OChK to dostawca rozwiązań chmurowych. Działa w modelu multicloud oferując zarówno usługi świadczone z autorskiej Platformy OChK, jak i chmur publicznych Google Cloud i Microsoft Azure. Wyróżnikiem firmy na rynku są usługi dodane: zespół certyfikowanych inżynierów i inżynierek OChK pomaga klientom w doborze technologii, migracji istniejących aplikacji, budowie, rozwoju i utrzymaniu natywnych rozwiązań w chmurach publicznych oraz monitorowaniu i zapewnieniu bezpieczeństwa środowiska IT. Dodatkowo wspiera ich w procesie budowy kompetencji niezbędnych, by w pełni wykorzystać potencjał chmury w realizacji ich strategii biznesowej. OChK łączy najnowsze technologie i ludzi, którzy potrafią je wykorzystać. Dzięki temu skutecznie pomaga zarówno przedsiębiorstwom (od dużych korporacji po małe startupy), jak i instytucjom publicznym, w procesach transformacji cyfrowej.

Aktualnie do naszego zespołu Cybersecurity szukamy:

Security Analyst (SOC Tier 2)

Miejsce pracy: **Warszawa (ul. Grzybowska 62) / hybrydowo**

Aplikuj

poziom stanowiska: **Intermediate**

wynagrodzenie: **10-15 tys. brutto**

rodzaj umowy: **UoP / B2B**

wymiar pracy: **pełny**

Twój zakres obowiązków:

- wspieranie klienta oraz pierwszej linii SOC,
- analizowanie i rozwiązywanie złożonych incydentów wykrytych przez SOC, w tym podejmowanie decyzji dotyczących eskalacji i wdrożenia odpowiednich działań naprawczych,
- tworzenie i optymalizowanie zaawansowanych scenariuszy SOC w celu zwiększenia skuteczności wykrywania zagrożeń,
- przygotowywanie kompleksowych raportów i rekomendacji opartych na wynikach analizy incydentów oraz działania SOC,
- rozwijanie, implementowanie i utrzymanie zaawansowanych systemów klasy SIEM, SOAR, w tym wdrażanie niestandardowych integracji i automatyzacji procesów,
- realizowanie zadań z zakresu Cyber Threat Intelligence na podstawie najnowszych technik i narzędzi,
- współpracowanie z zespołami IT i biznesowymi w celu poprawy ogólnego poziomu bezpieczeństwa infrastruktury organizacji.

Nasze wymagania:

- zaawansowana wiedza w zakresie bezpieczeństwa IT oraz praktyczne doświadczenie w analizie incydentów bezpieczeństwa,
- znajomość technologii i infrastruktury, w szczególności: sieci (np. TCP/IP, protokoły sieciowe), systemów operacyjnych (Windows, Linux), baz danych oraz aplikacji,
- doświadczenie w zarządzaniu i konfiguracji systemów klasy SIEM, SOAR oraz EDR (np. tworzenie reguł, integracje, automatyzacja),
- dobra znajomość zastosowań kryptografii w IT oraz protokołów bezpieczeństwa (np. TLS, IPsec),
- znajomość technik ataków i narzędzi używanych przez cyberprzestępców, a także mechanizmów obronnych,
- umiejętność pracy w zespole oraz samodzielnego rozwiązywania problemów.

Mile widziane:

- doświadczenie w realizacji projektów z zakresu DFIR, Threat Hunting lub Cyber Threat Intelligence będzie dodatkowym atutem.

Oferujemy:

W OChK:

- cenimy proaktywność i inicjatywę własną, dlatego wspieramy autonomię w podejmowaniu decyzji,
- budujemy kulturę organizacyjną na wartościach takich jak profesjonalizm, współodpowiedzialność i wzajemny szacunek,
- pracujemy zadaniowo w trybie hybrydowym lub zdalnym,
- przykładamy dużą wagę do efektywnego onboardingu, podczas którego w luźnej atmosferze i przy pełnym wsparciu Twojego CloudBuddiego poznajesz zespół, firmę i swoje obowiązki,
- inwestujemy w Twój rozwój poprzez finansowanie szkoleń i certów,
- od pierwszego dnia pracy udostępniamy Ci platformy edukacyjne Google i Microsoft,
- pracujemy w zwinnym środowisku pracy, z wykorzystaniem aplikacji zwiększających efektywność, takich jak Google Workspace, Slack, GitHub, Jira,
- oferujemy prywatną opiekę medyczną,
- umożliwiamy Ci przystąpienie do ubezpieczenia grupowego na preferencyjnych warunkach,
- pokrywamy koszt karty Multisport,
- organizujemy i współfinansujemy naukę języka angielskiego,
- lubimy się integrować podczas różnorodnych inicjatyw - firmowych i oddolnych, które pomagają nam się lepiej poznać i utrzymać dobrą atmosferę współpracy.