Ekspert ds. Cyberbezpieczeństwa IT i OT
w firmie RAMS DATA Sp z o.o. (Warszawa)

Twój zakres obowiązków

- Instalacja, konfiguracja, uruchamianie, wdrażanie, wykonywanie migracji i testowanie systemów, narzędzi i rozwiązań informatycznych, takich jak systemy wykrywania intruzów czy zapory ogniowe,, itp..
- Udział w wdrażaniu systemów związanych z Industry 4.0 pod kątem IIT
- Nadzór nad realizacją cybernetycznych zabezpieczeń systemów OT;
- Przeprowadzanie warsztatów technicznych, szkoleń, prezentacji, udzielania wsparcia technicznego i innych usług dotyczących obsługi i działania systemów i rozwiązań informatycznych
- Spotkania techniczne i obsługa umów serwisowych (zdalne lub u klienta na miejscu rozwiazywanie problemów w przypadku awarii. utrzymanie architektury serwerów, sieci, systemów bezpieczeństwa i komputerów, etc..)
- Weryfikacja dokumentów oraz opracowywanie dokumentacji przed i powdrożeniowej oraz dokumentów opisowych do celów marketingowych, tworzonych w ramach programu cyberbezpieczeństwa w zakresie IT i OT;
- Udział w projektach z zakresu bezpieczeństwa.
- Tworzenie architektury cyberbezpieczeństwa systemów IT i OT (działania w środowisku o sporej złożoności i zróżnicowanym zapleczu technologicznym)
- Uczestniczenie w ciągłym doskonaleniu z zakresu IT.
- Przestrzeganie zasad cyberbezpieczeństwa IT.
- Praca z najnowszymi technologiami i z topowymi dostawcami usług powiązanych z bezpieczeństwem,
- Weryfikacja rynku rozwiązań cyberbezpieczeństwa OT;
- Analizowanie trendów rynkowych i występujących zagrożeń, proponowanie nowych rozwiązań mechanizmów i systemów cyberbezpieczeństwa w celu zwiększenia odporności na zagrożenia.

Nasze wymagania

- Udokumentowane doświadczenie zawodowe w zakresie systemów informatycznych i automatyki przemysłowej — co najmniej 5 lat;
- Wiedza z zakresu cyberbezpieczeństwa poparta min. 3 letnim doświadczeniem w pracy na stanowisko analityka cyberbezpieczeństwa, testera bezpieczeństwa, specjalisty ds. cyberbezpieczeństwa
- Umiejętność obsługi umów serwisowych w dziedzinie IT i bezpieczeństwa IT, poparta min. 2 letnim doświadczeniem
- Praktyczna umiejętność wyszukiwania i analizy zagrożeń - Threat Hunting
- Wiedza z zakresu technik ofensywnych, umiejętność wykrywania podatności z listy OWASP Top 10
- znajomość frameworku ATT&CK
- zrozumienie cyber killchain oraz MITRE ATT&CK, praca ze standardami takimi jak NIST, ISO czy CIS,
- Znajomość technologii SCADA i DCS, w szczególności Emerson Ovation;

- Znajomość protokołów komunikacyjnych wykorzystywanych w OT, w szczególności Modbus i Profinet;
- Technologie przemysłowe i protokoły komunikacyjne (OPC-DA, OPC-UA, czytnik skanujący Datamatrix, RS232, Modbus, TCP/IP).
- Znajomość zagadnień związanych z bezpieczeństwem maszyn CE.
- Znajomość technologii PLC;
- Znajomość zagadnień związanych z ochroną DMZ, DNS, VPN, IDS/IPS, WebProxy, AntyMalware,
- znajomość rozwiązań klasy: Web Proxy, Email Security Gateway, SIEM, DLP, AV, EDR, PAM, SOAR, Sandbox, Skaner podatności.
- Znajomość sieci komputerowych, urządzeń sieciowych (firewall, router, switch),protokołów sieciowych,
- Rozumienie zasad cyberbezpieczeństwa i warstw TCP/IP,
- Znajomość systemów EDR i XDR,
- Znajomość systemów SIEM
- Znajomość narzędzi diagnostycznych typu Wireshark,
- Znajomość aktualnych trendów z zakresu branży IT,
- Znajomość systemów operacyjnych Linux/Windows oraz rozwiżań do wirtualizacji na poziomie co najmniej średniozaawansowanym,
- Znajomość rozwiązania Active Directory oraz związanych z nim kwestii bezpieczeństwa,
- Silne umiejętności analityczne i samodzielność w rozwiązywaniu problemów,
- Umiejętność tworzenia dokumentacji technicznej oraz wymagań i standardów IT i OT
- Umiejętność projektowania i testowania rozwiązań bezpieczeństwa
- Poświadczenie bezpieczeństwa osobowego upoważaniającego do dostępu do dokumentów niejawnych o klauzuli co najmniej „poufne” lub gotowość do poddania się, po dokonaniu zatrudnienia, procedurze sprawdzającej związanej z uzyskaniem poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych.
- Wykształcenie wyższe (preferowane kierunki: sieci, systemy operacyjne, bezpieczeństwo teleinformatyczne, analiza po-włamaniowa)
- Znajomość języka angielskiego na poziomie pozwalającym na rozumienie dokumentacji technicznej i swobodnej komunikacji z osobami anglojęzycznymi
- Dobre zdolności i oratorskie i prezentacyjne (umiejętność opisywania i przedstawiania rzeczy w prosty i zrozumiały sposób)
- Bardzo dobra organizacja pracy, umiejętność pracy w zespole
- Umiejętność nawiązywania kontaktów,
- Elastyczność i dostosowywanie się do zmieniających się priorytetów
- Umiejętność analizy i rozwiązywania problemów
- Nastawienie na skuteczność oraz terminowość realizacji zadań, umiejętność pracy pod presją czasu
- Inicjatywa i pro-aktywność, która poprawi ogólny wizerunek firmy
- determinacja do osiągnięcia celu, mimo napotkanych po drodze trudności.
- Prawo jazdy kategorii B,
- Nieposzlakowana opinia, dyskrecja (zaświadczenie o niekaralności)
- Gotowość do pracy zdalnej lub stacjonarnej

Mile widziane

- Znajomość języków programowania java, python, c++, inne
- Wiedza czym różni się cloud od on-prem oraz jakie akcje trzeba podjąć, aby jak najlepiej zabezpieczyć chmurę przed zagrożeniami,
- Znajomość akronimów takich jak AAD, 2FA, SSO oraz stojących za nimi koncepcji,
- Podstawowa wiedza o konteneryzacji
- Wiedza o platformie M365 i powiązanych z nią rozwiązaniach,
- Zrozumienie czym jest pentesting i znajomość podstawowych metodyk (np. OWASP) czy narzędzi jego prowadzenia (Kali, Burp, etc.),
- Certyfikaty branżowe (CompTIA, AWS, Azure, GCP, ISC2, ISACA itd.).
- Certyfikat CEH, Security+, SSCP lub podobny
- Certyfikaty bezpieczeństwa OSCP, CEH, Mitre MAD20, crest CPTIA, ec-Council CTIA

- Znajomość rozwiązań sieciowych bezpieczeństwa IT i OT producentów: Palo Alto Networks, F5, Cisco, Forcepoint, Ivanti, Trelix, Tennable, etc..
- Znajomość tworzenia filmów videdo i stron WWW

Takie dajemy możliwości rozwoju

- Przestrzeń do eksperymentowania
- Szkolenia wewnątrz firmowe i zewnętrzne
- Wsparcie merytoryczne od liderów technologicznych
- Wymiana wiedzy technicznej w firmie

To oferujemy

- Możliwości rozwoju zawodowego oraz ciekawe wyzwania
- Praca w ambitnym i dynamicznie rozwijającym się zespole
- Atmosferę wsparcia i współpracy
- Atrakcyjne wynagrodzenie i system nagradzania
- Możliwość współpracy w oparciu o Umowę o Pracę, bądź kontrakt B2B
- Praca zdalna w tygodniu na bieżąco oraz dodatkowe dni w weekend w wyjątkowych sytuacjach (możliwość pracy stacjonarnej (WARSZAWA) w razie takiej potrzeby)
- Elastyczne godziny pracy
- Przestrzeń do eksperymentowania,
- Możliwość samodoskonalenia i rozwoju w wielu dziadzinach, takich jak: automatyka przemysłowa, programowanie, administracja rozwiązaniami on-prem lub cloud,
- Współpracę opartą na wartościach - jesteśmy zespołem, który kieruje się określonymi wartościami. Wspieramy atmosferę pracy opartą na szacunku, zaufaniu i współpracy. Promujemy innowacyjność, kreatywność i odpowiedzialność
- Możliwości rozwoju - wierzymy w nieustanne doskonalenie i chcemy pomagać naszym pracownikom w rozwoju potencjału (oferujemy szkolenia wewnętrzne i zewnętrzne, warsztaty szkolenia e-learningowe, programy rozwojowe, oraz możliwość uczestniczenia w rekrutacjach wewnętrznych)
- Przyjazną atmosferę, zarówno w pracy jak i poza nią
- Wsparcie merytoryczne od liderów technologicznych

Zainteresowanych prosimy o przesyłanie aplikacji na adres: kontakt@ramsdata.com.pl