



Senior SOC security mérnök



MVM Informatika Zrt.

Munkavégzés helye	Szerződés típusa	Szakterület	Napi munkaidő
Budapest	Határozatlan idejű	IT biztonságtechnika	Teljes munkaidőben

Az MVM Informatikai Zrt. IT Security Üzemeltetési Osztálya senior SOC security mérnököt keres, aki kulcsszerepet vállal a vállalat IT és – szükség esetén – OT környezetének kiberbiztonsági felügyeletében, a biztonsági események technikai elemzésében, valamint a SOC detektálási, monitoring- és reakcióképessegeinek folyamatos fejlesztésében.

Olyan tapasztalt, technikailag erős szakembert várunk, aki magabiztosan mozog SOC, incidenskezelési és biztonsági monitoring környezetben, képes detektálási szabályok és use case-ek kialakítására, a riasztások minőségének javítására, valamint a biztonsági rendszerek üzemeltetésének szakmai támogatására.

Feladatok

- Detektálási szabályok, use case-ek és korrelációs logikák tervezése, fejlesztése és dokumentálása SIEM/SOAR környezetben.
- SOC riasztások elemzése, hangolása, fals pozitív esetek csökkentése, prioritások és súlyossági szintek finomítása.
- SOAR-automatizmusok és incidenskezelési playbookok műszaki támogatása, tesztelése és folyamatos fejlesztése.
- Komplex biztonsági események technikai elemzésének támogatása, detektálási hiányosságok azonosítása és visszacsatolása a szabályrendszerbe.
- SOC platformok és biztonsági rendszerek – például SIEM, SOAR, EDR/NDR, naplógyűjtő és korrelációs komponensek – konfigurálása, karbantartása és fejlesztése.
- Új IT és releváns OT naplóforrások SOC felügyeletbe történő bevonása, loggyűjtés, normalizálás és adatminőség-ellenőrzés támogatása.
- Szakmai együttműködés SOC elemzőkkel, incidenskezelőkkel, IT üzemeltetési és alkalmazásgazdai területekkel, valamint tudásmegosztás és mentorálás támogatása.

Amit kérünk

- rendelkezni legalább 3 év IT-biztonsági, SOC vagy incidenskezelési tapasztalattal,
- felsőfokú informatikai, műszaki vagy információbiztonsági végzettséggel van,
- van gyakorlatod biztonsági események technikai elemzésében és kezelésében,
- magabiztosan használod angol nyelvet szakmai környezetben,
- precíz, elemző gondolkodású vagy, és nem riadsz meg komplex technikai kihívásoktól.

Miért jó nálunk dolgozni?

- versenyképes bér
- teljesítmény alapján prémium vagy bónusz
- folyamatos szakmai fejlődési lehetőségek (tréningek, konferenciák)
- széles körű béren kívüli juttatási csomag (cafeteria, egészségbiztosítás, kockázati balesetbiztosítás)
- üdülési, sportolási lehetőségek, rendezvények
- mobilitási támogatás
- kiemelkedő teljesítmény jutalmazása
- rugalmas munkaidő
- vállalati szabadidős és szakmai rendezvények

Előnyt jelent

Jelentkezés



-
- SIEM / SOAR / EDR rendszerek mélyebb ismerete, <https://mvm.karrierportal.hu/allashirdetes-jelentkezés/10981>
 - detektációs szabálytervezés vagy use case-fejlesztési tapasztalat,
 - OT-környezetekkel kapcsolatos alapismeretek.