HM EI
HM Elektronikai, Logisztikai és Vagyonkezelő Zártkörűen Működő Részvénytársaság

A HM Elektronikai, Logisztikai és Vagyonkezelő Zrt.

a magyar védelmi ipar vezető vállalataként minősített, egyedi informatikai fejlesztésekkel és üzemeltetéssel foglalkozó csapatába keres munkatársakat

• JUNIOR IT BIZTONSÁGI ESEMÉNYKEZELŐ •

munkakörbe

FŐ FELADATAI LESZNEK:

- LOG elemző munkatársként feladata lesz a SOC (Security Operations Center) IT biztonsági monitoring tevékenységének támogatása logelemzés és log management oldaláról
- IT biztonsági események azonosítása, felderítése, kivizsgálása, ezek alapján kockázatelhárító tevékenységek azonnali végrehajtása, kockázatcsökkentő javaslatok megtétele. Incidensekhez kapcsolódó biztonsági jelentések, elemzések, beszámolók készítése
- új logforrások bekötése, meglévő logforrások javítása, felülvizsgálata
- nem gyári kollektorok harmonizálása a SIEM rendszerhez, parszolási feladatok végrehajtása
- LOG menedzsmenttel kapcsolatos folyamatok kiértékelése és javítása
- SIEM rendszer adminisztrálása, monitorozása, szupporttal való feladatok menedzselése
- igény szerinti SIEM szabályok, kollerációk írása, meglévő szabályok felülvizsgálata, javaslattétel
- az alkalmazásokkal kapcsolatos lefejlesztett LOG minták véleményezése az elvárt IT biztonsági események tekintetében
- IT biztonsági incidensek kapcsán logelemzői támogatás nyújtása a SOC felkérései alapján
- LOG folyamatokkal kapcsolatos szakértői tanácsadás, valamint projektek ilyen jellegű támogatása

KOMPETENCIÁK:

- közép- vagy felsőfokú végzettség (informatikai, műszaki) Legalább 6 hónapos LOG management/LOG elemzés területen szerzett releváns információbiztonsági tapasztalat
- LOG gyűjtő és/vagy elemző rendszerek ismerete, logolással kapcsolatos folyamatok ismerete
- SYSLOG protokollok szakértő szintű ismerete
- CEF, JSON, XML formátumok és REGEXP mélyebb ismerete
- alap infrastruktúra által generált logok (OS, FW, DB) eseményeinek alap szintű ismerete
- hálózati szabványok, informatikai hálózatok ismerete (LAN, WLAN, VPN, tűzfal, DNS, NAT, DHCP, TCP/IP)
- kockázatkezelési és elemzési készség
- nyitottság a folyamatos fejlődésre, szakmai trendek követésére
- strukturált gondolkodás, problémamegoldó készség
- kiváló együttműködési képesség, csapatmunka
- megbízható, precíz munkavégzés

ELŐNYT JELENT:

- Security Operations Centerrel kapcsolatos 2 éves LOG elemzőként szerzett tapasztalat
- Linux/UNIX OS ismeret, programozási ismeretek, SYSLOG-NG ismerete
- QRadar/Resilient, Sentinel ismeretek
- információbiztonsági védelmi eszközök ismerete

MUNKAVÉGZÉS HELYE:

- Budapest

JELENTKEZZEN HOZZÁNK, MERT

- hosszú távú munkalehetőséget, határozatlan idejű munkaszerződést biztosítunk
- megbízható, stabil, nagyvállalati környezetben dolgozhat
- részt vehet kutatás-fejlesztési és projekt feladatokban
- egyedülálló szakmai kihívások várják
- munkaköri feladatokhoz kapcsolódó szakmai továbbképzéseken vehet részt
- béren kívüli juttatást, csoportos élet-, baleset- és egészségbiztosítást, valamint mobiltelefont biztosítunk
- lendületes csapattal, jó közösségben dolgozhat

Kérjük, hogy jelentkezésének elküldése előtt olvassa el az álláspályázatra jelentkezőknek szóló Adatkezelési tájékoztatót a HM EI Zrt. weboldalán.

Amennyiben hirdetésünk felkeltette érdeklődését, és szívesen lenne tagja egy stabil nagyvállalat csapatának, önéletrajzát juttassa el hozzánk az **allas@hmei.hu** e-mail címre.