ACCURA
Industrial & Information Cybersecurity

OT Security Operation Center

Spoločnosť Accura poskytuje Centrum Cybernetickej Obrany (CDO), známe tiež ako Centrum bezpečnostných operácií (SOC), kde dohľadujeme industriálnu prevádzku pomocou osvedčených princípov postavenej na špičkovej technológii, ktorá rozumie priemyselným prostrediam.

PROAKTÍVNY PRIEMYSELNÝ MONITORING HROZIEB

Priemyselné siete spájajú digitálny svet s fyzickým a predstavujú tak kritické ciele. OT prostredia často pozostávajú zo starších a citlivých systémov, ktoré nie sú dostatočne chránené bezpečnostnými opatreniami. Konvergenciou IT a OT systémov a nasadzovaním IIoT vznikajú nové vektory pre útočníkov zvonka ako i zvnútra.

Accura pomáha spoločnostiam chrániť IT aj OT systémy bez zasahovania do industriálnych procesov. OT Security Monitoring umožňuje neinvazívny monitoring sieťovej prevádzky. To umožňuje lepšie pochopenie a hlbší prehľad o základných procesoch a celkovo vedie k väčšej bezpečnosti vašich kritických priemyselných aktív.

KĽÚČOVÉ VLASTNOSTI A SLUŽBY OT SOC

✓	• Analýza správania privilégovaných príkazov (integrity alerts) • Analýza anomálií a detekcia hrozieb (zero days) • Detekcia hrozieb na základe signatúr (známe hrozby) • Vizualizácia zariadení a ich prepojení v reálnom čase na základe Purdue Modelu
✓	• Nepretržité a pasívne skenovanie zariadení + Safe Active Query • Automatický výpočet vektora útoku do OT siete • Prehľad o rizikách a hrozbách v reálnom čase • Detekcia a extrahovanie informácií z rôznych priemyselných protokolov (150+)
✓	• Pasívna správa zraniteľnosti (PLC, RTU, IED, DCS atď.) • OT honeypot na chytanie útočníkov • Automatické oznamovanie incidentov • Detailná vizualizácia zariadení a zozbierané poznatky pre forenznú analýzu

VÝHODY OT SOC

- **Včasné monitorovanie bezpečnosti:** Monitorovanie prostredí OT v reálnom čase umožňuje včasnú detekciu hrozieb, čo pomáha predchádzať nákladným prestojom a udržiavať prevádzkovú integritu.
- **Spravodajstvo o hrozbách:** OT SOC využíva informácie o hrozbách IT aj OT a poskytuje prehľad o jedinečných hrozbách zameraných na priemyselné systémy, ako je napríklad industrial ransomvér prispôsobený pre OT prostredia.

- **Nepretržité riadenie zraniteľnosti:** OT SOC identifikuje zraniteľnosti a zmierňuje riziká, pretože staršie systémy sú zraniteľné voči kybernetickým útokom.
- **Zníženie prevádzkových prestojov:** Preventívnym riešením problémov a rýchlou reakciou na hrozby OT SOC minimalizuje HSE incidenty a maximalizuje dobu prevádzkyschopnosti kritických ICS / DCS systémov.

- **Súlad s legislatívou:** Od mnohých priemyselných odvetví sa vyžaduje dodržiavanie prísnych regulačných noriem ako ZKB 69/2018, NIS2, IEC 62443, NIST 800-82 atď.

Karpatské námestie 7770/10A | 831 06 Bratislava | accura@accura.io| www.accura.io