SOC AKO SLUŽBA

Chráňte svoje IT a OT prostredie s istotou, že vašu infraštruktúru monitoruje tím certifikovaných expertov 24 hodín denne, 7 dní v týždni, počas celého roka.

Vo void SOC bojujeme proti kybernetickým hrozbám. Naše špecializované stredisko kybernetickej bezpečnosti (SOC) monitoruje, analyzuje a reaguje na incidenty v reálnom čase - aby útoky, prieniky či pokusy o zneužitie vašich systémov boli zastavené skôr, než spôsobia škodu.

PREČO VOID SOC?

Kybernetické útoky sú dnes rýchlejšie, sofistikovanejšie a častejšie než kedykoľvek predtým. Úspešná obrana vyžaduje technológie, procesy a ľudí, ktorí dokážu reagovať okamžite. Náš **SOC ako služba** spája všetky tieto prvky do jedného bezpečnostného ekosystému:

- 24/7 — nepretržité 24/7 monitorovanie vašej infraštruktúry
- odborná analýza a koordinácia pri incidentoch
- včasná detekcia a reakcia na hrozby
- podpora pri obnove systémov a prevencii opakovaných útokov

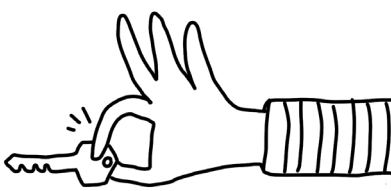
AKO SOC SLUŽBA FUNGUJE

Neustály dohľad nad vašou bezpečnosťou

Zariadenia umiestnené vo vašej sieti zhromažďujú bezpečnostne relevantné údaje (logy, udalosti, sieťovú komunikáciu) a prenášajú ich cez šifrovaný kanál do technologického klastra void SOC.
Naše systémy tieto údaje normalizujú, obohacujú a analyzujú v reálnom čase - aby sme dokázali identifikovať podozrivé aktivity okamžite po ich vzniku.

Detekcia a overenie incidentov

Pomocou pokročilých analytických nástrojov a skúseností našich špecialistov dokážeme odhaliť aj skryté alebo dlhodobé útoky. Každý incident overuje náš bezpečnostný analytik - eliminujú sa falošné poplachy (tzv. false positive) a vy dostávate len relevantné a presne vyhodnotené informácie.

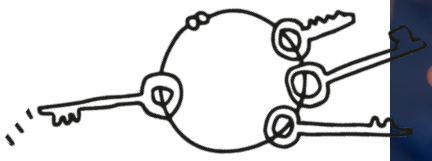


Rýchla reakcia a odborná podpora

Pri potvrdení skutočného incidentu naši experti:
• okamžite informujú váš IT tím podľa dohodnutej komunikačnej matice,
• poskytujú presné odporúčania pre riešenie,
• pomáhajú s izoláciou, zmiernením a odstránením dopadov útoku.
V prípade kritických situácií preberáme koordinačnú úlohu - riadime reakciu naprieč tímami, zabezpečujeme komunikáciu a dohliadame na obnovu systémov.

Obnova a prevencia

Po incidente vám pomôžeme s obnovou dát, auditom zraniteľností a implementáciou opatrení, ktoré zabránia opakovaniu rovnakého typu útoku.
Cieľom nie je len reagovať - ale posilniť celkovú odolnosť vašej organizácie voči budúcim hrozbám.



AKO SOC SLUŽBA FUNGUJE

Ako void SOC poskytujeme služby z dvoch geograficky nezávislých a bezpečne oddelených lokalít:

• Bratislava (EÚ) - pre klientov v rámci Európskej únie,
• Istanbul (Turecko) - pre klientov mimo EÚ.

Každé stredisko má vlastné technologické zázemie v dátovom centre s certifikáciou PCI DSS a - pre EÚ lokalitu - aj NATO certifikáciu pre spracovanie utajovaných skutočností do úrovne „Tajné".

Zároveň garantujeme, že dáta klientov z EÚ nikdy neopúšťajú územie Európskej únie. Naše dátové centrá sú odolné voči prírodným katastrofám a výpadkom, pričom celkové riešenie void SOC dosahuje garantovanú dostupnosť 99,8 %.

ĽUDIA, KTORÍ STOJA ZA OCHRANOU VAŠICH DÁT

Za službou SOC ako služba stojí tím viac ako 100 odborníkov v rámci Soitron Group, ktorí dodávajú bezpečnostné služby v siedmich európskych krajinách.
V samotnom bratislavskom SOC-u pôsobí vyše 15 špecializovaných analytikov a operátorov, držiteľov renomovaných certifikácií ako:

• CEH Master / CEH
• CHFI - Computer Hacking Forensic Investigator
• CySA+ - Cybersecurity Analyst
• CISSP - Certified Information Systems Security Professional
• CCIE - Cisco Certified Internetwork Expert
• MCSE - Microsoft Certified Systems Engineer
• Bezpečnostné previerky NBÚ SR/ČR - úroveň II (Dôverné)

Naši odborníci kombinujú praktické skúsenosti z reálnych incidentov s najmodernejšími technológiami, aby vaša organizácia bola vždy o krok pred útočníkmi.

SOC PRE PRIEMYSELNÉ SIETE (OT)

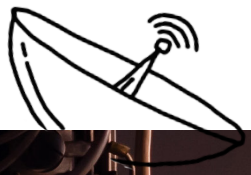
Kybernetická bezpečnosť už dávno nie je len o IT. Vo void SOC preto poskytujeme špecializované služby aj pre OT (Operational Technology) a priemyselné prostredia, kde výpadok systémov znamená nielen finančné, ale aj prevádzkové riziko.
V spolupráci so systémom Cisco Cyber Vision, doplnené o riešenie ako Claroty, Nozomi, Armis či Gerycortex dokážeme monitorovať a chrániť výrobné technológie, SCADA systémy a ďalšie prevádzkové siete. Zároveň vyvíjame vlastný nástroj SOCulus_OT, podporovaný Európskym kompetenčným centrom pre kybernetickú bezpečnosť v rámci programu Digital Europe. Naším cieľom je priniesť lokálne vyvinuté riešenie pre detekciu hrozieb v priemyselných sieťach, optimalizované pre potreby slovenských a českých výrobných podnikov.

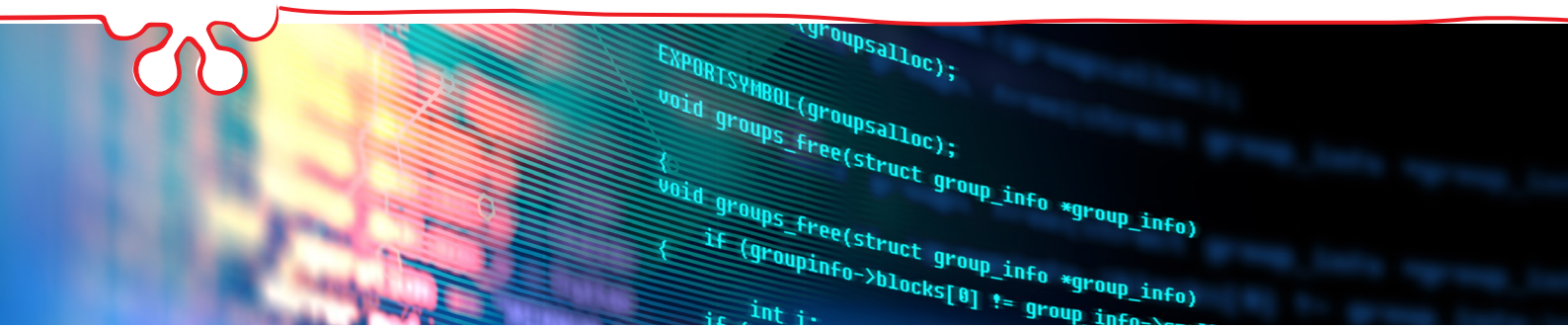
CISCO CYBER VISION AKO CENTRÁLNY NÁSTROJ MONITORINGU

Cisco Cyber Vision umiestnený vo vašej infraštruktúre je špeciálne navrhnutý pre priemyselné organizácie a kritickú infraštruktúru. Poskytuje chranu OT prostredí, znižuje riziko útokov, zabraňuje šíreniu hrozieb, zabezpečuje vzdialený prístup a rozširuje IT bezpečnosť do priemyselných sietí.

Cisco Cyber Vision poskytuje:

- reálnu viditeľnosť OT aktív, ich automatickú inventarizáciu , sledovanie zraniteľností, vzorcov komunikácie, anomálií. Deteguje škodlivú prevádzku a upozorňuje na zraniteľnosti
- segmentáciu siete pre bezpečné oddelenie OT prostredí zero Trust vzdialený prístup - bezpečný prístup pre tímy a dodávateľov s politikou minimálnych oprávnení (MFA, SSO, časové obmedzenia)
- využitie senzorov zabudovaných v sieťových zariadeniach - bez potreby samostatných zariadení, aktiváciou funkcie v Cisco switchoch a routeroch
- flexibilné nasadenie v brownfield prostrediach cez podporu Docker a hardvérových senzorov
- detailnú viditeľnosť aj na najnižších úrovniach Purdue modelu

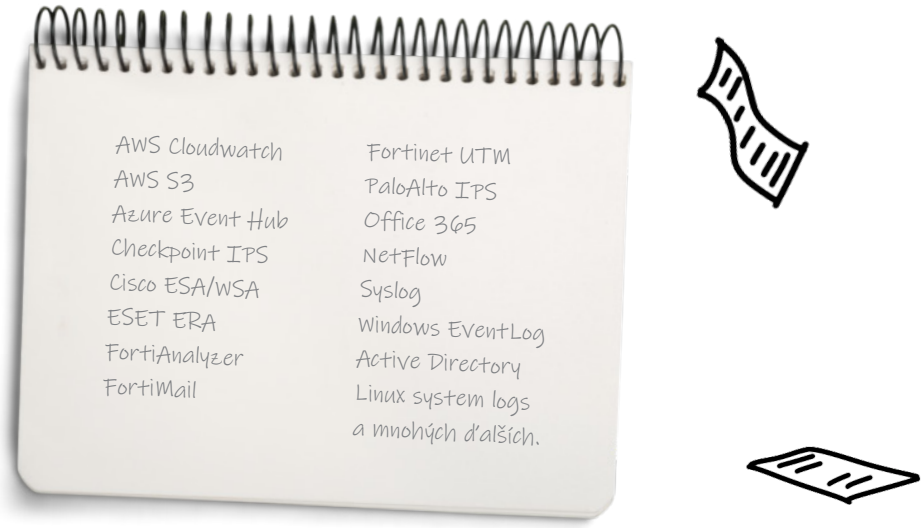




PODPOROVANÉ TECHNOLÓGIE A ZDROJE DÁT

Vo void SOC spracúvame široké spektrum bezpečnostných dát z IT aj cloudových prostredí, vrátane:

Vďaka flexibilným konektorom dokážeme integrovať aj vaše vlastné alebo menej štandardné systémy - bez obmedzenia platformy či výrobcu.



KĽÚČOVÉ PRÍNOSY VOID SOC

Nonstop ochrana 24/7
nepretržitý dohľad nad všetkými systémami, zariadeniami a sieťami

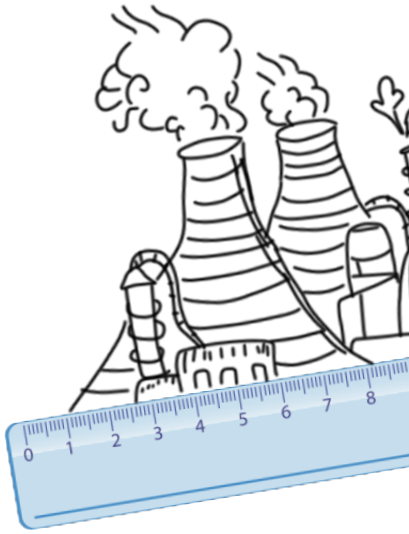
Bezpečné dátové centrá v EÚ aj mimo EÚ
oddelené prostredia, žiadne zdieľanie dá

Rýchla detekcia a reakcia
skracujeme čas od zistenia po riešenie (MTTD/MTTR)

IT & OT
Plná podpora IT aj OT infraštruktúr

Skúsení certifikovaní experti
sme váš bezpečnostný tím na diaľku

Dostupnosť služby
Vysoká dostupnosť služby (SLA 99,8 %)



SOITRON, člen skupiny SOITRON Group

Spoločnosť Soitron je stredoeurópsky integrátor, ktorý pôsobí na IT trhu od roku 1991. Filozofiou spoločnosti je snaha neustále napredovať, a aj preto je lídrom v zavádzaní unikátnych technológií a inovatívnych riešení. Svojim klientom ponúka produkty a služby v oblasti sieťových a komunikačných riešení, kybernetickej bezpečnosť, dátových centier, IT outsourcingu, IT supportu a poradenstva. Do portfólia spoločnosti patrí aj riešenie pre inteligentné policajné autá - Mosy a služby dohľadového centra kybernetickej bezpečnosti - void SOC (Security Operations Center).
Soitron je členom skupiny Soitron Group, v ktorej pracuje viac ako 850 medzinárodných odborníkov. Skupina združuje profesionálne tímy na Slovensku, v Českej republike, Rumunsku, Turecku, Bulharsku, Poľsku a Veľkej Británii.