Security Operations Center

Moderný prístup k riadeniu kybernetickej bezpečnosti

Andrej Ižold

Systems Engineer

Aktuálne výzvy

Rozširujúce sa prostredie hrozieb

- Multi-Vendor
- On-premise a Cloud
- Home Office
- Komplexnejšie útoky

Nedostatočná viditeľnosť

- Pochopenie IT aktív
- Nedostatok ľudí
- Množstvo konzol

Súlad s predpismi

- Regulačné
- Interné
- Osvedčené postupy

Prečo tradičný SOC prestáva stačiť

Chaos

- Priveľa alertov, málo kontextu
- Priveľa konzol
- Manuálna triáž
- Reakcia cez email a ticket
- Chybovosť
- Reaktívny prístup

Moderný SOC

Jednotný

- Jeden pohľad na všetky bezpečnostné udalosti
- Menej konzol, viac kontextu
- Jedna pravda pre rozhodovanie

AI-driven

- Alerty s prioritou a koreláciou.
- Automatizované triedenie
- AI pomáha analytikovi rozhodovať rýchlejšie
- Agentic AI

Automatizovaný

- Detekcia bez reakcie nestačí
- Incident spúšťa automatickú reakciu
- Automatizácia zrýchľuje bez straty kontroly

Nástroje moderného SOC

SecOps

FortiSOC

FortiSOAR

Incident Management

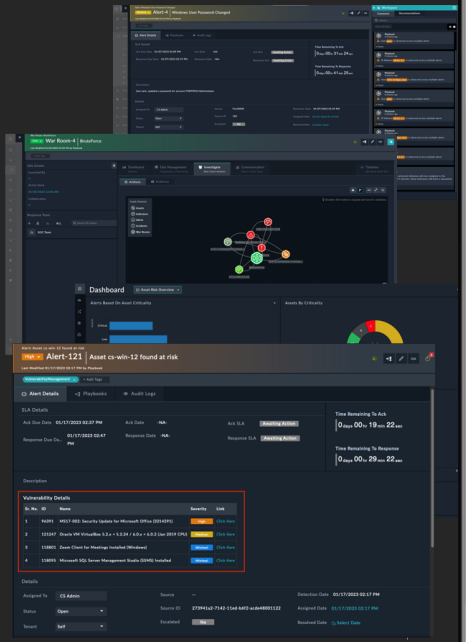
- Automaticky spracováva upozornenia
- Prešetruje incidenty a reaguje na ne
- Využíva umelú inteligenciu a automatizáciu v každom kroku

Asset Visibility & Risk Management

- Zobrazenie a sledovanie inventára IT/OT aktív a kompletný stav zabezpečenia aktív
- Obohatenie a stanovenie priorít aktivít

Vulnerability Management

- Centralizácia a automatizácia správy zraniteľností IT/OT
- Urýchlenie vyšetrovania hrozieb pomocou integrovanej analýzy zraniteľností

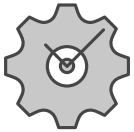


SOCaaS workflow

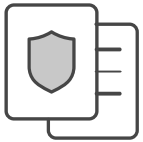
FortiSOAR incident

SOAR mení alert na riadený incident

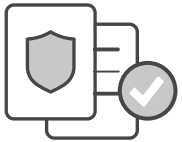
SOC Analytik



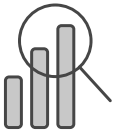
Automatické spracovanie emailu



Extrahovanie indikátorov a vytvorenie alertu



Analýza, korelácia a rozhodnutie



Reakcia a automatizovaná mitigácia

Pred incidentom → **Počas incidentu** → **Po incidente**

Ktorá cesta dáva zákazníkovi zmysel

Potrebujem automatizovať

- Mám ľudí aj procesy, ale reakcia je ešte stále príliš manuálna.

→ **FortiSOAR**

Potrebujem moderný dohľad

- Chcem zjednotený cloudový SOC model bez budovania veľkej architektúry

→ **FortiSOC**

Potrebujem výsledok

- Nemám kapacitu na 24/7 interný tím, ale potrebujem monitoring a eskaláciu incidentov.

→ **FortiSOCaaS**

Ďakujem za pozornosť


FORTINET®