Tjedan 7.4. - 11.4.

Obrađeno: https://www.peerspot.com/products/comparisons/cisco-sourcefire-snort_vs_darktrace_vs_vectra-ai
Autor: PeerSpot
Pristupljeno: 9.4.2025

Usporedba Snort, Darktrace i Vectra AI alata

Udio pojedinog alata u IDPS (*Intrusion Detection and Prevention Software*) tržištu:
Darktrace - 19.5%
Vectra AI - 11.3%
Snort - 3.3%

Snort

Prednosti	**Mane**
Jednostavno skaliranje za veće radne okoline	Integracija sa ostalim alatima (uključujući i Ciscove alate)
Tehnička podrška je izuzetno korisna	Cijena
Jako dobra usluga filtriranja prometa i URL-ova kao i zaštita od *malware*-a	Uređivanje pravila se može pojednostaviti
Detekcija prijetnji izuzetno dobra (malo FP-a)	Performanse se mogu poboljšati i alarmi mogu biti informativniji
Jednostavan za konfiguraciju i *deployment*	Početno postavljanje može biti kompliciranо za razliku od sličnih proizvoda (ovisi o okruženju)

Izvor: https://www.peerspot.com/products/cisco-sourcefire-snort-pros-and-cons#pro-aspect-container

Darktrace

Prednosti	Mane
Stabilan, nema skoro nikakvog *downtime*-a	Jako skup, model naplate se može poboljšati
Alarmi izuzetno informativni, minimalan šum	Manjka u mogućnostima vidljivosti i zaštite krajnjih točaka, fokusira se više na mrežnu detekciju
AI analitika i strojno učenje nude efektivno uočavanje i sprječavanje prijetnji	Izbacuje puno FP-a, zahtjeva puno ručnog konfiguriranja i razumijevanja pri čitanju logova
Antigena nudi instantne odgovore na prijetnje (automatiziran TH)	Manjkava integracija i automatizacija sa ostalim alatima
Mrežno i email nadgledanje posebice dobri	Dokumentacija i korisnička podrška mogu biti bolji

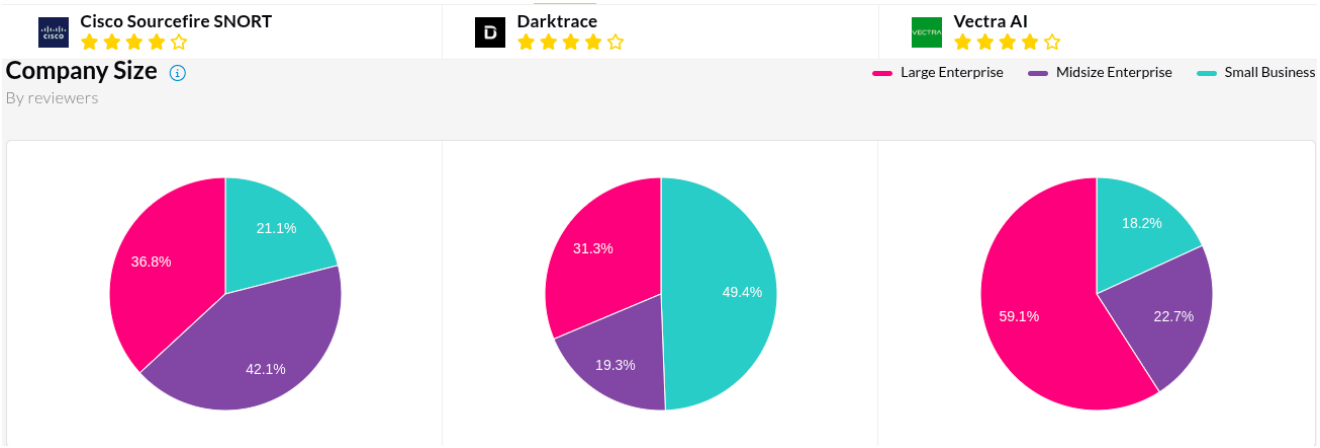
Izvor: https://www.peerspot.com/products/darktrace-pros-and-cons#pro-aspect-container

Vectra AI

Prednosti	Mane
Daje ocjene rizika za bolje prioritete i manji zamor od upozorenja	Zahtjeva integraciju sa SIEM kako nedovoljno umanjuje SA količinu posla
AI detekcija omogućuje brže i učinkovitije reagiranje	Logovi koje šalje SIEM-u su previše minimalni
Integracija s Microsoftom poboljšava vidljivost prijetnji i olakšava rad	Kako je temeljena na mreži ne daje potpunu vidljivost na prijetnje i aktivnosti na domaćinu
Povezuje prijetnje s uređajima za bolju analizu napada	Ograničene mogućnosti prilagodbe
Cognito Streams detaljan pregled mreže i lakša detekcija problema	Namještanje FP-a je teško

Izvor: https://www.peerspot.com/products/vectra-ai-pros-and-cons#pro-aspect-container

Usporedba



Ovdje možemo vidjeti po veličini kako koje poduzeće po veličini preferira koji alat

Mala poduzeća
Preferiraju: **Darktrace**
Darktrace malim podutzećima nudi odličnu i potpunu zaštitu uz relativno pristojnu cijenu

Srednja poduzeća
Preferiraju: **Cisco SNORT**
Snort je zlatna sredina što se tiče cijene i usluge. 24/7, dobro obučena korisnička potpora im također ide u korist.

Velika poduzeća
Preferiraju: **Vectra AI**
Vectra ima transparentan cjenik i servis koji dobro pronalazi bilo kakve greške i nekonzistentnosti uz minimalnu informacijsku redundanciju što odgovara velikim poduzećima.

Zaključak

- Darktrace dominira na IDPS tržištu s udjelom od 19.5%, slijedi Vectra AI s 11.3%, dok Snort ima samo 3.3% tržišta
- Svaki alat ima svoju ciljanu skupinu korisnika:
  - Mala poduzeća preferiraju Darktrace zbog odlične zaštite uz pristojnu cijenu
  - Srednja poduzeća biraju Snort kao zlatnu sredinu po pitanju cijene i usluge, uz dobru korisničku podršku
  - Velika poduzeća se odlučuju za Vectra AI zbog transparentnog cjenika i učinkovitog pronalaženja grešaka uz minimalnu

redundanciju

- Ključne prednosti Snorta: jednostavno skaliranje, dobra tehnička podrška, kvalitetno filtriranje prometa i detekcija prijetnji
- Ključne prednosti Darktrace-a: stabilnost, informativni alarmi, snažna AI analitika i automatiziran odgovor na prijetnje
- Ključne prednosti Vectra AI: dobro ocjenjivanje rizika, učinkovita AI detekcija, kvalitetna integracija s Microsoftom
- Glavni nedostaci Snorta: problematična integracija s drugim alatima, cijena i kompliciranо početno postavljanje
- Glavni nedostaci Darktrace-a: visoka cijena, ograničena zaštita krajnjih točaka, brojni lažno pozitivni rezultati
- Glavni nedostaci Vectra AI: potreba za integracijom sa SIEM-om, minimalni logovi, ograničena vidljivost prijetnji na razini domaćina