



medior SOC security mérnök



MVM Informatika Zrt.

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

A medior SOC Security mérnök feladata a társaság informatikai és – szükség szerint – ipari (OT) környezetében felmerülő biztonsági események és incidensek technikai szintű elemzése, kezelése és mitigációjának támogatása, a SOC működéséhez kapcsolódó biztonsági detektálási, monitoring- és reagálási folyamatok aktív végrehajtása és fejlesztése.

A munkakör elsődleges célja az operatív kiberbiztonsági védekezési képességek fenntartása és erősítése, a biztonsági események gyors és szakszerű feldolgozásán, dokumentálásán és eskalációján keresztül, az érvényben lévő eljárásrendek szerint.

Feladatok

- Detektálási logikák, use case-ek és korrelációs szabályok , implementálása, karbantartása és dokumentálása. a senior szakértői iránymutatások alapján.
- Use case-ek kialakítása fenyegetési információk (CTI), incidens-tapasztalatok, audit- és üzemi visszajelzések alapján.
- Közreműködés a detektálási szabályrendszer kialakításában és karbantartásában.
- A SOC-ban keletkező riasztások elemzése és minőségértékelése a zaj-/érték arány javítása érdekében.
- Fals pozitív esetek okainak feltárása, szabály- és küszöbérték-módosítások elvégzése.
- Riasztási prioritások és súlyossági szintek finomhangolása az üzleti hatások figyelembevételével.
- SOAR automatizmusok és playbookok működésének támogatása.
- Automatizmusok tesztelése, és az észlelt hibák jelzése, dokumentálása.
- Közreműködés a szükséges korrekciók végrehajtásában
- Annak biztosítása, hogy az automatizált lépések ne veszélyeztessék az üzemi működést.
- A SOC működéséhez alkalmazott biztonsági rendszerek (különösen SIEM, SOAR, EDR/NDR, naplógyűjtő és korrelációs komponensek) konfigurációs és üzemeltetési feladatainak végrehajtása.
- Új funkciók és verziók tesztelésében, bevezetésében való közreműködés.
- A rendszerek integrációjának biztosítása más IT- és biztonsági megoldásokkal (naplóforrások, végpontvédelem, hálózati eszközök).

Amit kérünk

- rendelkezzel legalább 3 év IT biztonsági, SOC vagy incidenskezelési tapasztalattal,
- felsőfokú informatikai, műszaki vagy információbiztonsági végzettséged 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 (belső és külső tréningek, konferenciák)
- széles körű béren kívüli juttatási csomag (cafeteria, egészségbiztosítás, balesetbiztosítás, nyugdíj előtakarékosság)
- üdülési, sportolási lehetőségek, rendezvények
- mobilitási támogatás
- munkavégzéshez notebook, mobiltelefon használat biztosítása
- kiemelkedő teljesítmény jutalmazása
- rugalmas munkaidő
- vállalati szabadidős és szakmai rendezvények

Előnyt jelent

- SIEM / SOAR / EDR rendszerek mélyebb ismerete,
- detektációs szabálytervezés vagy use case fejlesztési tapasztalat,
- OT környezetekkel kapcsolatos alapismeretek.

Jelentkezés

<https://mvm.karrierportal.hu/allashirdetes-jelentkezés/11435>