SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

SEMINARSKI RAD N/a

USPOREDBA ALATA ZA NADZOR I INTERVENCIJU NA KRAJNJIM TOČKAMA (ENDPOINT DETECTION AND RESPONSE)

Ante Čavar

Voditelj: prof.dr.sc. Stjepan Groš

Zagreb, lipanj, 2025.

Zahvaljujem se prijateljima i obitelji koji su mi bili podrška prilikom pisanja ovog rada.

Sadržaj

1. Uvod

U današnjem digitalnom okruženju, sigurnost informacijskih sustava postala je jedan od ključnih izazova za organizacije svih veličina. S povećanjem složenosti cyber napada i njihove učestalosti, tradicionalni pristup sigurnosti koji se oslanja na perimetarsku zaštitu više nije dovoljan. Organizacije moraju usvojiti proaktivne i sveobuhvatne sigurnosne strategije koje omogućavaju brzu detekciju, analizu i odgovor na sigurnosne prijetnje.

Potreba za naprednim sigurnosnim rješenjima

Moderna sigurnosna prijetnja krajolika karakterizira nekoliko ključnih trendova:

- **Sofisticiranost napada** - Napredni perzistentni prijetnje (APT) koriste složene tehnike za izbjegavanje tradicionalnih sigurnosnih mjera
- **Brzina širenja** - Malware i ransomware mogu se proširiti kroz mrežu u minutama
- **Heterogenost IT okruženja** - Organizacije koriste hibridne oblak-lokalne infrastrukture koje otežavaju sigurnosno nadziranje
- **Nedostatak sigurnosnih stručnjaka** - Globalni nedostatak kvalificiranog osoblja otežava pravilno upravljanje sigurnošću

Evolucija sigurnosnih tehnologija

Kao odgovor na ove izazove, razvile su se napredne sigurnosne tehnologije koje omogućavaju:

- Kontinuirano nadziranje sigurnosnih događaja
- Automatiziranu detekciju anomalija i prijetnji
- Brz i koordiniran odgovor na incidente
- Korelaciju podataka iz različitih izvora
- Proaktivno ‘lov na prijetnje’ (threat hunting)

Tri ključne kategorije ovih tehnologija su:

- **EDR (Endpoint Detection and Response)** - fokus na krajnje točke
- **NDR (Network Detection and Response)** - fokus na mrežni promet
- **XDR (Extended Detection and Response)** - integrirani pristup

Cilj seminara

Ovaj seminar istražuje navedene tehnologije kroz detaljnu analizu njihovih karakteristika, mogućnosti i ograničenja. Posebnu pozornost posvećujemo usporedbi vodećih komercijalnih i open-source rješenja, kao i preporukama za različite veličine organizacija. Cilj je pružiti sveobuhvatan pregled koji će omogućiti informirane odluke o odabiru najprikladnijih sigurnosnih rješenja.

2. EDR (Endpoint Detection and Response)

Definicija i osnove

EDR (Endpoint Detection and Response) je sigurnosna tehnologija koja kontinuirano nadzire krajnje točke - laptope, desktop računala, mobilne uređaje i ostalu računalnu opremu koja se može povezati na unutrašnji sustav organizacije. EDR rješenja predstavljaju evoluciju tradicionalnih antivirus programa, pružajući daleko naprednije mogućnosti za detekciju, analizu i odgovor na sigurnosne prijetnje.

Ključne karakteristike EDR rješenja

Kontinuirani nadzor EDR sustavi rade 24/7, neprestano analizirajući aktivnosti na krajnjim točkama:

- Nadzor procesa i aplikacija
- Praćenje mrežnih veza
- Analiza datotečnih operacija
- Monitoring registra sustava (Windows)
- Praćenje korisničkih aktivnosti

Usmjerenost na krajnje točke EDR rješenja tretiraju svaki uređaj kao potencijalni vektor napada, što im omogućava:

- Detaljnu analizu ponašanja na svakom uređaju
- Izolaciju kompromitiranih uređaja
- Forenzičku analizu sigurnosnih incidenata
- Rollback funkcionalnosti za oporavak od napada

Walled Garden pristup EDR rješenja rade po principu "walled garden" - fokusiraju se isključivo na krajnje točke unutar organizacije, što im omogućava duboku integraciju i detaljnu analizu, ali ograničava vidljivost na mrežne aktivnosti između uređaja.

Prednosti EDR rješenja

- **Visoka granularnost detekcije** - Mogućnost analize na razini procesa i datoteka
- **Rad od doma** - Posebno korisno za zaštitu udaljenih radnika
- **Forenzička analiza** - Detaljni logovi omogućavaju rekonstrukciju napada
- **Brz odgovor** - Mogućnost trenutne izolacije kompromitiranih uređaja
- **Vidljivost administratora** - Centralizada administracija svih krajnjih točaka

Ograničenja EDR rješenja

- **Ograničena mrežna vidljivost** - Ne pružaju uvid u mrežni promet između uređaja
- **Ovisnost o agentima** - Zahtijevaju instalaciju softvera na svakom uređaju
- **Ograničenost na uređaje** - Ne mogu detektirati napade koji zaobilaze krajnje točke
- **Potrošnja resursa** - Kontinuirani nadzor može utjecati na performanse uređaja

Proizvod	Ključne karakteristike
CrowdStrike Falcon	Nativna cloud arhitektura, AI/ML analiza, lagani agent
Microsoft Defender for Endpoint	Integracija s Microsoft ekosustavom, ugrađen u Windows
SentinelOne	Autonomni AI agent, offline mogućnosti, rollback funkcionalnost
Carbon Black (VMware)	Fokus na forenziku, napredna analiza ponašanja
Cybereason	Vizualizacija napada, proaktivno "lov na prijetnje"

Tablica 2.1. Vodeći EDR proizvodi i njihove karakteristike

Implementacijske preporuke

Pri implementaciji EDR rješenja, organizacije trebaju razmotriti:

1. **Pokrivenost uređaja** - Svi kritični uređaji moraju biti uključeni
2. **Mrežna povezanost** - Osigurati pouzdanu vezu s centralnim sustavom
3. **Obuka osoblja** - Sigurnosni tim mora razumjeti alate i procedure
4. **Integracija** - Povezivanje s postojećim SIEM i SOAR sustavima

5. **Testiranje** - Redovito testiranje detection i response procedura

3. NDR (Network Detection and Response)

Definicija i osnove

NDR (Network Detection and Response) je sigurnosna tehnologija slična EDR sustavu, ali se fokusira na analizu mrežnog prometa umjesto na krajnje točke. NDR rješenja kontinuirano nadziru i analiziraju mrežne komunikacije kako bi identificirali sumnjive aktivnosti, anomalije i sigurnosne prijetnje koje se mogu proširiti kroz mrežu.

Ključne karakteristike NDR rješenja

Mrežno usmjerenje NDR sustavi analiziraju mrežni promet na različitim razinama:

- Praćenje prometa na vatrozidima, ruterima i switchevima
- Analiza east-west prometa (između internal sustava)
- Nadzor north-south prometa (prema vanjskim mrežama)
- Deep packet inspection (DPI) za detaljnu analizu sadržaja

Analitičke tehnologije NDR rješenja koriste napredne analitičke metode:

- **Strojno učenje** - Za detekciju anomalija u mrežnom prometu
- **Analiza ponašanja** - Prepoznavanje neobičnih komunikacijskih obrazaca
- **Signature/Fingerprint analiza** - Prepoznavanje poznatih prijetnji
- **Statistička analiza** - Otkrivanje odstupanja od normalnih vrijednosti

Mrežno pokrivanje NDR sustavi pružaju "veći prostor" analize u odnosu na EDR:

- Vidljivost u cjelokupnu mrežnu infrastrukturu
- Mogućnost otkrivanja lateral movement napada
- Analiza komunikacije između sustava bez agenata

- Detekcija skrivenih tunela i kovertnih kanala

Prednosti NDR rješenja

- **Bolja efikasnost** - Ranije primjećivanje napada kroz mrežnu analizu
- **Neovisnost o agentima** - Ne zahtijeva instalaciju softvera na krajnje točke
- **Sveobuhvatna vidljivost** - Analiza cjelokupnog mrežnog prometa
- **Detekcija lateral movement-a** - Otkrivanje širenja napada kroz mrežu
- **Forenzička analiza** - Mogućnost rekonstrukcije mrežnih aktivnosti

Ograničenja NDR rješenja

- **Ograničena granularnost** - Manje detaljna analiza na razini uređaja
- **Enkriptirani promet** - Poteškoće s analizom šifriranog prometa
- **Potreba za mrežnim pristupom** - Zahtijeva konfiguraciju mrežne infrastrukture
- **Složenost implementacije** - Potrebno duboko razumijevanje mrežnih protokola

Proizvod	Ključne karakteristike
Darktrace	AI-pogonjeno samoučenje, Enterprise Immune System
Vectra AI	AI detekcija, fokus na ransomware i lateral movement
Cisco Stealthwatch	Integracija s Cisco mrežnom opremom, NetFlow analiza

Tablica 3.1. Vodeći NDR proizvodi i njihove karakteristike

Tehnologije korištene u NDR sustavima

Mrežno prikupljanje podataka

- **Network TAPs** - Fizički pristup mrežnom prometu
- **SPAN portovi** - Kopiranje prometa s mrežnih uređaja
- **Flow podatci** - NetFlow, sFlow, IPFIX protokoli
- **Packet capture** - Snimanje kompletnih mrežnih paketa

Analitički motori

- **Behavior analytics** - Prepoznavanje normalnih i anomalnih obrazaca
- **Threat intelligence** - Usporedba s bazama poznatih prijetnji

- **Machine learning modeli** - Kontinuirano učenje i poboljšanje detekcije
- **Statistical analysis** - Statistička obrada mrežnih metrika

Implementacijske preporuke

1. **Mrežna arhitektura** - Planiranje pristupnih točaka za analizu prometa
2. **Bandwidth planning** - Osiguravanje dovoljne propusnosti za analizu
3. **Storage requirements** - Planiranje kapaciteta za čuvanje mrežnih podataka
4. **Integration** - Povezivanje s postojećim SIEM i SOC procesima
5. **Tuning** - Konfiguriranje za smanjenje false positive alarma

4. XDR (Extended Detection and Response)

Definicija i evolucija

XDR (Extended Detection and Response) predstavlja sljedeću evoluciju sigurnosnih tehnologija koja kombinira elemente EDR i NDR sustava u jedinstvenu, integriranu platformu. XDR se često naziva "evoluiranom EDR" jer proširuje fokus s krajnjih točaka na cjelokupno IT okruženje organizacije, uključujući email, mreže, aplikacije, oblak servise i krajnje točke.

Holistički pristup sigurnosti

XDR rješenja nastoje riješiti fragmentaciju tradicionalnih sigurnosnih alata kroz:

Široki spektar nadzora

- **Krajnje točke** - Laptopi, desktop računala, serveri, mobilni uređaji
- **Mrežni promet** - East-west i north-south komunikacije
- **Email sustavi** - Detekcija phishing i malicious email prijetnji
- **Cloud aplikacije** - SaaS i IaaS platforme
- **Aplikacijski sloj** - Web aplikacije i API-ji
- **Identity sustavi** - Upravljanje identitetima i pristupima

Korelacija podataka XDR platforme prikupljaju i koreliraju podatke iz različitih izvora:

- Centralizirani pristup analizi sigurnosnih događaja
- Automatska korelacija između različitih sigurnosnih slojeva
- Kontekstualno povezivanje povezanih događaja
- Smanjenje false-positive alarma kroz multi-source validaciju

Ključne prednosti XDR rješenja

- **Holističan pregled** - Potpuna vidljivost u sigurnosni status organizacije
- **Smanjeni false-positives** - Korelacija podataka smanjuje lažne alarme
- **Brža detekcija** - Kombiniranje različitih detection metoda
- **Koordiniran odgovor** - Automatizirana reakcija kroz različite sustave
- **Pojednostavljena administracija** - Jedna platforma umjesto više alata
- **Poboljšana threat hunting** - Mogućnost praćenja prijetnji kroz različite slojeve

Arhitekturni pristup

Native XDR Proizvodi razvijeni iz temelja kao XDR rješenja:

- Jedinstvena arhitektura za sve komponente
- Optimizirana integracija između modula
- Konzistentno korisničko iskustvo
- Primjer: Microsoft Defender XDR

Open XDR Platforme koje integriraju postojeće sigurnosne alate:

- Fleksibilnost u odabiru najboljih alata za svaku komponentu
- Mogućnost zadržavanja postojećih investicija
- Kompleksnija implementacija i održavanje
- Primjer: Palo Alto Cortex XDR

Matematička reprezentacija odnosa

Odnos između različitih detection and response tehnologija može se prikazati kao:

$$.NDR\ EDR/\ XDR \tag{4.1}$$

$$NIDS\ IDS \tag{4.2}$$

$$IDS\ XDR \tag{4.3}$$

Gdje su:

- - unija (union) skupova
- - podskup (subset) relacija
- *NDR* - Network Detection and Response
- *EDR* - Endpoint Detection and Response
- *XDR* - Extended Detection and Response
- *IDS* - Intrusion Detection System
- *NIDS* - Network Intrusion Detection System

Ova matematička notacija pokazuje da XDR obuhvaća funkcionalnosti NDR i EDR sustava, dok tradicionalni IDS sustavi predstavljaju podskup XDR mogućnosti.

Primjeri vodećih XDR rješenja

Proizvod	**Tržišni udio**	**Ključne karakteristike**
Microsoft Defender XDR	6.9%	Native integracija s Microsoft ekosustavom, AI-powered analytics
Palo Alto Cortex XDR	5.6%	Open XDR platforma, robusna integracija podataka
CrowdStrike XDR	-	Cloud-native arhitektura, proširenje Falcon platforme
Trend Micro Vision One	-	Comprehensive threat visibility, risk prioritization
SentinelOne Singularity XDR	-	Autonomous response, Purple AI platform

Tablica 4.1. Vodeći XDR proizvodi prema tržišnom udjelu

Implementacijske preporuke

Planiranje implementacije

1. **Assessment postojeće infrastrukture** - Inventar postojećih sigurnosnih alata
2. **Gap analiza** - Identifikacija nedostataka u pokrivanju
3. **Integration planning** - Strategija integracije s postojećim sustavima
4. **Pilot implementacija** - Postupno proširivanje kroz organizaciju

Ključni faktori uspjeha

- **Executive podrška** - Potrebna podrška top managementa

- **Cross-team suradnja** - Koordinacija između IT i sigurnosnih timova
- **Skill development** - Edukacija osoblja za korištenje XDR platformi
- **Process optimization** - Prilagodba postojećih sigurnosnih procesa

Budućnost XDR tehnologija

XDR tehnologije kontinuirano evoluiraju prema:

- Većoj automatizaciji odgovora na incidente
- Integraciji s SOAR (Security Orchestration, Automation and Response) platformama
- Naprednijem machine learning i AI mogućnostima
- Boljoj integraciji s cloud-native okruženjima
- Proširenju na IoT i OT (Operational Technology) sustave

5. IDS i NIDS sustavi

Definicija i osnove

IDS (Intrusion Detection System) predstavlja temeljnu sigurnosnu tehnologiju za skeniranje sustava i detekciju upada. NIDS (Network Intrusion Detection System) je specijalizirana varijanta IDS-a fokusirana na skeniranje mrežnog prometa i detekciju mrežnih upada. Ovi sustavi predstavljaju prethodnice modernih Detection and Response tehnologija.

Ključne razlike između IDS/NIDS i DR sustava

Osnovna funkcionalnost

- **IDS/NIDS sustavi** - Pasivno nadgledanje i uzbunjivanje o detektiranim prijetnjama
- **Detection and Response sustavi** - Aktivno nadgledanje s mogućnostima automatskog odgovora

Mogućnosti odgovora IDS sustavi su ograničeni na detekciju i uzbunjivanje, dok DR sustavi mogu imati konfigurirane automatske radnje:

- Automatska izolacija kompromitiranih uređaja
- Blokiranje sumljive mrežne komunikacije
- Pokretanje forenzičkih procesa
- Eskalacija incidenata prema odgovornim timovima

Vodeći IDS/NIDS alati

Snort Snort je jedan od najpoznatijih open-source IDS/IPS alata:

Karakteristike:

- IDS s mogućnostima IPS-a (Intrusion Prevention System)

- Pravila zasnovana na prepoznavanju uzoraka (signature-based detection)
- Lagana arhitektura pogodna za manje mreže
- Može biti ograničen kod velikih mrežnih opterećenja
- Jednostavan za konfiguraciju i deployment
- Dostupnost gotovih pravila za poznate vulnerabilities

Suricata Suricata predstavlja napredni IDS/IPS alat s boljim performansama:

Karakteristike:

- Paralelna obrada paketa što rezultira boljom izvedbom od Snorta
- Podrška za multi-threading i GPU akceleraciju
- Kompatibilnost sa Snort pravilima
- Naprednije mogućnosti za veliku propusnost mreža
- Built-in support za moderne mrežne protokole

Zeek (bivši Bro) Zeek se razlikuje od tradicionalnih IDS alata fokusiranjem na mrežnu analizu:

Karakteristike:

- Fokus na detaljnoj analizi mrežnog prometa umjesto detekcije prijetnji putem pravila
- Pogodan za dubinsku inspekciju mreže i zapisivanje podataka
- Izvrsne mogućnosti za forenzičku analizu
- Skriptni jezik za prilagođene analize
- Strukturirani logovi za lakšu integraciju s drugim sustavima

Tržišno pozicioniranje

DR sustavi se tretiraju kao skuplji i bolji proizvod u odnosu na tradicionalne IDS sustave. Od DR sustava, najtraženiji su XDR-ovi zbog njihovih sveobuhvatnih mogućnosti. Ova evolucija reflektira potrebu organizacija za proaktivnijim pristupom sigurnosti koji ne samo detektira, već i automatski odgovara na prijetnje.

Implementacijski model

Hibridni pristup

Sustav	Primarni fokus	Odgovor na prijetnje
IDS/NIDS	Detekcija i uzbunjivanje	Manualine intervencije potrebne
EDR	Krajnje točke	Automatski i poluautomatski
NDR	Mrežni promet	Automatski i poluautomatski
XDR	Holistički pristup	Orkestrirani automatski odgovor

Tablica 5.1. Usporedba fokusa i mogućnosti odgovora različitih sustava

Mnoge organizacije implementiraju hibridne pristupe koji kombiniraju:

- Postojeće IDS/NIDS sustave za osnovnu detekciju
- Moderna DR rješenja za naprednu analizu i odgovor
- Centralizirane SIEM platforme za korelaciju događaja
- SOAR sustave za orkestaciju odgovora na incidente

Ovakav pristup omogućava postupnu modernizaciju sigurnosne infrastrukture uz zadržavanje postojećih investicija.

6. Komparativna analiza: Snort vs Suricata vs Zeek

Metodologija evaluacije

Na osnovu istraživanja provedenog 2022. godine u radu "Evaluating the Efficacy of Network Forensic Tools: A Comparative Analysis of Snort, Suricata, and Zeek in Addressing Cyber Vulnerabilities", analizirana su tri vodeća mrežna sigurnosna alata. Testiranje je provedeno na simuliranom mrežnom okruženju s fokusom na tri ključna kriterija.

Kriteriji procjene

Točnost detekcije Mjerena kroz:

- Broj ispravnih pozitivnih detekcija (true positives)
- Broj lažno pozitivnih slučajeva (false positives)
- Sposobnost prepoznavanja poznatih vulnerability signatures
- Detekcija anomalnih mrežnih obrazaca

Performanse Analizirane kroz:

- Brzina obrade mrežnog prometa
- Latencija u analizi paketa
- Sposobnost rada s velikim opterećenjima
- Stabilnost sustava pod stresom

Resursna potrošnja Mjerena kao:

- CPU utilizacija
- Memorijska potrošnja
- Disk I/O zahtjevi

- Mrežna bandwidth potreba

Rezultati evaluacije

Alat	Točnost detekcije	Performanse	Resursna potrošnja	Prosjek
Suricata	1	1	3	**1.67**
Zeek	3	2	1	**2.00**
Snort	2	3	2	**2.33**

Tablica 6.1. Rangiranje alata (1 = najbolji, 3 = najlošiji)

Detaljni rezultati po kategorijama

Točnost detekcije - Suricata (1. mjesto)

- **Najbolji rezultati** u prepoznavanju prijetnji
- Napredni detection engine s multi-threading podrškom
- Efikasna korelacija između različitih mrežnih slojeva
- Manje false-positive alarma u odnosu na konkurenciju

Performanse - Suricata (1. mjesto)

- **Najbrža obrada** zbog paralelne arhitekture
- Multi-threading omogućava bolje iskorištenje modernih CPU-ova
- GPU akceleracija za kompleksne pattern matching operacije
- Optimizirana za high-throughput mrežna okruženja

Resursna potrošnja - Zeek (1. mjesto)

- **Najmanji utjecaj** na performanse sustava
- Efikasno upravljanje memorijom
- Optimizirana arhitektura za kontinuiran rad
- Minimalna CPU potrošnja u idle stanju

Specifičnosti pojedinih alata

Snort - Karakteristike Prednosti:

- Umjerena potrošnja resursa
- Široka podrška zajednice i dokumentacija

- Jednostavnost konfiguracije za osnovne scenarije
- Kompatibilnost s mnogim SIEM sustavima

Nedostaci:

- Najveće kašnjenje u analizi prometa
- Više lažno pozitivnih detekcija
- Ograničene performanse kod velikih mreža
- Single-threaded arhitektura

Suricata - Karakteristike Prednosti:

- Najbolja kombinacija točnosti i performansi
- Paralelna obrada omogućava skalabilnost
- Kompatibilnost sa Snort pravilima
- Napredni inspection capabilities

Nedostaci:

- Najveće zahtjevi za resursima
- Složenija konfiguracija za optimalne performanse
- Potrebna veća memorija za napredne značajke

Zeek - Karakteristike Prednosti:

- Najbolje za forenzičku analizu
- Detaljni strukturirani logovi
- Izvrsne mogućnosti za threat hunting
- Mogućnost custom scripting

Nedostaci:

- Nije dizajniran za real-time detekciju napada
- Zahtijeva više stručnog znanja za konfiguraciju
- Kompleksniji za integraciju s existing infrastructure

Preporuke za implementaciju

Suricata - Optimalno za

- Sustave koji trebaju brzu i točnu detekciju prijetnji
- Organizacije s high-throughput mrežnim zahtjevima
- Okruženja gdje su performanse kritične
- Hybrid cloud/on-premise arhitekture

Snort - Optimalno za

- Manje mreže s ograničenim resursima
- Organizacije koje traže stabilno i dobro podržano rješenje
- Environments s postojećom Snort infrastrukturom
- Budget-conscious implementacije

Zeek - Optimalno za

- Forenzičku analizu i post-incident investigation
- Threat hunting aktivnosti
- Research i advanced analytics
- Okruženja gdje je dubinska analiza prioritet

Zaključak komparativne analize

Rezultati pokazuju da ne postoji univerzalno "najbolji" alat, već je izbor ovisan o specifičnim potrebama organizacije:

- **Za općenite sigurnosne potrebe**: Suricata pruža najbolji ukupni rezultat
- **Za ograničene resurse**: Snort predstavlja dobru kompromis opciju
- **Za naprednu analizu**: Zeek je nezamjenjiv za forenzičke potrebe

Mnoge organizacije implementiraju hibridne pristupe koristeći kombinaciju ovih alata za različite scenarije korištenja.

7. Usporedba vodećih tržišnih rješenja

Tržišni udjeli IDPS segmenta

Prema analizama PeerSpot platforme, tržište IDPS (Intrusion Detection and Prevention Software) karakteriziraju sljedeći udjeli:

Proizvod	Tržišni udio
Darktrace	19.5%
Vectra AI	11.3%
Palo Alto NATP	7.4%
Snort	3.3%

Tablica 7.1. Tržišni udjeli u IDPS kategoriji

Detaljne usporedbe komercijalnih rješenja

Darktrace Darktrace dominira tržište s revolucionarnim AI pristupom sigurnosti.

Ključne prednosti:

- **Enterprise Immune System** - Samoučeći AI sustav koji se prilagođava mrežnom okruženju
- **Stabilan rad** - Minimalan downtime s pouzdanim performansama
- **Informativni alarmi** - Kontekstualni alarmi s minimalnim "šumom"
- **Antigena funkcionalnost** - Instantni automatiziran odgovor na prijetnje
- **Mrežno i email nadgledanje** - Posebice efikasno za ove domene

Glavni nedostaci:

- **Visoka cijena** - Model naplate se smatra problematičnim
- **Ograničena endpoint zaštita** - Fokus više na mrežnu nego endpoint detekciju

- **Brojni false-positives** - Zahtijeva značajno ručno konfiguriranje
- **Slaba integracija** - Ograničena automatizacija s drugim alatima
- **Dokumentacija** - Potrebno poboljšanje korisničke podrške

Vectra AI Vectra AI se fokusira na AI-pogonjena rješenja za detekciju naprednih prijetnji.

Ključne prednosti:

- **Ocjene rizika** - Napredni scoring sustav za bolje prioritete
- **AI detekcija** - Omogućava brže i učinkovitije reagiranje
- **Microsoft integracija** - Poboljšava vidljivost prijetnji u Microsoft okruženju
- **Povezivanje prijetnji** - Korelacija s uređajima za bolju analizu napada
- **Cognito Streams** - Detaljan pregled mreže za lakšu detekciju

Glavni nedostaci:

- **SIEM ovisnost** - Zahtijeva integraciju sa SIEM za punu funkcionalnost
- **Minimalni logovi** - Ograničene informacije proslijeđene SIEM sustavu
- **Ograničena host vidljivost** - Nedostatna vidljivost na domaćinu
- **Ograničena prilagodba** - Fewer customization mogućnosti
- **False-positive tuning** - Težak proces podešavanja FP alarma

Cisco Sourcefire SNORT Cisco Snort predstavlja enterprise verziju popularnog open-source alata.

Ključne prednosti:

- **Skalabilnost** - Jednostavno skaliranje za veće radne okoline
- **Cisco integracija** - Izvrsna integracija s Cisco mrežnom opremom
- **Tehnička podrška** - Profesionalna 24/7 podrška
- **Cijena** - Kompetitivne cijene u odnosu na premium rješenja
- **Filtriranje prometa** - Vrlo dobra zaštita od malware-a i web prijetnji
- **Niska FP stopa** - Dobra točnost detekcije s malo false-positives

Glavni nedostaci:

- **Performanse** - Mogućnost poboljšanja brzine obrade
- **Informativnost alarma** - Alarmi mogu biti informatiniji
- **Kompleksno postavljanje** - Početna konfiguracija može biti izazovna
- **Integracija** - Ograničena integracija s non-Cisco alatima

Palo Alto Networks Advanced Threat Prevention Palo Alto NATP predstavlja integrirani pristup sigurnosti kroz next-generation vatrozide.

Ključne prednosti:

- **Robusna zaštita** - Napredna zaštita protiv zlućudnog koda
- **Napredni vatrozid** - Najnapredniji vatrozid s intuitivnim sučeljem
- **Upravljanje aplikacijama** - Kvalitetno upravljanje i propusnost mreže
- **Filtar sadržaja** - Napredni content filtering i IP management
- **Machine learning** - Poboljšano otkrivanje nepoznatih prijetnji

Glavni nedostaci:

- **Tehnička podrška** - Nedostatna razina tehničke podrške
- **Složena implementacija** - Kompleksna početna instalacija
- **Visoka cijena** - Skupo licenciranje i hardware troškovi
- **ICAP podrška** - Nedostaje podrška za ICAP protokol

XDR segment - vodeći proizvodi

CrowdStrike Falcon (15.5% tržišni udio) Ocjena korisnika: 4.8/5 (1410 recenzija)

Prednosti:

- Napredna detekcija prijetnji u stvarnom vremenu
- Nativna cloud arhitektura s fleksibilnošću implementacije
- AI/ML tehnologija za detekciju i prevenciju
- Lagani agent s minimalnim utjecajem na performanse
- Napredne mogućnosti forenzike i threat hunting

Nedostaci:

- Viša cijena u odnosu na konkurenciju

- Složenost prilagodbe upozorenja i izvještaja
- Zahtijeva internetsku vezu za optimalnu zaštitu
- Strma krivulja učenja za potpuno iskorištavanje

Microsoft Defender XDR (6.9% tržišni udio) Ocjena korisnika: 4.4/5 (1452 recenzije)

Prednosti:

- Besprijekorna integracija s Microsoft proizvodima
- Cjenovno pristupačniji uz Microsoft 365 pretplatu
- Automatizacija odgovora na incidente
- Jednostavna implementacija za postojeće Microsoft korisnike

Nedostaci:

- Ograničene integracije s alatima trećih strana
- Složen proces početnog postavljanja
- Visoka potrošnja sistemskih resursa
- Složena struktura licenciranja

Wazuh (13.0% tržišni udio) Ocjena korisnika: 7.5/10

Prednosti:

- Besplatna open-source platforma
- Visoka prilagodljivost i fleksibilnost
- Sveobuhvatna analiza logova
- Podrška za različite platforme

Nedostaci:

- Zahtijeva značajnu tehničku stručnost
- Ograničena profesionalna podrška
- Nedostatna dokumentacija za complex troubleshooting
- Može se boriti s velikim količinama podataka

Trendovi i insights

AI i Machine Learning dominacija Sva vodeća rješenja integriraju napredne AI/ML capabilities:

- Darktrace s Enterprise Immune System konceptom
- Vectra AI s fokusiranošću na AI-driven detection
- CrowdStrike s cloud-native AI platformom
- Palo Alto s machine learning za nepoznate prijetnje

Hibridni pristupi Organizacije sve više kombiniraju:

- Komercijalna rješenja za kritične komponente
- Open-source alate za specifične potrebe (Wazuh, Snort)
- Cloud-native platforms za skalabilnost
- On-premise rješenja za compliance zahtjeve

8. Analiza prema veličini poduzeća

Segmentacija tržišta

Različite veličine organizacija imaju specifične sigurnosne potrebe, budžetska ograničenja i tehničke kapacitete. Analiza preferencija prema veličini poduzeća pokazuje jasne trendove u odabiru sigurnosnih rješenja.

Mala poduzeća (1-100 zaposlenika)

Ključni faktori odlučivanja

- **Ograničen budžet** - Potreba za cost-effective rješenja
- **Minimalna IT podrška** - Potreba za jednostavne, "plug-and-play" alate
- **Osnovno sigurnosno znanje** - Ograničena ekspertiza za kompleksne sustave
- **Compliance zahtjevi** - Osnovni regulatory requirements

Preporučena rješenja

1. Microsoft Defender XDR

- **Razlog**: Već uključen u Microsoft 365 subscription
- **Prednosti**: Jednostavna implementacija, poznato sučelje
- **Ograničenja**: Ograničene advanced značajke

2. Darktrace

- **Razlog**: Odličnu potpunu zaštitu uz relativno pristojnu cijenu
- **Prednosti**: Samoučeći sustav, minimalno održavanje
- **Ograničenja**: Početni troškovi mogu biti visoki

3. Wazuh (za tehnički potkovane timove)

- **Razlog**: Besplatno rješenje s dobrim capabilities
- **Prednosti**: Nulti licencijski troškovi
- **Ograničenja**: Zahtijeva značajnu tehničku ekspertizu

Srednja poduzeća (100-1000 zaposlenika)

Ključni faktori odlučivanja

- **Balans cijena/performanse** - Potreba za "zlatnu sredinu"
- **Rastući IT timovi** - Veći tehnički kapaciteti
- **Compliance složenost** - Veći regulatory zahtjevi
- **Hibridna infrastruktura** - Kombinacija cloud/on-premise sustava

Preporučena rješenja

1. Cisco Sourcefire SNORT

- **Razlog**: Zlatna sredina između cijene i usluge
- **Prednosti**: 24/7 tehnička podrška, dobra skalabilnost
- **Ograničenja**: Može zahtijevati dodatnu integraciju

2. SentinelOne

- **Razlog**: Dobar balans između cijene i naprednih značajki
- **Prednosti**: Autonomni AI agent, rollback capabilities
- **Ograničenja**: Srednji troškovi implementacije

3. Vectra AI + Darktrace

- **Razlog**: Kombinacija AI detection s network focus
- **Prednosti**: Napredne AI capabilities, good ROI
- **Ograničenja**: Potreba za SIEM integracijom

Velika poduzeća (1000+ zaposlenika)

Ključni faktori odlučivanja

- **Napredne sigurnosne potrebe** - Kompleksni threat landscape
- **Regulatory compliance** - Strogi industrijski zahtjevi

- **Velike IT organizacije** - Dedicated sigurnosni timovi
- **Complex infrastructure** - Multi-cloud, hybrid okruženja
- **24/7 SOC operations** - Kontinuirani sigurnosni nadzor

Preporučena rješenja

1. CrowdStrike Falcon

- **Razlog**: Najčešći izbor zbog naprednih mogućnosti
- **Prednosti**: Premium detekcija, threat hunting, cloud-native
- **Ograničenja**: Visoka cijena, complex learning curve

2. Vectra AI

- **Razlog**: Transparentan cjenik i efikasno pronalaženje grešaka
- **Prednosti**: Minimalna redundancija, advanced AI
- **Ograničenja**: Potrebna SIEM integracija

3. Palo Alto Cortex XDR

- **Razlog**: Najkompletniji set značajki za complex environments
- **Prednosti**: Robusna integracija podataka, comprehensive coverage
- **Ograničenja**: Kompleksna implementacija, visoki troškovi

Usporedni prikaz preferencija

Kriterij	Mala poduzeća	Srednja poduzeća	Velika poduzeća
Primarni fokus	Jednostavnost i cijena	Balans cijena/performanse	Napredne mogućnosti
Budžet	$5,000-$50,000 godišnje	$50,000-$500,000 godišnje	$500,000+ godišnje
IT ekspertiza	Osnovna	Umjerena	Napredna
Preferirana rješenja	Microsoft Defender, Darktrace, Wazuh	Snort, SentinelOne, Vectra AI	CrowdStrike, Cortex XDR, Vectra AI
Deployment model	Cloud-first	Hybrid	Multi-cloud hybrid

Tablica 8.1. Usporedba karakteristika prema veličini poduzeća

Specifični slučajevi korištenja

Finansijske institucije Posebni zahtjevi:

- Strogi compliance (PCI DSS, SOX, Basel III)
- 24/7 monitoring zahtjevi
- Low latency potrebe
- Advanced threat protection

Preporučena rješenja:

- **Velike banke**: CrowdStrike + Cortex XDR
- **Regionalne banke**: SentinelOne + Vectra AI
- **Credit unions**: Microsoft Defender + Darktrace

Zdravstvene organizacije Posebni zahtjevi:

- HIPAA compliance
- Legacy system support
- Patient data protection
- Minimal disruption requirements

Preporučena rješenja:

- **Veliki health systems**: CrowdStrike + specialized healthcare SIEM
- **Manje klinike**: Microsoft Defender + cloud backup solutions
- **Telemedicine**: Darktrace za network anomaly detection

Proizvodne tvrtke Posebni zahtjevi:

- OT/IT convergence security
- Industrial control system protection
- Supply chain security
- Minimal production disruption

Preporučena rješenja:

- **Large manufacturers**: Specialized OT security + Cortex XDR
- **Mid-size**: Darktrace (excellent for OT) + endpoint protection
- **Small manufacturing**: Simplified solutions s OT awareness

Migracija između rješenja

Postupni pristup za rast organizacije

Faza 1: Startup → Mala tvrtka

- Start: Osnovni antivirus + Windows Defender
- Evolucija: Microsoft Defender XDR
- Next step: Dodavanje network monitoring (Darktrace entry-level)

Faza 2: Mala → Srednja tvrtka

- Assessment postojećih rješenja
- Pilot testiranje advanced platforms (SentinelOne, Vectra AI)
- Postupna migracija s overlap periodom
- Staff training i process adaptation

Faza 3: Srednja → Velika tvrtka

- Comprehensive security architecture review
- Enterprise-grade platform selection (CrowdStrike, Cortex XDR)
- SOC establishment ili outsourcing
- Advanced threat hunting capabilities

ROI analize po segmentima

Mala poduzeća Tipični ROI metrics:

- Incident response time reduction: 60-80%
- Security admin time savings: 40-60%
- Compliance cost reduction: 30-50%
- Payback period: 6-12 mjeseci

Srednja poduzeća Tipični ROI metrics:

- False positive reduction: 50-70%
- Mean time to detection improvement: 70-85%
- Security team productivity gain: 50-80%
- Payback period: 12-18 mjeseci

Velika poduzeća Tipični ROI metrics:

- Advanced threat detection improvement: 80-95%
- Incident containment time reduction: 85-95%
- Security operations cost optimization: 60-80%
- Payback period: 18-24 mjeseca

Preporuke za implementaciju

Ključni faktori uspješne implementacije

1. Proper sizing

- Realistic assessment organizacijskih potreba
- Budžetiranje za rast (20-30% buffer)
- Planiranje za staff augmentation

2. Phased approach

- Pilot s kritičnim sustavima
- Postupno proširivanje coverage
- Continuous optimization

3. Change management

- Executive sponsorship
- User training programs
- Process documentation updates

Česti problemi i rješenja

Mala poduzeća:

- **Problem**: Nedostatak expertise
- **Rješenje**: Managed security services ili cloud-native rješenja

Srednja poduzeća:

- **Problem**: Integration complexity

- **Rješenje**: Professional services za implementation

Velika poduzeća:

- **Problem**: Scale i performance issues
- **Rješenje**: Enterprise architecture planning i performance testing

9. Zaključak

Ključni nalazi istraživanja

Analiza sigurnosnih tehnologija za detekciju i odgovor na prijetnje pokazuje jasnu evoluciju od tradicionalnih IDS/NIDS sustava prema sofisticiranim XDR platformama. Ova evolucija reflektira rastuće potrebe organizacija za proaktivnim, automatiziranim i sveobuhvatnim sigurnosnim rješenjima.

Tehnološka evolucija

Istraživanje pokazuje sljedeći progresivni razvoj:

1. **IDS/NIDS era** - Pasivna detekcija i uzbunjivanje
2. **EDR era** - Fokusirani endpoint response capabilities
3. **NDR era** - Mrežno-centrirana detection i response
4. **XDR era** - Holistička integracija svih sigurnosnih slojeva

Matematički odnos $.NDR\ EDR/\ XDR$ potvrđuje da XDR predstavlja superset postojećih tehnologija, a ne njihovu zamjenu.

Tržišne dinamike

Analiza tržišta otkriva:

- **AI/ML dominaciju** - Sva vodeća rješenja integriraju napredne AI capabilities
- **Cloud-first pristup** - Nativna cloud arhitektura postaje standard
- **Konsolidaciju alata** - Organizacije preferiraju integrirane platforme
- **Demokratizaciju sigurnosti** - Dostupnost naprednih capabilities i manjim organizacijama

Komparativni uvidi

Performanse alata

Na osnovu detaljne analize Snort, Suricata i Zeek sustava:

- **Suricata** se pokazala kao najbolji overall performer (prosjek 1.67)
- **Zeek** excels u forenzičkoj analizi i resource efficiency
- **Snort** predstavlja solid middle-ground opciju

Komercijalna rješenja

Tržišni lideri pokazuju jasnu segmentaciju:

- **Darktrace (19.5%)** - Pionir u AI-driven security
- **CrowdStrike (15.5%)** - Premium endpoint protection leader
- **Wazuh (13.0%)** - Dominant open-source alternative
- **Vectra AI (11.3%)** - Specialized AI network detection

Segmentacijske preporuke - prema veličini organizacije

Istraživanje potvrđuje da ne postoji 'one-size-fits-all' rješenje:

Mala poduzeća:

- Preferirane opcije: Microsoft Defender XDR, Darktrace, Wazuh
- Ključni faktori: Jednostavnost, cijena, minimal maintenance
- ROI focus: Quick wins i operational efficiency

Srednja poduzeća:

- Preferirane opcije: Cisco Snort, SentinelOne, Vectra AI
- Ključni faktori: Balans performansi i cijene, skalabilnost
- ROI focus: False positive reduction i team productivity

Velika poduzeća:

- Preferirane opcije: CrowdStrike Falcon, Cortex XDR, Vectra AI
- Ključni faktori: Advanced capabilities, enterprise integration

- ROI focus: Advanced threat protection i operational optimization

Buduće perspektive

Tehnološki trendovi

Očekujemo sljedeće razvojne smjerove:

- **Autonomous security** - Potpuno automatizirani odgovor na incidente
- **Quantum-resistant security** - Priprema za post-quantum cryptography
- **Zero Trust integration** - Dublja integracija s Zero Trust arhitekturama
- **Edge security** - Proširenje na IoT i edge computing okruženja
- **Privacy-preserving analytics** - Balans između sigurnosti i privatnosti

Tržišne evolucije

- **Platform konsolidacija** - Fewer, ali comprehensive vendors
- **Democratization** - Advanced capabilities dostupne manjim organizacijama
- **Specialization** - Sector-specific security solutions
- **Outcome-based pricing** - Shift od capacity-based prema results-based pricing

Praktične implikacije

Za IT profesionalce

1. **Skill development** - Ulaganje u AI/ML i cloud security expertise
2. **Architecture thinking** - Holistički pristup sigurnosnoj arhitekturi
3. **Automation focus** - Automatizacija kao competitive advantage
4. **Business alignment** - Povezivanje sigurnosnih investicija s business outcomes

Za organizacije

1. **Strategic planning** - 3-5 godina visibility u sigurnosnoj roadmap
2. **Vendor relationships** - Partnership approach s key security vendors
3. **Hybrid approaches** - Kombinacija commercial i open-source rješenja
4. **Continuous assessment** - Regular evaluation sigurnosne efikasnosti

Završne preporuke

Immediate actionables

- **Assessment** - Audit postojećih sigurnosnih capabilities
- **Gap analysis** - Identifikacija nedostataka u detection/response coverage
- **Pilot testing** - Controlled evaluation odabranih rješenja
- **ROI planning** - Quantified business case za sigurnosne investicije

Long-term considerations

- **Platform approach** - Migracija prema integriranim platforms umjesto point solutions
- **Cloud readiness** - Priprema za cloud-first security architectures
- **Skill investment** - Continuous learning i certification programs
- **Threat landscape monitoring** - Active tracking evolving threat landscape

Sigurnosni krajolika kontinuirano evoluira, a organizacije koje će uspješno navigirati ovim promjenama bit će one koje kombiniraju tehnološku inovaciju s promišljenim strategijskim planiranjem i kontinuiranim ulaganjem u ljudski kapital. XDR tehnologije predstavljaju značajan korak naprijed, ali njihov uspjeh ovisi o proper implementation i ongoing optimization prema specifičnim organizacijskim potrebama.

Usporedba alata za nadzor i intervenciju na krajnjim točkama (Endpoint Detection and Response)

Ante Čavar

Sažetak

Comparison of EDR tools

Ante Čavar

Abstract