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. Jego wyróżnikiem na rynku są usługi dodane. Zespół certyfikowanych inżynierów i architektów chmurowych 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 klientów 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 przedsiębiorstwom i instytucjom publicznym w procesach transformacji cyfrowej.

Aktualnie do naszego zespołu Cybersecurity szukamy:

SOC Architect

Miejsce pracy: **Warszawa / zdalnie**

Aplikuj

poziom stanowiska: **Senior**

wynagrodzenie: **20-28 tys brutto**

rodzaj umowy: **UoP / B2B**

wymiar pracy: **pełny**

O projekcie:

Pracując z nami znajdziesz się w zespole ekspertów, którego celem jest zapewnianie bezpieczeństwa systemów naszych klientów w hybrydowych środowiskach chmurowych.

Będziesz:
- opracowywać architekturę bezpieczeństwa dla naszych klientów, którą następnie wdrożysz w życie,
- uruchamiać i utrzymywać oraz rozwijać monitoring naszych klientów z wykorzystaniem rozwiązań chmurowych, a także optymalizować ich bezpieczeństwo w chmurze,
- rekomendować propozycje zmian klientom, które mogą mieć pozytywny wpływ na poziom bezpieczeństwa ich organizacji.

Twój zakres obowiązków:

- wdrażanie i konfiguracja usługi Microsoft Sentinel z uwzględnieniem procesu monitorowania, wykrywania i reagowania na zagrożenia cybernetyczne,
- konfigurowanie zabezpieczeń oraz reguł detekcji w Microsoft Defender XDR w celu optymalnej ochrony środowiska klienta,
- ocena poziomu bezpieczeństwa infrastruktury IT, ze szczególnym uwzględnieniem rozwiązań budowanych w chmurach publicznych (Azure, M365, GCP),
- przeprowadzenie klienta przez kompleksowy proces wdrażania i konfiguracja rozwiązań klasy SIEM/SOAR oraz Microsoft Defender,
- ścisła współpraca z zespołem operacyjnym oraz klientami w celu zapewnienia skutecznej ochrony przed zagrożeniami cybernetycznymi,
- udzielanie wsparcia technicznego i szkoleń dla personelu klienta w zakresie korzystania z narzędzi SOC,
- udział w tworzeniu dokumentacji analitycznej w zakresie bezpieczeństwa.

Nasze wymagania:

- doświadczenie we wdrażaniu usług SOC oraz znajomość narzędzi Microsoft Sentinel i Defender - warunek konieczny,
- znajomość procesów monitorowania i reagowania na incydenty bezpieczeństwa IT (Mitre ATT&CK, SIEM, SOAR, doświadczenie w testach blue team/red team),
- wiedza na temat bezpieczeństwa systemów operacyjnych (Linux/Windows),
- praktyczne doświadczenie w zabezpieczaniu AD/Entra, Google Cloud Identity oraz zarządzanie bezpieczeństwem kont i sekretów, a także zabezpieczenie dostępu uprzywilejowanego (IAM/IDM, PIM/PAM, PAW, Vault),
- znajomość rozwiązań bezpieczeństwa do ochrony środowisk chmurowych oraz sieciowych (SDN, VPC, FW,WAF),
- doświadczenie w merytorycznym prowadzeniu zespołu analityków i operatorów SOC,
- umiejętności komunikacyjne i zdolność do pracy w zespole.

Mile widziane:

- automatyzacja pracy za pomocą skryptów (np. Python/Shell/PowerShell, Infrastructure as Code: Terraform, Terragrunt, Chef, Puppet, Ansible itp.),
- znajomość procesów i narzędzi DevOps/DevSecOps,
- doświadczenie w pracy przy tworzeniu oprogramowania w modelu CI/CD,
- certyfikaty branżowe z zakresu bezpieczeństwa IT będą dodatkowym atutem (np. CompTIA Security+, CISSP, CEH).

Oferujemy:

- tworzymy kulturę otwartej komunikacji i wymiany wzajemnych doświadczeń,
- cenimy inicjatywę własną i wspieramy autonomię w podejmowaniu decyzji,
- naszych pracowników obejmujemy opieką medyczną oraz dobrowolnym ubezpieczeniem grupowym,
- pokrywamy też koszty karty Multisport,
- organizujemy i współfinansujemy naukę języka angielskiego,
- pracujemy w elastycznych godzinach, w zwinnym środowisku pracy z wykorzystaniem czołowych aplikacji zwiększających jej efektywność takich jak: Google Workspace, Slack, GitHub, Jira,
- od pierwszego dnia pracy uzyskasz dostęp do materiałów szkoleniowych i platform edukacyjnych w obszarze rozwiązań Google oraz Microsoft - liczą się Twoje chęci,
- staramy się być z pracownikami w ważnych momentach nie tylko życia zawodowego - wspólnie celebrujemy również ważne wydarzenia w życiu prywatnym,
- w pierwszych dniach przywitamy Cię na onboardingu, w trakcie którego w luźnej atmosferze poznasz zespół, firmę i swoje obowiązki - nie zapominamy o powitalnym prezencie, oraz przypisaniu Ci “cloud buddy”, aby jeszcze bardziej wesprzeć proces Twojej aklimatyzacji.