SOC analytik

Miesto práce
Košice

Druh pracovného pomeru
plný úväzok

Termín nástupu
ASAP

Mzdové podmienky (brutto)
2 000 EUR/mesiac
Mzda - podľa rozsahu znalosti - od 2000,-€

Informácie o pracovnom mieste

Náplň práce, právomoci a zodpovednosti
- samostatné posudzovanie stavu bezpečnosti na základe podkladov z dostupných nástrojov
- analýza a riešenie incidentov v monitorovanom prostredí dostupnými nástrojmi a komunikáciou so zákazníkom
- aktívna spolupráca s kolegami pri odovzdávaní informácií z vyšetrovania a stavu bezpečnosti v monitorovanom prostredí
- aktívna spolupráca s kolegami pri detailnej analýze špecifických incidentov (sieťové problémy, problémy staníc, problémy databáz, atď.)
- tvorba postupov pre vyšetrovanie vybraných typov incidentov
- návrhy na úpravu konfigurácie monitorovaného prostredia a zvýšenie jeho bezpečnosti
- návrhy na doplnenie mechanizmov a technológií a zvýšenie efektivity odhaľovania incidentov
- úprava nastavenia analytických bezpečnostných nástrojov

Zamestnanecké výhody, benefity
- Flexibilný čas
- Možnosť home office
- Školenia a profesionálny rast
- Prístup k najnovším technológiám

Informácie o výberovom konaní
Svoje životopisy zasielajte e-mailom na adresu: jobs@lynx.sk

Požiadavky na zamestnanca
Pozícii vyhovujú uchádzači so vzdelaním
- vysokoškolské II. stupňa

Vzdelanie v odbore
- Informatika

Jazykové znalosti
- Anglický jazyk - Stredne pokročilý (B2)

Vodičský preukaz
- B

Prax na pozícii/v oblasti
- IT bezpečnosť

Počet rokov praxe
- 3

Kontakt
Kontaktná osoba: JUDr. Mária Cicoňová
Tel.: +421557271717
E-mail: jobs@lynx.sk

Osobnostné predpoklady a zručnosti
Požiadavky - nutné:
- skúsenosti v oblasti IT bezpečnosti aspoň 3 roky
- výborná znalosť v oblasti sieťovej komunikácie
- znalosť princípov logovania na úrovni operačných systémov a zariadení
- znalosť MITRE
- znalosť SIEM riešení a postupu vyšetrovania (niektorý z QRadar, SPLUNK, ArcSight)

- anglický jazyk
- dobré komunikačné schopnosti
- chuť učiť sa nové veci
- schopnosť tímovej práce aj samostatnej činnosti
- zvládanie časového stresu
- rýchla orientácia v problémoch
- zodpovedné a empatické vystupovanie

Požiadavky - výhodou:
- detailná znalosť vybraných bezpečnostných platforiem a možností ich funkcionalít (firewall, IPS/IDS, AV, EDR a iné)
- znalosť riešenia bezpečnostných incidentov v organizácii
- certifikácia v oblasti SIEM riešení (QRadar, SPLUNK, ArcSight)
- certifikácia/školenia v oblasti IT bezpečnosti (CompTIA Security+ a pod.)
- znalosť technickej normy ISO2700X
- skúsenosti s ITIL