



Slovakia

Viac hodnoty.
Viac dôvery.

IT-OT SOC - Security Operations Center

Chráňte sa pred kyber útokmi.

Prvý Priemyselný IT-OT SOC na Slovensku

SOC (Security Operations Center) je centralizovaná funkcia v organizácii, ktorá integruje ľudí, procesy a technológie na nepretržité sledovanie a zlepšovanie bezpečnostného zabezpečenia organizácie pri predchádzaní, odhaľovaní, analýze a reakcii na kybernetické bezpečnostné incidenty.

Čo ponúka IT-OT SOC spoločnosti TÜV SÜD?

Služba IT-OT SOC od spoločnosti TÜV SÜD zásadným spôsobom zvyšuje efektívnosť, účinnosť a konzistenciu zabezpečovacej prevádzky spoločnosti. SOC IT-OT nepretržite monitoruje produkčné prostredie, preventívne skenuje medzery v digitálnom zabezpečení a zdôrazňuje a uprednostňuje uplatniteľné opatrenia na zníženie rizika podľa ich potenciálnych obchodných dopadov.

Ako priemyselne zameraný SOC má osobitnú úlohu pri udržiavaní bezpečnosti, spoľahlivosti a produktivity prevádzkových procesov. Organizuje a automatizuje správu informácií o hrozbách, monitorovanie bezpečnostných udalostí a procesy reakcie na incidenty.

Prevádzkové režimy TÜV SÜD OT SOC

OT SOC od TÜV SÜD je možné implementovať ako samostatný OT SOC alebo integrovaný s IT SOC a SIEM (Security Information and Event Management). Umožňuje flexibilnú prevádzku s rôznymi operačnými režimami. Pre riadenie na diaľku je vzdialené pripojenie a prístup k SOC chránené unikátnym a zabezpečeným riešením spoločnosti TÜV SÜD.

Pre koho nevyhnutná služba SOC

Služba SOC je určená predovšetkým pre spoločnosti, ktoré sú povinné splniť zákonné požiadavky zákonom 69/2018 o kybernetickej bezpečnosti ale aj pre spoločnosti, ktoré si uvedomujú potrebu riadenia kybernetických hrozieb.

- Voda a atmosféra
- Energetika
- Zdravotníctvo
- Priemysel
- Digitálny infraštruktúra
- Doprava
- Prvky kritickej infraštruktúry

BASIC

- Základný monitoring v režime 8/5 (8 hodín x 5 dní služby),
- sledovanie bezpečnostných udalostí 8/5,
- klasifikácia a kategorizácia incidentov,
- tvorba a vedenie záznamov k incidentom,
- návrh základných mitigačných opatrení.

STANDARD

- Základný monitoring v režime 24/7 (24 hodín x 7 dní služby),
- sledovanie bezpečnostných udalostí 24/7,
- klasifikácia a kategorizácia incidentov,
- tvorba a vedenie záznamov k incidentom,
- analýza bezpečnostných incidentov,
- detailné mitigačné a preventívne opatrenia.

PREMIUM

- Monitoring 24/7
- prípady použitia na základe aktualizovaných dát,
- aktívna podpora zákazníka pri riešení incidentov a implementácií nápravných opatrení,
- služby bezpečnostného spravodajstva pre konkrétny sektor zákazníka,
- hĺbková analýza prostredia a infraštruktúry zákazníka v rámci "threat huntingu", odhaľovania APT hrozieb,
- forenzné analýzy.

Poskytované úrovne služieb

SOC poskytuje komplexné bezpečnostné služby podľa štandardného multi-tier modelu (3+), využívaného v IT svete u poskytovateľov expertných služieb. Voľba multi-tier modelu prináša flexibilitu v oblasti návrhu balíkov služieb (basic, standard, premium), takto je možné pristupovať k jednotlivým spoločnostiam individuálne a pokryť potreby riešenia aktívnej bezpečnosti pre firmy rôznych veľkostí. Implementácia jednotlivých projektov SOC je realizovaná v rámci štandardného projektového riadenia.

SLA parametre sa nastavujú podľa dobrej praxe v oblasti SOC služieb a zároveň tak, aby zákazníci SOC, ktorí sú regulovaní zákonom č. 69/2018 o kybernetickej bezpečnosti boli schopní naplniť požiadavky §20 ods. 4 pís. a) b) c). Zákon č. 69/2018 ani vyhláška 165/2018 neurčujú časové faktory pre bezpečnostné incidenty, určené sú iba identifikačné kritéria závažných kybernetických bezpečnostných incidentov a podrobnosti o ich hlásení NBÚ.

Prečo si vybrať TÜV SÜD?

Ako odborníci v oblasti bezpečnosti IT a ochrany údajov TÜV SÜD môže poskytovať služby IT a kybernetickej bezpečnosti podľa najvyšších štandardov. Naše špecializované interdisciplinárne tímy vám pomôžu identifikovať a vysporiadať sa s informačným a kybernetickým rizikom, vylepšiť zabezpečenie vašich IT systémov a aplikácií, minimalizovať riziko zneužitia firemných informácií a splniť požiadavky na ochranu údajov.

Viac hodnoty. Viac dôvery.

TÜV SÜD je poskytovateľ riešení prémiovej kvality, bezpečnosti a udržateľnosti, ktorý sa špecializuje na testovacie, inšpekčné, auditorské, certifikačné, školiace a znalostné služby. Zastúpenie máme na viac ako 1000 pobočkách po celom svete a sme držiteľmi akreditácií v Európe, Amerike, na Strednom východe, v Ázii a Afrike. Poskytovaním odborných riešení poskytujeme zákazníkovi, firmám, spotrebiteľom a životnému prostrediu hmatateľnú pridanú hodnotu.

Ďalšie služby

- GAP analýza kybernetickej bezpečnosti
- Audit kybernetickej bezpečnosti podľa 69/2018 Z.z.
- Penetračné testy
- Software Escrow
- GDPR audity
- Audit informačnej bezpečnosti podľa EN ISO 27001