Tjedan 12.5. - 16.5.

#seminar2

Usporedba 1

Obrađeno: https://www.g2.com/compare/crowdstrike-falcon-endpoint-protection-platform-vs-wazuh-the-open-source-security-platform-vs-sentinelone-singularity-vs-microsoft-defender-xdr
Autor: G2
Pristupljeno: 14.5.2025

TL;DR
Usporedba CrowdStrike Falcon, Wazuh, SentinelOne i Microsoft Defender XDR sigurnosnih platformi za zaštitu krajnjih točaka i proširenu detekciju i odgovor na prijetnje.

Udio na tržištu (XDR kategorija)

CrowdStrike Falcon - 15.5%
Microsoft Defender - 6.9%
Wazuh - 13.0%
SentinelOne - nije specificirano

Ocjene korisnika

CrowdStrike Falcon - 4.8/5 (1410 recenzija)
Microsoft Defender - 4.4/5 (1452 recenzije)
SentinelOne - 4.8/5 (1465 recenzija)
Wazuh - 7.5/10

CrowdStrike Falcon

Prednosti	Mane
Napredna detekcija prijetnji u stvarnom vremenu	Viša cijena u odnosu na konkurenciju
Nativna cloud arhitektura s fleksibilnošću implementacije	Složenost u prilagodbi upozorenja i izvještaja
AI/ML tehnologija za detekciju i prevenciju prijetnji	Manje fleksibilan model licenciranja
Lagani agent s minimalnim utjecajem na performanse sustava	Zahtjeva internetsku vezu za optimalnu zaštitu
Odlična integracija s različitim sigurnosnim alatima	Strma krivulja učenja za potpuno iskorištavanje platforme
Napredne mogućnosti forenzike i lova na prijetnje	Visoki početni trošak implementacije

Wazuh

Prednosti	Mane
Besplatna open-source platforma	Zahtijeva tehničku stručnost za postavljanje i održavanje
Visoka prilagodljivost i fleksibilnost implementacije	Ograničena korisnička podrška u odnosu na komercijalna rješenja
Sveobuhvatna analiza logova i detekcija sigurnosnih događaja	Nedostatna dokumentacija za rješavanje problema
Dobra integracija s raznim sigurnosnim alatima	Složeni proces integracije za različite sustave
Podržava Windows, Linux i ostale platforme	Može se boriti s velikim količinama podataka
Mogućnost napredne prilagodbe za specifične sigurnosne potrebe	Duže vrijeme odgovora korisničke podrške

SentinelOne

Prednosti	Mane
Autonomni AI agent koji djeluje lokalno na svakom krajnjem uređaju	Viši troškovi implementacije u odnosu na neka rješenja
Mogućnost rollback-a nakon ransomware napada	Korisničko sučelje može biti intuitivnije
Radi offline bez potrebe za stalnom vezom s oblakom	Proces ažuriranja ponekad stvara probleme
Automatizirano otkrivanje i ublažavanje prijetnji	Ograničena granularnost upozorenja
Jednostavnije upravljanje i manje potrebe za SOC timom	Visoke cijene za napredne značajke
Dobra podrška za cloud, hibridne i lokalne okoline	Problemi s podrškom za integraciju

Microsoft Defender XDR

Prednosti	Mane
Besprijekorna integracija s Microsoft proizvodima	Ograničene integracije s alatima trećih strana
Cjenovno pristupačniji uz Microsoft 365 pretplatu	Složen proces početnog postavljanja
Automatizacija odgovora na incidente	Visoka potrošnja sistemskih resursa
Objedinjeno sigurnosno iskustvo unutar Microsoft ekosustava	Nedovoljno prilagodbe za specifične industrijske zahtjeve

Prednosti	Mane
Jednostavna implementacija za postojeće Microsoft korisnike	Složena struktura licenciranja
Poboljšava sigurnosni položaj uz minimalno dodatno ulaganje	Manje naprednih značajki u odnosu na specijalizirane alate

Usporedba po veličini poduzeća

- **Mala poduzeća**: Microsoft Defender XDR i Wazuh su često izbor zbog pristupačnosti. Microsoft za postojeće korisnike Microsoft usluga, Wazuh za tehnički potkovane timove s ograničenim budžetom.
- **Srednja poduzeća**: SentinelOne nudi dobar balans između cijene i naprednih značajki.
- **Velika poduzeća**: CrowdStrike Falcon je najčešći izbor zbog naprednih mogućnosti, iako uz veću cijenu.

Zaključak

CrowdStrike Falcon predstavlja premium rješenje s najboljim mogućnostima detekcije i odgovora na prijetnje, ali uz najvišu cijenu. SentinelOne nudi konkurentne značajke s fokusom na autonomnu zaštitu i jednostavnije upravljanje. Microsoft Defender XDR pruža dobru vrijednost za postojeće Microsoft korisnike uz sve bolju integraciju. Wazuh je najbolji izbor za organizacije s tehničkim znanjem koje traže besplatno, prilagodljivo rješenje.

Izbor rješenja ovisi o veličini organizacije, proračunu, tehničkoj stručnosti tima i postojećoj infrastrukturi. Najvažnije značajke koje treba razmotriti su: mogućnosti detekcije, jednostavnost upravljanja, integracija s postojećim alatima i ukupni trošak vlasništva.

Usporedba 2

#seminar2 Obrađeno: https://www.g2.com/compare/palo-alto-networks-cortex-xdr-vs-wazuh-the-open-source-security-platform-vs-vectra-ai-platform-vs-darktrace-detect
Autor: G2
Pristupljeno: 16.5.2025

TL;DR Usporedba Palo Alto Networks Cortex XDR, Wazuh, Vectra AI Platform i Darktrace Detect sigurnosnih rješenja za otkrivanje i odgovor na prijetnje.

Udio na tržištu (XDR kategorija)

Palo Alto Cortex XDR - 5.6%
Wazuh - 13.0%
Vectra AI - nije specificirano
Darktrace Detect - 19.5% (prema podacima iz ranije usporedbe)

Cortex XDR by Palo Alto Networks

Prednosti	Mane
Robustna integracija podataka kroz različite sigurnosne slojeve	Kompleksna implementacija koja zahtijeva tehničku stručnost
Napredna analitika za otkrivanje prijetnji	Visoka cijena za male i srednje organizacije
Automatizirani odgovor na incidente	Potrebno poboljšanje funkcionalnosti izvještavanja
Sveobuhvatna pokrivenost krajnjih točaka, mreže i oblaka	Integracija s alatima trećih strana može biti izazovna
Proaktivna detekcija prijetnji	Korisničko sučelje ponekad može biti nepregledno
Snažna korelacija sigurnosnih događaja za bolju analizu	Visoka potrošnja resursa na nekim sustavima

Wazuh

Prednosti	Mane
Besplatna open-source platforma	Zahtijeva značajnu tehničku stručnost za implementaciju
Visoka prilagodljivost i fleksibilnost	Ograničena profesionalna podrška u odnosu na komercijalna rješenja
Sveobuhvatna analiza logova	Nedostatna dokumentacija za rješavanje složenih problema
Dobra integracija s različitim sigurnosnim alatima	Kompleksni proces implementacije za heterogene sustave
Podrška za različite platforme (Windows, Linux, macOS)	Može se boriti s masovnim količinama podataka
Snažna zajednica korisnika i razvojnih inženjera	Korisničko sučelje za upravljanje može biti intuitivnije

Vectra AI Platform

Prednosti	Mane
Izvrsno ocjenjivanje rizika za bolje određivanje prioriteta	Ograničena vidljivost prijetnji na razini domaćina
AI-detekcija omogućuje brže i učinkovitije reagiranje	Zahtijeva integraciju sa SIEM rješenjima za potpunu funkcionalnost
Kvalitetna integracija s Microsoft okruženjem	Logovi za SIEM su često preminimalni

Prednosti	Mane
Povezivanje prijetnji s uređajima za bolju analizu napada	Ograničene mogućnosti prilagodbe
Smanjuje zamor od upozorenja kroz preciznu detekciju	Ovisnost o mrežnoj detekciji za prepoznavanje prijetnji
Stabilan rad s minimalnim potrebama za održavanjem	Podešavanje lažno pozitivnih rezultata je izazovno

Darktrace Detect

Prednosti	Mane
Stabilan rad s minimalnim prekidima	Visoka cijena, model naplate se može poboljšati
Informativna upozorenja s minimalnim šumom	Ograničena vidljivost i zaštita krajnjih točaka
AI analitika i strojno učenje za otkrivanje anomalija	Veliki broj lažno pozitivnih rezultata u početnim fazama
"Antigena" funkcionalnost za trenutne automatizirane odgovore	Manjkava integracija s drugim sigurnosnim alatima
Izvrsno nadgledanje mreže i emaila	Dokumentacija i korisnička podrška mogu biti bolji
Samoučeći sustav koji se prilagođava okolini	Zahtijeva značajno ručno podešavanje za optimalne rezultate

Usporedba kvalitete podrške i jednostavnosti korištenja

- **Cortex XDR**: Kvalitetna podrška, ali složen za implementaciju i korištenje za manje iskusne timove
- **Wazuh**: Ograničena formalna podrška, oslanja se na zajednicu; zahtijeva tehničku stručnost
- **Vectra AI**: Dobra podrška koja varira ovisno o dodijeljenom inženjeru; srednje složenosti za korištenje
- **Darktrace**: Prosječna podrška; relativno jednostavan za postavljanje ali izazovan za fino podešavanje

Usporedba po veličini poduzeća

- **Mala poduzeća**: Wazuh je najbolji izbor za tehnički potkovane timove s ograničenim budžetom
- **Srednja poduzeća**: Vectra AI i Darktrace nude dobar balans između mogućnosti i cijene
- **Velika poduzeća**: Cortex XDR pruža najkompletniji set značajki za složene sigurnosne potrebe velikih organizacija

Zaključak

- Palo Alto Networks Cortex XDR predstavlja premium rješenje s najnaprednijim mogućnostima integracije i analize različitih sigurnosnih slojeva, ali uz visoku cijenu i kompleksnost
- Darktrace Detect dominira na tržištu sa svojim samoučećim AI pristupom koji odlično otkriva anomalije, iako uz ograničenu zaštitu krajnjih točaka
- Vectra AI pruža odličan balans između AI-vođene detekcije i jednostavnosti, posebice za organizacije koje koriste Microsoft okruženje
- Wazuh nudi iznimnu vrijednost kao besplatno, otvoreno rješenje, ali zahtijeva značajnu tehničku stručnost za implementaciju i održavanje

Izbor platforme prvenstveno ovisi o veličini organizacije, tehničkim mogućnostima sigurnosnog tima, specifičnim sigurnosnim potrebama i dostupnom budžetu. Organizacije s manjim tehničkim timovima bi trebale razmotriti komercijalna rješenja poput Darktrace ili Vectra AI zbog jednostavnije implementacije, dok tehnički potkovani timovi mogu iskoristiti fleksibilnost i ekonomičnost Wazuha.