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 i evolucija tehnologija

Sigurnosni krajolik kontinuirano evoluira od tradicionalnih IDS/NIDS sustava prema sofisticiranim XDR platformama. Ova evolucija reflektira rastuće potrebe organizacija za proaktivnim, automatiziranim i sveobuhvatnim sigurnosnim rješenjima.

Progresivni razvoj može se prikazati kroz četiri glavne ere. IDS/NIDS era karakterizirana je pasivnom detekcijom i uzbunijavanjem, EDR era donosi fokusirane endpoint response capabilities, NDR era uvodi mrežno-centriranu detekciju i response, dok XDR era predstavlja holističku integraciju svih sigurnosnih slojeva. Matematički odnos $.NDR\ EDR/\ XDR$ potvrđuje da XDR predstavlja superset postojećih tehnologija, a ne njihovu zamjenu.

2. Komparativna analiza osnovnih alata

2.1. IDS i NIDS sustavi

IDS (Intrusion Detection System) predstavlja temeljnu sigurnosnu tehnologiju za skeniranje sustava i detekciju upada, dok je NIDS (Network Intrusion Detection System) specijalizirana varijanta fokusirana na mrežni promet. Osnovna razlika između IDS/NIDS i DR sustava leži u tome što IDS sustavi pružaju pasivno nadgledanje i uzbunjivanje, dok DR sustavi omogućavaju aktivno nadgledanje s mogućnostima automatskog odgovora poput izolacije kompromitiranih uređaja i blokiranja sumljive komunikacije.

Snort je jedan od najpoznatijih open-source IDS/IPS alata s pravilima zasnovanim na prepoznavanju uzoraka. Pogodan je za manje mreže ali može biti ograničen kod velikih mrežnih opterećenja zbog single-threaded arhitekture. Suricata predstavlja napredni IDS/IPS alat s paralelnom obradom paketa što rezultira boljim performansama od Snorta. Kompatibilan je sa Snort pravilima i ima naprednije mogućnosti za veliku propusnost mreža kroz multi-threading i GPU akceleraciju. Zeek se razlikuje fokusiranjem na detaljnu analizu mrežnog prometa umjesto detekcije putem pravila, što ga čini izvrsnim za forenzičku analizu kroz strukturirane logove i skriptni jezik za prilagođene analize.

2.2. Rezultati evaluacije performansi

Na osnovu istraživanja provedenog 2022. godine [1], analizirana su tri vodeća mrežna sigurnosna alata kroz kriterije točnosti detekcije, performansi i resursne potrošnje.

Suricata se pokazala kao najbolji overall performer s prosječnom ocjenom 1.67, posebice excelerajući u točnosti detekcije i performansama zbog naprednog detection engine-a s multi-threading podrškom. Zeek dominira u resursnoj potrošnji s najmanjih utjecajem na perfor-

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 2.1. Rangiranje alata (1 = najbolji, 3 = najlošiji)

manse sustava, što ga čini optimalnim za kontinuiran rad i forenzičku analizu. Snort predstavlja solid middle-ground opciju s umjerenom potrošnjom resursa ali najvećim kašnjenjem u analizi prometa.

3. EDR tehnologija

EDR (Endpoint Detection and Response) tehnologija kontinuirano nadzire krajnje točke poput laptopa, desktop računala i mobilnih uređaja [2, 3]. EDR rješenja predstavljaju evoluciju tradicionalnih antivirus programa kroz kontinuirani 24/7 nadzor koji analizira procese, aplikacije, mrežne veze, datotečne operacije i korisničke aktivnosti.

EDR sustavi rade po principu "walled garden" - fokusiraju se isključivo na krajnje točke unutar organizacije, što omogućava duboku integraciju i detaljnu analizu, ali ograničava vidljivost na mrežne aktivnosti između uređaja. Glavne prednosti uključuju visoku granularnost detekcije na razini procesa i datoteka, posebnu korisnost za zaštitu udaljenih radnika, detaljne logove za forenzičku analizu te mogućnost trenutne izolacije kompromitiranih uređaja.

Ograničenja EDR rješenja obuhvaćaju ograničenu mrežnu vidljivost jer ne pružaju uvid u mrežni promet između uređaja, ovisnost o agentima koji zahtijevaju instalaciju softvera na svakom uređaju te potencijalnu potrošnju resursa koja može utjecati na performanse uređaja.

4. NDR tehnologija

NDR (Network Detection and Response) tehnologija se fokusira na analizu mrežnog prometa umjesto na krajnje točke [4, 5]. NDR rješenja kontinuirano nadziru i analiziraju mrežne komunikacije identificirajući sumnjive aktivnosti, anomalije i sigurnosne prijetnje koje se mogu proširiti kroz mrežu.

NDR sustavi analiziraju mrežni promet na različitim razinama kroz praćenje prometa na vatrozidima, ruterima i switchevima, analizu east-west prometa između internal sustava, nadzor north-south prometa prema vanjskim mrežama te deep packet inspection za detaljnu analizu sadržaja. Koriste napredne analitičke metode uključujući strojno učenje za detekciju anomalija, analizu ponašanja za prepoznavanje neobičnih komunikacijskih obrazaca te statističku analizu za otkrivanje odstupanja.

NDR rješenja pružaju "veći prostor" analize u odnosu na EDR kroz vidljivost u cjelokupnu mrežnu infrastrukturu, mogućnost otkrivanja lateral movement napada, analizu komunikacije između sustava bez agenata te detekciju skrivenih tunela i kovertnih kanala. Glavna ograničenja uključuju ograničenu granularnost na razini uređaja, poteškoće s analizom šifriranog prometa te složenost implementacije koja zahtijeva duboko razumijevanje mrežnih protokola.

5. XDR tehnologija

XDR (Extended Detection and Response) predstavlja sljedeću evoluciju sigurnosnih tehnologija koja kombinira elemente EDR i NDR sustava u jedinstvenu, integriranu platformu [6–8]. 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.

XDR rješenja nastoje riješiti fragmentaciju tradicionalnih sigurnosnih alata kroz široki spektar nadzora koji obuhvaća krajnje točke, mrežni promet, email sustave, cloud aplikacije, aplikacijski sloj i identity sustave. Korelacija podataka omogućava centralizirani pristup analizi sigurnosnih događaja, automatsku korelaciju između različitih sigurnosnih slojeva, kontekstualno povezivanje povezanih događaja te smanjenje false-positive alarma kroz multi-source validaciju.

6. Usporedba vodećih tržišnih rješenja

6.1. Tržišni udjeli i pozicioniranje

Prema analizama PeerSpot platforme [9], tržište karakteriziraju sljedeći udjeli: Darktrace s 19.5% dominira IDPS segment kroz revolucionarni AI pristup, Vectra AI drži 11.3% fokusirajući se na AI-pogonjena rješenja, dok CrowdStrike Falcon vodi XDR segment s 15.5% tržišnog udjela [10]. Wazuh predstavlja dominantnu open-source alternativu s 13.0% udjela.

6.2. Analiza ključnih proizvoda

Darktrace dominira tržište s Enterprise Immune System konceptom - samoučećim AI sustavom koji se prilagođava mrežnom okruženju [11]. Prednosti uključuju stabilan rad s minimalnim downtime-om, informativne alarme s kontekstualnim informacijama te Antigena funkcionalnost za instantni automatiziran odgovor. Glavni nedostaci su visoka cijena s problematičnim modelom naplate, ograničena endpoint zaštita jer je fokus više na mrežu, brojni false-positives koji zahtijevaju značajno ručno konfiguriranje te slaba integracija s ograničenom automatizacijom.

CrowdStrike Falcon predstavlja premium endpoint protection leader s nativnom cloud arhitekturom, AI/ML tehnologijom za detekciju i prevenciju, lagenim agentom s minimalnim utjecajem na performanse te naprednim mogućnostima forenzike i threat hunting [10]. Nedostaci uključuju višu cijenu u odnosu na konkurenciju, složenost prilagodbe upozorenja, zahtjev za internetskom vezom za optimalnu zaštitu te strmu krivulju učenja.

Cisco Sourcefire SNORT se ističe kao zlatna sredina između cijene i usluge s 24/7 tehničkom

podrškom [12, 13]. Prednosti uključuju jednostavno skaliranje za veće radne okoline, dobru integraciju s Cisco alatima, izvrsnu tehničku podršku te dobru detekciju prijetnji s malo false-positives. Nedostaci obuhvaćaju performanse koje se mogu poboljšati, alarme koji mogu biti informativniji te kompliciranо početno postavljanje.

Wazuh kao dominantna open-source alternativa nudi besplatnu platformu s visokom prilagodljivošću, sveobuhvatnom analizom logova i podrškom za različite platforme [10, 14]. Glavni izazovi su potreba za značajnom tehničkom stručnošću, ograničena profesionalna podrška, nedostatna dokumentacija za complex troubleshooting te potencijalni problemi s velikim količinama podataka.

7. Analiza prema veličini poduzeća

Različite veličine organizacija imaju specifične sigurnosne potrebe, budžetska ograničenja i tehničke kapacitete što rezultira jasnim trendovima u odabiru sigurnosnih rješenja [9].

7.1. Mala poduzeća (1-100 zaposlenika)

Mala poduzeća karakteriziraju ograničen budžet od $5,000-$50,000 godišnje, minimalna IT podrška koja zahtijeva jednostavne "plug-and-play" alate, osnovno sigurnosno znanje s ograničenom ekspertizom za kompleksne sustave te osnovni compliance zahtjevi. Preporučena rješenja uključuju Microsoft Defender XDR zbog uključenosti u Microsoft 365 subscription s jednostavnom implementacijom, Darktrace za odličnu potpunu zaštitu s relativno pristojnom cijenom kroz samoučeći sustav koji zahtijeva minimalno održavanje, te Wazuh za tehnički potkovane timove kao besplatno rješenje s dobrim capabilities ali značajnim tehničkim zahtjevima.

7.2. Srednja poduzeća (100-1000 zaposlenika)

Srednja poduzeća traže balans cijena/performanse kao "zlatnu sredinu" s budžetom od $50,000-$500,000 godišnje, imaju rastuće IT timove s većim tehničkim kapacitetima, suočavaju se s većim regulatory zahtjevima te upravljaju hibridnom infrastrukturom kombiniranjem cloud/on-premise sustava. Optimalna rješenja su Cisco Sourcefire SNORT kao zlatna sredina između cijene i usluge s 24/7 tehničkom podrškom [9], SentinelOne koji pruža dobar balans između cijene i naprednih značajki kroz autonomni AI agent s rollback capabilities, te kombinacija Vectra AI s Darktrace za napredne AI capabilities s dobrim ROI-jem.

7.3. Velika poduzeća (1000+ zaposlenika)

Velika poduzeća imaju napredne sigurnosne potrebe s budžetom od $500,000+ godišnje, suočavaju se s kompleksnim threat landscape-om i strogim industrijskim zahtjevima, imaju dedicated sigurnosne timove s velikim IT organizacijama te upravljaju multi-cloud, hybrid okruženjima s 24/7 SOC operacijama. Preporučena rješenja su CrowdStrike Falcon kao najčešći izbor zbog premium detekcije, threat hunting capabilities i cloud-native arhitekture [10], Vectra AI s transparentnim cjennikom i efikasnim pronalaženjem grešaka kroz minimalnu redundanciju [15], te Palo Alto Cortex XDR s najkompletnijim setom značajki za complex environments kroz robusnu integraciju podataka [14].

8. Zaključak

Ključni nalazi

Analiza sigurnosnih tehnologija pokazuje jasnu evoluciju od tradicionalnih IDS/NIDS sustava prema sofisticiranim XDR platformama. Suricata se pokazala kao najbolji overall performer među open-source alatima s prosječnom ocjenom 1.67 [1], dok u komercijalnom segmentu Darktrace dominira s 19.5% tržišnog udjela kroz AI-driven pristup [9].

Tržišne dinamike pokazuju AI/ML dominaciju u svim vodećim rješenjima, cloud-first pristup kao novi standard, konsolidaciju alata gdje organizacije preferiraju integrirane platforme te demokratizaciju sigurnosti kroz dostupnost naprednih capabilities manjim organizacijama.

Segmentacijske preporuke

Ne postoji "one-size-fits-all" rješenje već je optimalan izbor ovisan o veličini organizacije. Mala poduzeća trebaju fokus na jednostavnost i cijenu kroz Microsoft Defender XDR, Darktrace ili Wazuh. Srednja poduzeća zahtijevaju balans performansi i cijene kroz Cisco Snort, SentinelOne ili Vectra AI. Velika poduzeća trebaju napredne capabilities kroz CrowdStrike Falcon, Cortex XDR ili Vectra AI [10, 14].

Buduće perspektive

Očekujemo evoluciju prema autonomous security s potpuno automatiziranim odgovorom na incidente, quantum-resistant security za pripremu post-quantum cryptography ere, dublju Zero Trust integraciju, proširenje na IoT i edge computing okruženja te privacy-preserving analytics za balans između sigurnosti i privatnosti.

Sigurnosni krajolik 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.

9. Sažetak

Ovaj rad analizira evoluciju sigurnosnih tehnologija za detekciju i odgovor na prijetnje, fokusirajući se na prijelaz od tradicionalnih IDS/NIDS sustava prema modernim XDR platformama. Istraživanje obuhvaća komparativnu analizu ključnih tehnologija (EDR, NDR, XDR), evaluaciju performansi vodećih alata te segmentacijske preporuke prema veličini organizacije.

Analiza je provedena kroz sistematičku evaluaciju akademskih istraživanja, komercijalnih usporedbi te tržišnih podataka. Glavni empirijski izvor predstavlja istraživanje iz 2022. godine koje uspoređuje performanse Snort, Suricata i Zeek alata kroz kriterije točnosti detekcije, performansi i resursne potrošnje. Dodatno su analizirani tržišni udjeli i korisničke evaluacije vodećih komercijalnih rješenja putem PeerSpot i G2 platformi.

Istraživanje pokazuje da Suricata predstavlja najbolji overall performer među open-source alatima s prosječnom ocjenom 1.67, excelerajući u točnosti detekcije i performansama. U komercijalnom segmentu, Darktrace dominira IDPS tržište s 19.5% udjela kroz revolucionarni AI pristup, dok CrowdStrike Falcon vodi XDR segment s 15.5% tržišnog udjela. Wazuh se etablirao kao dominantna open-source alternativa s 13.0% udjela.

Sigurnosni krajolik kontinuirano evoluira prema integriranim, AI-pogonjenim rješenjima koja kombiniraju detekciju i automatiziran odgovor kroz multiple sigurnosne slojeve. Uspješne organizacije bit će one koje kombiniraju tehnološku inovaciju s promišljenim strategijskim planiranjem i kontinuiranim ulaganjem u ljudski kapital, prilagođavajući odabir tehnologija specifičnim organizacijskim potrebama i ograničenjima.

10. Literatura

[1] “Evaluating the efficacy of network forensic tools: A comparative analysis of snort, suricata, and zeek in addressing cyber vulnerabilities”, 2022., pristupljeno: 24.3.2025. [Mrežno]. Adresa: https://sansorg.egnyte.com/dl/l1u6Zjhdgy

[2] CrowdStrike, “Endpoint detection and response (edr)”, pristupljeno: 10.3.2025. [Mrežno]. Adresa: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/

[3] Microsoft, “What is edr (endpoint detection and response)”, pristupljeno: 10.3.2025. [Mrežno]. Adresa: https://www.microsoft.com/en-us/security/business/security-101/what-is-edr-endpoint-detection-response

[4] Fortinet, “What is ndr”, pristupljeno: 10.3.2025. [Mrežno]. Adresa: https://www.fortinet.com/resources/cyberglossary/what-is-ndr

[5] Cisco, “What is network detection response”, pristupljeno: 10.3.2025. [Mrežno]. Adresa: https://www.cisco.com/c/en/us/products/security/what-is-network-detection-response.html

[6] Corelight, “Xdr extended detection and response”, pristupljeno: 10.3.2025. [Mrežno]. Adresa: https://corelight.com/resources/glossary/xdr-extended-detection-and-response

[7] P. A. Networks, “What is extended detection response (xdr)”, pristupljeno: 10.3.2025. [Mrežno]. Adresa: https://www.paloaltonetworks.com/cyberpedia/what-is-extended-detection-response-XDR

[8] CrowdStrike, “Extended detection and response (xdr)”, pristupljeno: 10.3.2025. [Mrežno]. Adresa: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-

security/extended-detection-and-response-xdr/

[9] PeerSpot, “Cisco sourcefire snort vs darktrace vs vectra ai”, 2025., pristupljeno: 9.4.2025. [Mrežno]. Adresa: https://www.peerspot.com/products/comparisons/cisco-sourcefire-snort_vs_darktrace_vs_vectra-ai

[10] G2, “Crowdstrike falcon endpoint protection platform vs wazuh vs sentinelone singularity vs microsoft defender xdr”, 2025., pristupljeno: 14.5.2025. [Mrežno]. Adresa: https://www.g2.com/compare/crowdstrike-falcon-endpoint-protection-platform-vs-wazuh-the-open-source-security-platform-vs-sentinelone-singularity-vs-microsoft-defender-xdr

[11] PeerSpot, “Darktrace pros and cons”, pristupljeno: 9.4.2025. [Mrežno]. Adresa: https://www.peerspot.com/products/darktrace-pros-and-cons#pro-aspect-container

[12] ——, “Cisco sourcefire snort pros and cons”, pristupljeno: 9.4.2025. [Mrežno]. Adresa: https://www.peerspot.com/products/cisco-sourcefire-snort-pros-and-cons#pro-aspect-container

[13] ——, “Cisco sourcefire snort vs palo alto networks advanced threat prevention”, 2025., pristupljeno: 16.4.2025. [Mrežno]. Adresa: https://www.peerspot.com/products/comparisons/cisco-sourcefire-snort_vs_palo-alto-networks-advanced-threat-prevention

[14] G2, “Palo alto networks cortex xdr vs wazuh vs vectra ai platform vs darktrace detect”, 2025., pristupljeno: 16.5.2025. [Mrežno]. Adresa: https://www.g2.com/compare/palo-alto-networks-cortex-xdr-vs-wazuh-the-open-source-security-platform-vs-vectra-ai-platform-vs-darktrace-detect

[15] PeerSpot, “Vectra ai pros and cons”, pristupljeno: 9.4.2025. [Mrežno]. Adresa: https://www.peerspot.com/products/vectra-ai-pros-and-cons#pro-aspect-container