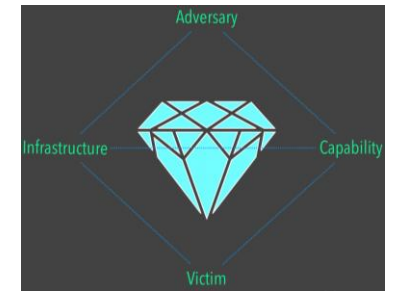
kasnije = skuplje i opasnije →

Diamond Model (2013)

Svaki proboj sistema ima 4 povezana vrha. Ako znate dva, često možete zaključiti ostale što ubrzava istragu.

- Adversary (protivnik): ko stoji iza napada
- Capability (sposobnost): malver, alati, eksploati
- Infrastructure: C2 serveri, domeni, mreža
- Victim (žrtva): meta i njena imovina

Meta-osobine: pravac, metodologija, resursi, vremenski okvir.



MITRE ATT&CK — zajednički jezik za TTP

Šta je ATT&CK?

- Baza znanja o realnom ponašanju protivnika
- Organizovana u Taktike (zašto) i Tehnike (kako)
- Besplatna, otvorena, globalno prihvaćena
- Domeni: Enterprise, Mobile, ICS
- Povezuje grupe, softver i kampanje sa tehnikama

v19

aktuelna verzija (apr. 2026)

15

taktika (Enterprise)

222

tehnika

475

podtehnika

Zašto je bitan za CTI

Daje zajednički rečnik: kad kažemo „T1566 Phishing“, svi u svetu znaju tačno o čemu govorimo — deljenje postaje precizno.

ATT&CK matica

Reconnaissance 12 techniques	Resource Development 9 techniques	Initial Access 11 techniques	Execution 20 techniques	Persistence 22 techniques	Privilege Escalation 13 techniques	Stealth 30 techniques	Defense Impairment 18 techniques	Credential Access 17 techniques	Discovery 34 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	BITS Jobs	Account Manipulation (0/7)	Abuse Elevation Control Mechanism (0/6)	Access Token Manipulation (0/5)	Disable or Modify System Firewall (0/3)	Adversary-in-the-Middle (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/4)	Application Layer Protocol (0/5)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	Cloud Administration Command	BITS Jobs		BITS Jobs		Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (0/1)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Command and Scripting Interpreter (0/13)	Boot or Logon Autostart Execution (0/14)	Access Token Manipulation (0/5)	Build Image on Host	Disable or Modify Tools (0/6)	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/8)	External Remote Services	Container Administration Command	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/7)	Debugger Evasion	Domain or Tenant Policy Modification (0/2)	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (0/2)		Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Deploy Container	Cloud Application Integration	Boot or Logon Autostart Execution (0/14)	Deobfuscate/Decode Files or Information	Downgrade Attack	Forced Authentication	Cloud Service Dashboard	Remote Services (0/8)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Defacement (0/2)
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	ESXi Administration Command	Compromise Host Software Binary	Boot or Logon Initialization Scripts (0/5)	Direct Volume Access	Exploitation for Defense Impairment	Forge Web Credentials (0/2)	Cloud Storage Object Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Disk Wipe (0/2)
Query Public AI Services	Generate Content (0/2)	Replication Through Removable Media	Exploitation for Client Execution	Create Account (0/3)	Create or Modify System Process (0/5)	Execution Guardrails (0/2)	File and Directory Permissions Modification (0/2)	Input Capture (0/4)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (0/2)		Email Bombing
Search Closed Sources (0/2)	Obtain Capabilities (0/7)	Supply Chain Compromise	Hijack Execution Flow (0/12)	Create or Modify System Process (0/5)	Domain or Tenant Policy Modification (0/2)	Hide Artifacts (0/14)	Modify Authentication Process (0/9)	Modify Authentication Process (0/9)	Debugger Evasion	Taint Shared Content	Data from Configuration Repository (0/2)	Fallback Channels	Exfiltration Over Physical Medium (0/1)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Stage Capabilities (0/6)	Trusted Relationship	Input Injection	Event Triggered Execution (0/18)	Escape to Host	Hijack Execution Flow (0/12)	Modify Cloud Compute Infrastructure (0/5)	Multi-Factor Authentication Interception	Device Driver Discovery	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/6)	Hide Infrastructure	Exfiltration Over Web Service (0/4)	Financial Theft
Search Open Websites/Domains (0/3)		Valid Accounts (0/4)	Inter-Process Communication (0/3)		Exclusive Control	Indicator Removal (0/8)	Modify Cloud Resource Hierarchy	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Threat Vendor Data		Wi-Fi Networks	Native API		External Remote Services	Masquerading (0/12)	Modify Registry	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Poisoned Pipeline Execution		Implant Internal Image	Obfuscated Files or Information (0/18)	Modify System Image (0/2)	OS Credential Dumping (0/8)	Group Policy Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (0/2)
			Scheduled Task/Job (0/5)		Modify Authentication Process (0/9)	Pre-OS Boot (0/5)	Network Boundary Bridging (0/1)	Steal Application Access Token	Local Storage Discovery		Data Staged (0/2)	Non-Standard Port		Resource Hijacking (0/4)
			Serverless Execution		Modify Registry	Process Injection (0/12)	Process Injection (0/12)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (0/3)	Protocol Tunneling		Service Stop
			Shared Modules		Office Application	Reflective Code Loading	Plist File		Network Service Discovery		Input Capture (0/4)	Proxy (0/4)		System Shutdown/Reboot
			Software Deployment Tools			Rootkit			Network Sniffing			Remote Access Tools (0/3)		
						Selective Exclusion			Password Policy Discovery			Traffic Signaling (0/2)		
						Social Engineering (0/2)			Peripheral Device					
						System Binary Proxy								

ATT&CK matrica i šta je novo u v19

Recon	Resource Dev	Initial Access	Execution	Persistence	Priv. Esc	Stealth*	Def. Impair*	Cred. Access	Discovery	Lateral Mov	Collection	C2	Exfil	Impact

Kolone = taktike · ćelije = tehnike



Novo u v19 (28. april 2026): taktika „Defense Evasion“ je podeljena na **Stealth (TA0005)** (prikriivanje) i **Defense Impairment (TA0112)** (aktivno onesposobljavanje odbrane). Postojeća pravila i mape pokrivenosti treba re-mapirati.

Frejmvorci nisu konkurenti nego slojevi odbrane

Najbolji rezultati dolaze iz kombinacije: Kill Chain daje redosled, ATT&CK detalje ponašanja, Diamond kontekst upada!



Kill Chain

„KADA“ — u kojoj fazi napada se nalazimo

Strateški pregled toka napada



MITRE ATT&CK

„KAKO“ — konkretne tehnike i procedure

Detekcija i mapiranje pokrivenosti



Diamond Model

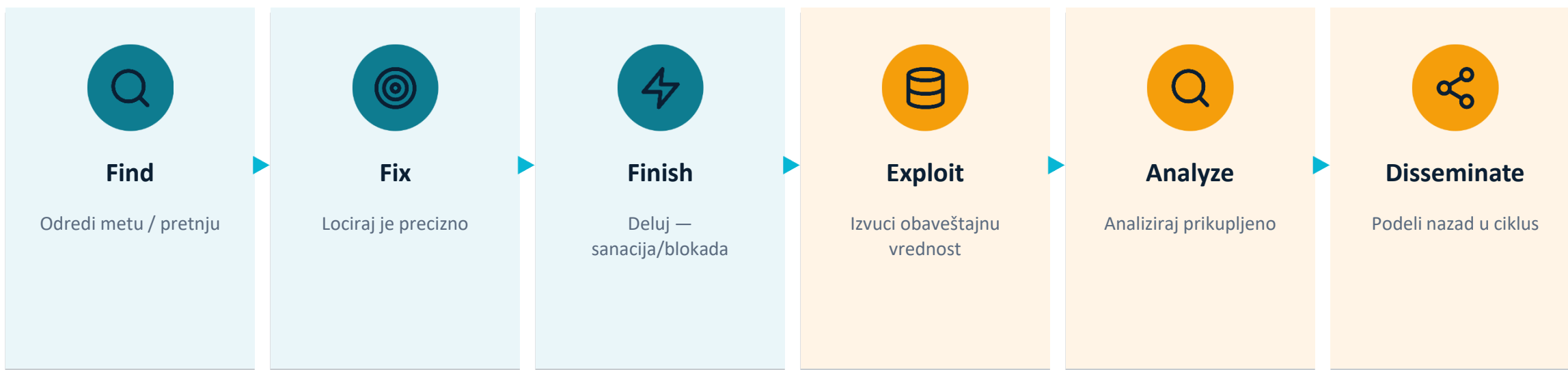
„KO/ŠTA“ — protivnik, alat, infra, žrtva

Analiza i pivotiranje istrage

Threat-informed defense = spajanje sva tri u jedan pogled na protivnika.

F3EAD

Vojno-poreklo, danas spaja obaveštajni rad sa akcijom. Idealan za saradnju CTI tima i IR/hunt tima.



F³ (Find–Fix–Finish) = operacije · **EAD (Exploit–Analyze–Disseminate) = obaveštajni rad**



SEKCIJA 04

Primena CTI u odbrani

Gde obaveštajni rad zaista dodiruje ICT sistem: detekcija, lov, odgovor, prioriteti i merenje.



CTI - od indikatora do pravila

- IOC → blok liste, watchliste, SIEM korelacija
- TTP → detekcija ponašanja (izdržljivija)
- Sigma pravila: prenosiva između SIEM-ova
- YARA: prepoznavanje malvera po sadržaju
- Mapiraj svako pravilo na ATT&CK tehniku

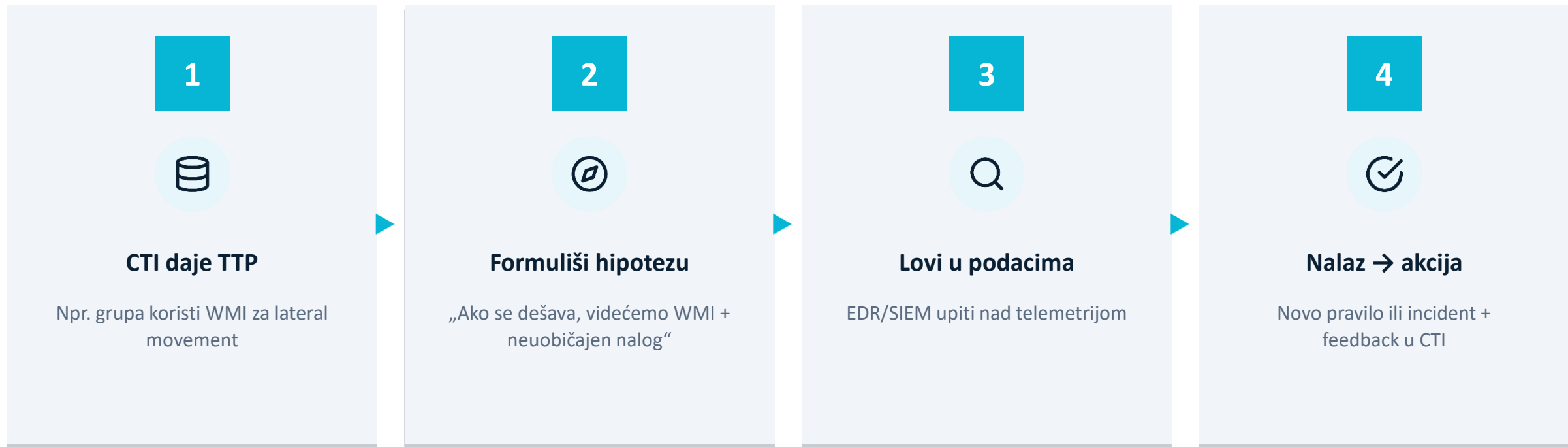
Primer: Sigma → SIEM

```
title: Suspicious PowerShell EncodedCommand
detection:
  selection:
    Image|endswith: '\powershell.exe'
    CommandLine|contains: '-enc'
  condition: selection
tags: attack.execution, attack.t1059.001
```

Jedno pravilo → mnogo platformi → mapirano na ATT&CK.

Threat Hunting vođen hipotezama

Ne čekamo alarm već polazimo od pretpostavke o protivnikovom ponašanju i tražimo dokaze u telemetriji.



Uspeh lova nije uvek nalaz i „ništa nije nađeno“ je vredna informacija o pokrivenosti.

CTI tokom odgovora na incident



Prepoznavanje

Poklapanje IOC/TTP → o kojoj kampanji ili grupi je reč



Predviđanje

Poznat protivnik → očekivani sledeći koraci i ciljevi



Obim (scoping)

Povezani indikatori otkrivaju širinu kompromitacije



Sanacija

TTP protivnika usmerava eradikaciju i ojačavanje



Nova saznanja

IR proizvodi svež CTI — vraća se u ciklus i deljenje

CTI i IR su dvosmerna ulica: intel ubrzava odgovor, a odgovor obogaćuje intel.

Prioritizacija ranjivosti: CVSS nije dovoljan

Hiljade CVE-a, ograničeno vreme. CTI odgovara na pravo pitanje: koja ranjivost se ZAISTA iskorišćava?



CVSS

Koliko je ranjivost ozbiljna u teoriji

Osnova, ali svi je imaju visoku



EPSS

Verovatnoća eksploatacije
(podaci)

Dodaje realnu procenu rizika



CISA KEV

Lista poznato-iskorišćavanih
ranjivosti

Ako je ovde — krpi ODMAH



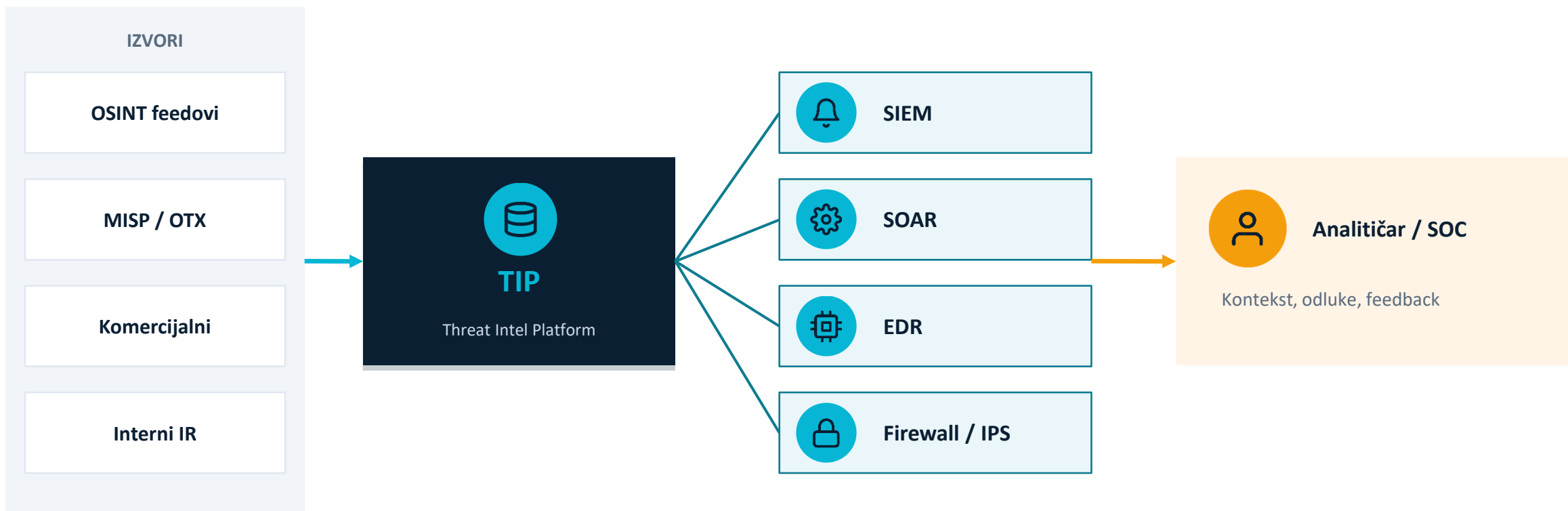
CTI kontekst

Da li baš vaš protivnik ovo koristi

Najprecizniji prioritet

Kombinuj sve → krpi ono što je opasno, verovatno i relevantno — ne sve odjednom.

CTI u sajber odbrambenim operacijama



TIP je centralno čvorište: normalizuje, obogaćuje i distribuira intel automatski — analitičar dodaje presudu.

CTI kao jezik za menadžment

Šta menadžment želi da čuje

- Ko nas realno cilja i zašto (sektorski kontekst)
- Koji poslovni procesi su najizloženiji
- Kako se rizik menja kroz vreme (trend)
- Da li ulaganja u kontrole daju rezultat

Rizik, verovatnoća, uticaj u novcu i posledicama.

Threat-informed odluke



Prioriteti ulaganja — gde uložiti sledeći dinar



Regulatorni izveštaji — NIS2, DORA, sektorski zahtevi



Tabele rizika (risk board) — pretnja + verovatnoća + uticaj



Scenariji i vežbe — table-top na osnovu realnih pretnji

Kako meriti vrednost CTI !?

↓ Dwell time

Kraće vreme zadržavanja napadača u mreži

↑ Relevantnost

Udeo intela koji vodi do konkretne akcije

↓ Lažni alarmi

Bolji kontekst = manje šuma za SOC

↑ Pokrivenost

Koliko ATT&CK tehnika detektujemo

Oprez sa metrikama

- Broj indikatora NIJE mera uspeha (vanity metric)
- Meri ishod (akcije, sprečeni incidenti), ne aktivnost
- Poveži svaki izveštaj sa donetom odlukom

Praktični KPI-jevi

- Vreme od saznanja do detekcionog pravila
- % alarma obogaćenih CTI kontekstom
- Broj hunt-ova pokrenutih iz intela
- Zadovoljstvo „korisnika usluga“ intela (feedback)



SEKCIJA 05

Standardi razmene i zajednice



STIX i TAXII — zajednički jezik i transport

STIX 2.1

„ŠTA“ opisujemo (OASIS standard)

- Struktuiran model za pretnje (JSON)
- Objekti: Indicator, Malware, Threat Actor...
- Relacije: „koristi“, „cilja“, „pripisano“
- Mašinski čitljivo — automatizacija bez ambigviteta

Zamislite graf: čvorovi = objekti, ivice = relacije.

TAXII 2.1

„KAKO“ razmenjujemo (transport)

- Protokol za razmenu STIX podataka (HTTPS/REST)
- Collections: povuci/objavi indikatore
- Channels: pretplata na izvore
- MISP, OpenCTI i drugi ga podržavaju

STIX = rečnik i gramatika · TAXII = pošta koja ih prenosi.

Kolektivna odbrana: *Sharing is caring*



CERT / CSIRT

Timovi za reagovanje — nacionalni, sektorski, organizacioni.
Koordinacija i rana upozorenja.



ISAC / ISAO

Sektorske zajednice za razmenu (finansije, energetika, zdravstvo).
Poverenje + specifičan kontekst.



FIRST

Globalni krovni forum CSIRT timova — standardi, saradnja, poverenje
preko granica.



Otvorene zajednice

MISP zajednice, abuse.ch, OTX „pulses“ — svako doprinosi i koristi.



FIRST — Forum of Incident Response & Security Teams

Šta je FIRST

- Globalni forum koji povezuje CSIRT/PSIRT timove
- Osnovan 1990. — jedna od najstarijih zajednica
- Gradi poverenje i saradnju preko granica
- Standardi, konferencije, obuke, radne grupe

Održava ključne standarde

TLP (Traffic Light Protocol) · CVSS (ocenjivanje ranjivosti)

1990

godina osnivanja

700+

članica (timova)

~100

zemalja

TLP + CVSS

standardi koje održava

first.org

Od globalnog ka lokalnom: nacionalni i sektorski timovi



Nacionalni CERT

- Koordinacija na nivou države, rana upozorenja
- Veza sa regulatorima i kritičnom infrastrukturuom
- Tačka kontakta prema međunarodnim partnerima
- Okvir za obavezno prijavljivanje incidenata



Finansijski sektor (FIN-CSIRT)

- Sektorska razmena prilagođena pretnjama nad bankama
- Zajednički IOC/TTP relevantni za region
- Poverenje među članicama — brža reakcija
- Usklađenost sa DORA / NIS2 zahtevima



06

SEKCIJA 06

Besplatni alati i resursi

Kompletan open-source ekosistem . . .



MISP — platforma za razmenu pretnji



MISP

Malware Information Sharing Platform (poreklo: CIRCL, Luksemburg)

- Najrasprostranjenija open-source TIP platforma
- Deljenje u „sharing groups“ sa kontrolom pristupa
- Automatska korelacija događaja i indikatora
- Taksonomije i galaksije (ATT&CK, grupe)
- Kvalitetni feedovi „iz kutije“ (uklj. abuse.ch)

Idealno za

- Zajedničku razmenu unutar sektora / ISAC-a
- Centralno skladište IOC-a za SOC
- Izvoz u SIEM/IDS (STIX, CSV, Suricata)

2.5.x

aktuelna verzija

STIX

izvoz/uvoz

100%

open-source

BESPLATNO / OPEN-SOURCE

misp-project.org

OpenCTI — moderni threat intelligence hub



OpenCTI

Filigran (osnovan 2022) · deo XTM ekosistema

- Model podataka zasnovan na STIX 2.1
- 300+ konektora „na jedan klik“ (feedovi, alati)
- Vizuelizacija veza: grafovi, timelines, ATT&CK
- Inference engine — automatski zaključuje relacije
- Community Edition besplatna (Apache 2.0)

Idealno za

- Modelovanje i analizu, ne samo listu IOC-a
- Produkciju strateških/operativnih izveštaja
- Vezivanje detekcije, huntinga i IR-a u celinu

STIX 2.1

model

300+

konektora

CE

besplatno

BESPLATNO / OPEN-SOURCE

filigran.io

AlienVault OTX — otvorena razmena pretnji



OTX (LevelBlue)

Open Threat Exchange · danas pod brendom LevelBlue (ex AT&T)

- Crowd-sourced: zajednica deli „pulses“ (kampanje)
- Osnovan 2012 — jedan od najvećih besplatnih izvora
- „Pulse“ = skup IOC-a sa kontekstom i tagovima
- DirectConnect API za automatsku integraciju
- Odličan ulaz u svet CTI za početnike

Idealno za

- Brzo obogaćivanje indikatora kontekstom
- Praćenje pretnji po temi / regionu / malveru
- Besplatan feed za manje timove

180k+

učesnika

140

zemalja

API

integracija

BESPLATNO / OPEN-SOURCE

otx.alienvault.com

abuse.ch × Spamhaus — visoko-kvalitetni besplatni feedovi



URLhaus

Zlonamerni URL-ovi koji distribuiraju malver



ThreatFox

IOC-i vezani za malver — 1.8M+ podeljeno



YARAify

Skeniranje i deljenje YARA pravila



MalwareBazaar

Baza uzoraka malvera i heševa (po familijama)



Feodo Tracker

Praćenje botnet C2 servera (banking trojani)

Zašto su odlični: nizak šum, visoka pouzdanost, laka integracija u MISP i SIEM. Idealna polazna tačka.

Alati za istragu i obogaćivanje indikatora



VirusTotal

Reputacija fajlova, URL-ova, domena; više skenera odjednom



Shodan

Pretraga izloženih uređaja i servisa na internetu



GreyNoise

Filtrira „internet šum“



urlscan.io

Bezbedno „snima“ i analizira sumnjive veb stranice



OpenPhish / PhishTank

Feedovi aktivnih phishing URL-ova



Maltego CE

Vizuelno povezivanje entiteta u istrazi (grafovi)

Napomena: OSINT alati imaju besplatne nivoe uz limite; poštuju uslove korišćenja i privatnost.

Još korisnih open-source alata



TheHive + Cortex

Case management za IR + automatska analiza



Sigma

Generički jezik detekcionih pravila



Suricata / Snort

Mrežna detekcija upada (IDS/IPS) sa pravilima



Yeti

Skladištenje i organizacija znanja o pretnjama



YARA

Pravila za prepoznavanje malvera



MITRE ATT&CK Navigator

Vizuelizacija i planiranje pokrivenosti tehnika

Besplatni resursi za učenje CTI



MITRE ATT&CK obuke

Zvanični besplatni kursevi (CTI, ATT&CK fundamentals)



SANS posteri i webinarari

„Cheat sheet“ posteri, snimci predavanja, blogovi



TryHackMe / praksa

Interaktivne CTI staze i hands-on laboratorije



Izveštaji vendara

APT izveštaji (npr. Mandiant, CrowdStrike) — čitajte kritički



Blogovi i newsletteri

abuse.ch, Filigran, CERT/CSIRT objave, istraživači



Zajednice i konferencije

FIRST, lokalni meetup-ovi, radne grupe

Savet: čitajte tuđe izveštaje aktivno — mapirajte ih na ATT&CK dok čitate. Tako se najbrže uči.

Kako izgraditi CTI kapacitete

1

Definiši PIR

Šta tačno treba da znaš? Kreni od pitanja, ne od alata

2

Startuj besplatno

abuse.ch + OTX + MISP;
jedan pouzdan feed je
bolji od deset šumnih

3

Postavi TIP

MISP ili OpenCTI kao
centralno mesto;
integriši u SIEM

4

Mapiraj na ATT&CK

Poveži intel sa
detekcijom; prati
pokrivenost tehnika

5

Uđi u zajednicu

Sektorski CSIRT/ISAC —
počni da primaš, pa da
deliš

6

Meri i iteriraj

Feedback petlja: da li
intel menja odluke?
Podesi PIR

Ne morate sve odjednom. Zrelost CTI-a raste postepeno — počnite malo, ali počnite.

Hvala na pažnji



DarkoS · CISO @ DCT