

WKPS.1121.1.2019
2019-00845

**Dyrektor Centrum Systemów Informatycznych Ochrony Zdrowia
poszukuje kandydata na stanowisko:
ARCHITEKT BEZPIECZEŃSTWA IT
w Wydziale Bezpieczeństwa Systemów Teleinformatycznych
Liczba stanowisk: 1 w wymiarze pełnego etatu**

Chcesz mieć wpływ na rozwiązania mające chronić Twoje dane medyczne i wyznaczać nowe standardy bezpieczeństwa w systemach informatycznych ochrony zdrowia. Czujesz się ekspertem z zakresu cyberbezpieczeństwa, a przede wszystkim posiadasz doświadczenie w prowadzeniu projektów związanych z cyberbezpieczeństwem? Nie boisz się wyzwań i szukania dziur w całym? Jeśli tak to zapraszamy do nas.

Centrum Systemów Informatycznych Ochrony Zdrowia

to agenda rządowa odpowiedzialna za budowę systemów teleinformatycznych dla służby zdrowia. W chwili obecnej do nowopowstałego Wydziału Bezpieczeństwa Systemów Teleinformatycznych poszukujemy architekta bezpieczeństwa IT. Wydział jest odpowiedzialny za zapewnienia bezpieczeństwa systemów teleinformatycznych Centrum, jak i Ministerstwa Zdrowia.

OPIS STANOWISKA/ REALIZOWANE ZADANIA

1. Tworzenie i rozwój architektury referencyjnej w obszarze cyberbezpieczeństwa, w tym wyznaczanie standardów i rozwiązań zgodnie z wymaganiami biznesowymi.
2. Opracowywanie dokumentacji architektonicznej i analitycznej, w tym specyfikacji funkcjonalnej i нефункциональной oraz projektów technicznych.
3. Koordynacja i nadzór nad wdrażaniem nowych rozwiązań technologicznych związanych z systemami zabezpieczeń (IDS, IPS, Firewall, SIEM, EDR, SAST, DLP, DAM, IDM itd.).
4. Rozwój narzędzi monitorowania bezpieczeństwa sieci infrastrukturalnych i systemów zarządzania incydentami bezpieczeństwa.
5. Analiza ryzyk związanych z bezpieczeństwem IT, przeglądy i audyty w obszarze bezpieczeństwa IT.
6. Podnoszenie świadomości pracowników Centrum i prowadzenie szkoleń z zakresu bezpieczeństwa IT.

WYMAGANIA

1. Wykształcenie wyższe o specjalności: informatyka, telekomunikacja i/lub pokrewne.
2. Minimum 5 lat doświadczenia zawodowego, w tym 3 lata na stanowisku architekta w obszarze bezpieczeństwa IT.
3. Znajomość zagadnień związanych z bezpieczeństwem baz danych, aplikacji, systemów, sieci teleinformatycznych.

4. Znajomość protokołów sieciowych: TCP/IP, DNS, HTTP/HTTPS, SMTP, SSL.
5. Znajomość rozwiązań kryptograficznych i zarządzania infrastrukturą klucza publicznego.
6. Umiejętność doboru rozwiązań i projektowania architektury systemów klasy: AV, DLP, DAM, IDM, IPS/IDS, SIEM.
7. Umiejętność formułowania i analizy wymagań funkcjonalnych i нефункциональных pod kątem bezpieczeństwa, ze szczególnym uwzględnieniem bezpieczeństwa informacji, ochrony danych osobowych oraz ciągłości działania.
8. Znajomość najlepszych praktyk w budowie i weryfikacji bezpieczeństwa rozwiązań teleinformatycznych.
9. Doskonałe umiejętności komunikacyjne, zdolność do zbudowania poparcia dla proponowanych rozwiązań.
10. Umiejętność dokumentowania i samodzielnego prezentowania wyników pracy.

DODATKOWE ATUTY

- Ogólna znajomość standardów z obszaru bezpieczeństwa IT, w szczególności norm serii ISO 27000, ISO 22301 oraz RODO.
- Umiejętność posługiwania się ramami architektonicznymi TOGAF oraz modelowania UML, BPMN.
- Doświadczenie w Cloud Security, blockchain.

OFERUJEMY

- Atrakcyjne wynagrodzenie zależne od posiadanego doświadczenia i umiejętności.
- Pracę w państwowej firmie informatycznej na podstawie umowy o pracę.
- Pakiet świadczeń socjalnych obejmujący m.in. atrakcyjne warunki korzystania z pakietu medycznego, ubezpieczenia grupowego.
- Dodatkowe wynagrodzenie roczne tzw. „13-tkę”.
- Dla najlepszych premie uznaniowe.
- Możliwości rozwoju i podnoszenia kwalifikacji.

WYMAGANE DOKUMENTY I OŚWIADCZENIA

Życiorys uzupełniony w zakresie informacji dotyczących wykształcenia, przebiegu dotychczasowego zatrudnienia.

MIEJSCE SKŁADANIA DOKUMENTÓW

Dokumenty aplikacyjne przyjmowane są:

- a) w postaci elektronicznej:
 - za pośrednictwem poczty elektronicznej pod adresem rekrutacie@csioz.gov.pl, poprzez przekazanie za pośrednictwem Elektronicznej Skrzynki Podawczej ePUAP,
 - przez formularz aplikacyjny dostępny na stronie internetowej www.csioz.gov.pl (w zakładce: praca),
- b) w postaci papierowej: w kancelarii Centrum pod adresem ul. Stanisława Dubois 5A, 00-184 Warszawa.

Dodatkowe informacje pod nr telefonu **(22) 597-09-45**

TERMIN SKŁADANIA DOKUMENTÓW do dnia 14 lutego 2019 r.

POZOSTAŁE INFORMACJE

1. Uprzejmie informujemy, że skontaktujemy się wyłącznie w wybranymi Kandydatami.
2. Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) informuję, iż:
 - a. administratorem Pani/Pana danych osobowych jest Centrum Systemów Informatycznych Ochrony Zdrowia, ul. Stanisława Dubois 5A, 00-184 Warszawa,
 - b. kontakt z Inspektorem Ochrony Danych - iod@csioz.gov.pl,
 - c. Pani/Pana dane osobowe przetwarzane będą dla potrzeb aktualnej i przyszłych rekrutacji - na podstawie Art. 6 ust. 1 lit. a ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. oraz Kodeksu Pracy z dnia 26 czerwca 1974 r,
 - d. Pani/Pana dane osobowe przechowywane będą przez okres rekrutacji / okres tej i przyszłych rekrutacji / przez okres 2 lat wyznaczony przez administratora,
 - e. odbiorcami Pani/Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa oraz podmioty współpracujące w procesie rekrutacji,
 - f. posiada Pani/Pan prawo do żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do przenoszenia danych, prawo do cofnięcia zgody w dowolnym momencie,
 - g. ma Pani/Pan prawo wniesienia skargi do organu nadzorczego,
 - h. podanie danych osobowych jest obowiązkowe w oparciu o przepisy prawa, a w pozostałym zakresie jest dobrowolne,
 - i. Pani/Pana dane będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania. Zautomatyzowane podejmowanie decyzji będzie odbywało się na zasadach określonych w regulaminie rekrutacji, konsekwencją takiego przetwarzania będzie kontakt tylko z wybranymi kandydatami.

WKPS.OP.WBST.9.2019