FortiAnalyzer

Komplexná platforma na analýzu bezpečnosti siete

O2 Business Services, a.s.

28.5.2024

- Úvod
- Funkcie
  - Pokročilá analytika a korelácia
  - Centralizované logovanie a ukladanie logov
  - Dodržiavanie predpisov a audit
  - Automatizácia a orchestrácia
- Zhrnutie

Úvod

Centralizované logovanie, reporty a analýza

- Poskytuje zaznamenávania a analýzu sieťových udalostí a bezpečnostných incidentov
- Umožňuje firme získať prehľad o sieťových aktivitách
- Identifikuje hrozby, optimalizuje výkon siete a zásady bezpečnosti

Zhromažďuje a ukladá logy z rôznych Fortinet a aj iných zariadení

- Podporuje vyše 300 logovacích formátov
- Dokáže spracovať až 100.000 logov za sekundu

FortiAnalyzer je integrovaný s FortiGate, FortiManager a FortiCloud

- Tým poskytuje unifikovaný management logov a ich analýzu pre rodinu Fortinet produktov

Popis produktu

- Pokročilá analytika a korelácia
- Využíva AI a strojové učenia na analýzu a koreláciu logov
- Deteguje anomálie a generuje alerty a reporty
- Vykonáva analýzu základných príčin (root cause analysis)
- Forenzné vyšetrovanie a vyhľadávanie hrozieb
- Používa výkonný dotazovací mechanizmus a vizualizačné nástroje

Technické vlastnosti

- Dodržiava regulačné a priemyselné normy
  - PCI DSS, HIPAA, GDPR, NIST, ISO
- Preddefinované a prispôsobiteľné reporty a dashboardy
- Pokrýva rôzne oblasti a požiadavky na súlad
- Vytvára auditné záznamy a dôkazy pre kontrolné audity

Automatizácia a orchestrácia

- Automatizuje a orchestruje úlohy pre bezpečnosť siete
- Zhromažďuje logy, robí analýzy a reporty
- Posiela výstrahy a návrhy na riešenia
- Integrácia s inými riešeniami spoločnosti Fortinet
  - FortiSOAR, FortiSIEM, FortiEDR a FortiSandbox
- Poskytuje komplexnú platformu pre bezpečnostné operačné centrum (SOC – Security Operations Center)

Ďalšie vlastnosti

- Možnosť inštalácie on-site v priestoroch spoločnosti, alebo v dátovom centre
- Ukladá logy v rôznych formátoch, napríklad syslog, SNMP, IPFIX a JSON
- Podporuje šifrovanie údajov, kompresiu a retenčné politiky