Cyber Threat Intelligence Analyst (Mid)

Szukamy osoby z udokumentowanym doświadczeniem w analizie zagrożeń cybernetycznych, która wesprze nasz zespół CTI w rozwoju i doskonaleniu zdolności w zakresie oceny monitorowanego ruchu IP oraz dostarczania danych strategicznych i technicznych dotyczących zagrożeń zewnętrznych z domeny cyber.

Chcesz wykorzystać swoje umiejętności, a jednocześnie rozwijać się u jednego z najciekawszych pracodawców na rynku?

Dołącz do naszego Zespołu!

DO TWOICH OBOWIĄZKÓW BĘDZIE NALEŻAŁO:

- Pozyskiwanie i analiza danych z wielu źródeł (OSINT, darknet, komercyjne feedy, ISAC, etc.),

Identy kacja kampanii APT, grup cyberprzestępczych, malware i technik ataku (TTPs),

Korelowanie informacji o zagrożeniach z incydentami wewnętrznymi i telemetrykĄ z SIEM, EDR, NDR,

Tworzenie raportów strategicznych, operacyjnych i technicznych (IOC, IOA, TTP, Attribution),

Prowadzenie pro li zagrożeЕ (Threat Actor Pro ling) i tworzenie bazy wiedzy o przeciwnikach,

Współpraca z zespołami SOC, IR, Threat Hunting i Vulnerability Management,

Praca z narzędziami: MISP, ThreatConnect, The Hive, Maltego, VirusTotal Enterprise, Recorded Future,

Współpraca z podmiotami zewnętrznymi: partnerzy TI, CERTy, fora ISAC.

WYMAGAMY:

UkoЕczonych lub (lub w trakcie ostatniego roku) studiów wyższych na kierunku: cyberbezpieczeЕstwo, informatyka, teleinformatyka, analiza danych, telekomunikacja lub inne kierunki ścisłe,

Min. 2 4 letniego doświadczenia w obszarze cyberbezpieczeЕstwa, z czego co najmniej 1 rok w CTI, SOC lub IR,

Praktycznej znajomości:

- MITRE ATT&CK, Cyber Kill Chain,
- IOC/IOA, STIX/TAXII, Diamond Model,
- Analizy technicznej malware/phishing/TTPs,
- Doświadczenie z narzędziami takimi jak Recorded Future, OpenCTI,Vertex Synapse, Censys, Shodan, Maltego, itp.,

Doświadczenia w pracy z narzędziami TI oraz systemami telemetrycznymi (SIEM, EDR, etc.),

Umiejętności samodzielnego przygotowywania i prezentowania analiz w języku angielskim (B2/C1),

Umiejętności pracy pod presją i analizy informacji niepełnych,

Samodzielności, odpowiedzialności, inicjatywy,

Zdolności komunikacyjnych i współpracy międzyzespołowej.

DODATKOWE ATUTY:

Certy katy branżowe, np.:

- CompTIA Security+ / CySA+,
- eJPT / eCTIA / eCDFI,
- GIAC GCTI, GCIH, GCIA,

- CEH,
- OSCP,

Umiejętności w zakresie analizy kodu malware (reverse engineering),

Znajomość Python lub Bash (automatyzacja zbierania, przetwarzania i enrichowania danych),

Doświadczenie w tworzeniu playbooków, YARA rules, integracjach z MISP, TheHive, etc.,

Znajomość języków obcych przydatnych w analizie zagrożeń (np. rosyjski, chiński).

OFERUJEMY:

Przewidywane zarobki pomiędzy 9000-11500 PLN netto + świadczenie teleinformatyczne, zgodnie z art. 5 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa),

Udział w projektach o znaczeniu strategicznym dla bezpieczeństwa państwa,

Pracę w zespole Threat Intelligence współpracującym z krajowymi i zagranicznymi CSIRT-ami,

Realny wpływ na bezpieczeństwo infrastruktury klasy enterprise i OT,

Dostęp do płatnych narzędzi TI i platform edukacyjnych (SANS, INE, HTB,TryHackMe),

Mentoring i ścieżka rozwoju do poziomu Threat Hunter lub Senior CTI Analyst,

Budżet szkoleniowy do wykorzystania,

Stabilne warunki zatrudnienia,

Elastyczne godziny pracy,

Możliwość doskonalenia kompetencji językowych,

Do nansowanie karnetów sportowych,

Opiekę medyczną,

Miejsca parkingowe,

Wewnętrzną siłownię i bufet.

MIEJSCE PRACY:

woj. mazowieckie - Warszawa (brak mozliwości pracy zdalnej)

Zobacz także

- Rekrutacja
- Służba vs. Praca
- Szkolenie
- Akty prawne

aplikuj

Poprzedni Strona
Następny Strona