Stanowisko:

specjalistka/specjalista do spraw obsługi incydentów

w Sektorowym Zespole Reagowania na Incydenty Bezpieczeństwa Komputerowego

CSIRT INFRASTRUKTURA w Biurze Zarządzania Kryzysowego

w Ministerstwie Infrastruktury

Miejsce pracy: Warszawa, ul. Puławska 125

Twój zakres obowiązków:

- Realizuje działania niezbędne do osiągnięcia gotowości operacyjnej CSIRT-u Infrastruktura poprzez wsparcie projektu utworzenia sektorowego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) w sektorach pozostających we właściwości Ministra Infrastruktury jako organu właściwego ds. cyberbezpieczeństwa
- Przyjmuje i rejestruje zgłoszenia o incydentach i podatnościach z różnych źródeł, dokonując ich wstępnej weryfikacji i klasyfikacji
- Prowadzi analizę zgłoszeń w celu oceny ich ważności, przypisania priorytetu oraz kwalifikacji jako incydenty poważne zgodnie z obowiązującymi przepisami, w tym analizuje dane z systemów monitorujących, źródeł threat intelligence oraz wewnętrznych narzędzi CSIRT-u sektorowego
- Realizuje wstępne działania koordynacyjne w ramach obsługi incydentów poważnych, zapewniając skuteczny przepływ informacji między zaangażowanymi podmiotami, w tym prowadzi korespondencję ze zgłaszającym
- Monitoruje kanały wymiany informacji z podmiotami sektora, weryfikuje informacje o potencjalnych incydentach z przestrzeni publicznej oraz podejmuje działania mające na celu ich potwierdzenie lub wykluczenie
- Współpracuje z zespołem analitycznym w celu identyfikacji przyczyn incydentu, wzorców ataku oraz możliwych środków zaradczych
- Dokumentuje przebieg obsługi incydentu, sporządza raporty operacyjne oraz przekazuje wnioski do dalszej analizy i wykorzystania
- Wspiera działania ograniczające skutki incydentów, w tym rekomenduje działania naprawcze i mitygujące
- Uczestniczy w dyżurach operacyjnych CSIRT-u sektorowego, zapewniając ciągłość działania zespołu w trybie 24/7
- Wspiera rozwój i doskonalenie procedur oraz narzędzi wykorzystywanych w obsłudze incydentów
- Współpracuje z innymi zespołami CSIRT-u sektorowego oraz partnerami zewnętrznymi w zakresie wymiany informacji i koordynacji działań na potrzeby obsługi incydentu

Potrzebne ci będą (wymagania niezbędne):

- Wykształcenie: średnie

- Doświadczenie zawodowe: co najmniej 1 rok doświadczenia w pracy w zespole typu CSIRT/SOC lub innym zespole reagowania na incydenty bezpieczeństwa informacji
- Posiadanie poświadczenia bezpieczeństwa do klauzuli POUFNE lub wyższej lub gotowość do poddania się procedurze weryfikacyjnej upoważniającej do dostępu do informacji niejawnych, zgodnie z przepisami ustawy o ochronie informacji niejawnych
- Znajomość języka angielskiego na poziomie B1 albo w zakresie umożliwiającym co najmniej swobodne korzystanie z dokumentacji technicznej oraz prowadzenie korespondencji i komunikacji służbowej
- Doświadczenie w pracy z systemami ticketowymi w kontekście obsługi zgłoszeń incydentów bezpieczeństwa informacji
- Doświadczenie w technicznej analizie i reagowaniu na zagrożenia IT, w tym podejmowaniu działań ograniczających skutki incydentów
- Znajomość typowych zagrożeń i podatności w obszarze cyberbezpieczeństwa
- Znajomość podstaw technicznych działania sieci komputerowych, w tym protokołów, architektury i mechanizmów komunikacji
- Znajomość procesów związanych z obsługą incydentów bezpieczeństwa
- Doświadczenie w korelacji danych z różnych źródeł w celu identyfikacji zagrożeń i anomalii
- Znajomość technik wyszukiwania i analizy informacji z ogólnodostępnych źródeł, przy jednoczesnym stosowaniu zasad bezpieczeństwa operacyjnego
- Skuteczna komunikacja
- Umiejętność organizacji pracy i zorientowanie na osiąganie celów
- Umiejętność współpracy
- Posiadanie obywatelstwa polskiego
- Korzystanie z pełni praw publicznych
- Nieskazanie prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe

Dodatkowym atutem będzie (wymagania dodatkowe)

- Doświadczenie w pracy zmianowej lub w trybie dyżurowym (24/7)
- Umiejętność prowadzenia podstawowej analizy złośliwego oprogramowania za pomocą narzędzi typu sandbox
- Umiejętność pracy pod presją czasu oraz działania w warunkach intensywnego napływu informacji
- Posiadanie certyfikatu: BTL1, CDSA, CompTIA Security+, GCIH lub ECIH
- Doświadczenie w dokumentowaniu incydentów oraz przygotowywaniu raportów technicznych i operacyjnych
- Wykształcenie wyższe (lub status studenta ostatniego roku) na kierunku informatyka, cybernetyka, automatyka, telekomunikacja, cyberbezpieczeństwo, teleinformatyka lub pokrewne

Oferujemy:

- możliwość rozwoju w strukturze administracji publicznej,
- udział w ciekawym projekcie,
- możliwość częściowej pracy zdalnej,
- bogaty pakiet szkoleń, refundację nauki języka obcego i studiów podyplomowych,
- atrakcyjny pakiet socjalny w formie systemu kafeteryjnego,

- możliwość wykupienia w preferencyjnej cenie pakietu medycznego, polisy na życie i zniżkowej legitymacji PKP,
- dodatkowe wynagrodzenie tzw. „trzynastka”; dodatek za wysługę lat powyżej 5 lat pracy; nagrody jubileuszowe za wieloletnią pracę; uznaniowe nagrody za szczególne osiągnięcia; dodatek specjalny; odprawę emerytalną / rentową.

Warunki pracy:

- praca przy komputerze oraz/lub przy użyciu urządzeń biurowych,
- praca w klimatyzowanych pomieszczeniach,

Twoja aplikacja musi zawierać:

- CV
- Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie wykształcenia
- Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie doświadczenia zawodowego - np. kopie świadectw pracy, zaświadczeń o zatrudnieniu, opisów stanowisk, zakresów czynności lub kopie innych zaświadczeń (należy potwierdzić zamknięty okres i obszar tematyczny doświadczenia zawodowego)
- Oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych do celów rekrutacji
- Oświadczenie o posiadaniu obywatelstwa polskiego
- Oświadczenie o korzystaniu z pełni praw publicznych
- Oświadczenie o nieskazaniu prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe
- Oświadczenie, że w okresie od dnia 22 lipca 1944 r. do dnia 31 lipca 1990 r. kandydatka/kandydat nie pracowała/ł, nie pełniła/ł służby w organach bezpieczeństwa państwa i nie była/był współpracownikiem tych organów w rozumieniu przepisów ustawy z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944–1990 oraz treści tych dokumentów. Dotyczy kandydatek/kandydatów urodzonych przed 1 sierpnia 1972 r.
- Kopie dokumentów potwierdzających posiadanie poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych o klauzuli POUFNE lub wyżej lub zgoda na poddanie się procedurze sprawdzającej
- Dołącz, jeśli posiadasz: kopie dokumentów potwierdzających spełnienie wymagania dodatkowego w zakresie doświadczenia zawodowego; kopie certyfikatów: BTL1, CDSA, CompTIA Security+, GCIH lub ECIH

Aplikuj mailowo na adres: rekrutacja@mi.gov.pl , w temacie wpisz: **„CSIRT-1/26”**

lub w formie papierowej **w zamkniętej kopercie** z dopiskiem: **"CSIRT-1/26"**
na adres:
Ministerstwo Infrastruktury
ul. Chałubińskiego 4/6; 00-928 Warszawa

Proponowane wynagrodzenie: nie mniej niż 10 000 zł brutto

Termin składania dokumentów: Termin składania dokumentów: 15 marca 2026 r. (liczy się data wpływu do urzędu)

Dodatkowe informacje

- ✓ Jeśli zostaniesz zakwalifikowany do kolejnego etapu, powiadomimy Cię o tym mailowo (lub telefonicznie – jeżeli nie podałeś adresu e-mail).
- ✓ Jeśli ofertę składasz elektronicznie, własnoręcznie podpisane oświadczenia z aktualną datą i dołącz w formie zeskanowanych dokumentów
- ✓ Kompletna aplikacja to taka, która zawiera wszystkie wymagane dokumenty i własnoręcznie podpisane oświadczenia.
- ✓ Zwróć uwagę na warunki pracy, które wskazaliśmy w ogłoszeniu – rzetelnie oceń, czy odpowiada Ci taka praca.
- ✓ Złożone przez Ciebie dokumenty zweryfikujemy pod względem formalnym na podstawie zapisów ogłoszenia dotyczących wymaganych i dodatkowych dokumentów.
- ✓ Informacja o metodach naboru:
  - weryfikacja formalna nadesłanych ofert
  - możliwość przeprowadzenia testu wiedzy merytorycznej
  - rozmowa kwalifikacyjna (możliwość przeprowadzenia rozmowy przez MS Teams)
- ✓ Nie rozpatrujemy ofert, które zostały dostarczone po terminie.
- ✓ Jeśli planujesz wysłać aplikację w formie papierowej, zadbaj o to, aby wpłynęła do nas w wyznaczonym terminie. Liczy się data wpływu do urzędu.
- ✓ W przypadku aplikacji elektronicznej - załączniki znajdujące się w udostępnionej w internecie przestrzeni dyskowej (tzw. chmury) nie będą pobierane.
- ✓ Ministerstwo zastrzega sobie prawo do kontaktu tylko z kandydatami, których oferty spełniają wymagania formalne.
- ✓ W Ministerstwie Infrastruktury możesz zgłosić naruszenie prawa w trybie określonym w Wewnętrznej procedurze dokonywania zgłoszeń naruszeń prawa i podejmowania działań następczych w Ministerstwie Infrastruktury, stanowiącej Załącznik do Zarządzenia nr 15 Dyrektora Generalnego z dnia 25 września 2024 r. w sprawie ustalenia wewnętrznej procedury zgłaszania informacji o naruszeniach prawa i podejmowania działań następczych. Szczegóły znajdują się na naszej stronie pod adresem: https://www.gov.pl/web/infrastruktura/wewnetrzne-zgloszenia-naruszenia-prawa

Informacja na temat przetwarzania danych osobowych

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej jako „RODO" informuję, że:

ADMINISTRATOR DANYCH OSOBOWYCH

Administratorem Państwa danych osobowych jest Minister Infrastruktury z siedzibą w Warszawie przy ul. T. Chałubińskiego 4/6 zwany dalej „administratorem".

Z administratorem można się kontaktować:
- telefonicznie, pod numerem: 22 630 10 10,
- mailowo, pod adresem: kancelaria@mi.gov.pl,
- za pomocą usługi e-Doręczenia: adres: AE:PL-99756-74876-WBAEG-25
- listownie oraz osobiście w siedzibie administratora.

CEL PRZETWARZANIA DANYCH OSOBOWYCH

Państwa dane osobowe będziemy przetwarzać w celu przeprowadzenia naboru na wolne stanowisko w Sektorowym Zespole Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT INFRASTRUKTURA w Biurze Zarządzania Kryzysowego w Ministerstwie Infrastruktury.

PODSTAWA PRAWNA PRZETWARZANIA DANYCH

Państwa dane podane w zakresie wynikającym z art. 22^1 *Kodeksu pracy* oraz ustawy *pracownikach urzędów państwowych* (m.in. imię, nazwisko, dane kontaktowe, wykształcenie, przebieg dotychczasowego zatrudnienia) będziemy przetwarzać na podstawie art. 6 ust. 1 lit. b RODO.

Podanie innych danych, których przekazanie nie jest wymagane przepisami prawa, zostanie potraktowane jako wyrażenie przez Państwa świadomej i dobrowolnej zgody na ich przetwarzanie (art. 6 ust. 1 lit. a RODO).

OKRES PRZECHOWYWANIA DANYCH OSOBOWYCH

Państwa dane osobowe będą przechowywane:

- w przypadku zatrudnienia - przez 10 lat od momentu zakończenia zatrudnienia, zgodnie z przepisami wydanymi na podstawie art. 6 ust. 2 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164, z 2025 r. poz. 1173);
- w przypadku, gdy Państwa aplikacja nie spełniła wymogów formalnych, nie wybrano Państwa do zatrudnienia albo w przypadku, gdy wygrali Państwo nabór, ale nie podjęli zatrudnienia – Państwa dane zostają w dokumentacji z naboru jedynie w zakresie: imię i nazwisko oraz miejsce zamieszkania (miasto) przez okres 10 lat na podstawie art. 6 ust. 2 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach. Pozostałe dane są niszczone (poprzez zmielenie lub usunięcie z poczty elektronicznej) po upływie 3 miesięcy od daty zakończenia naboru lub zatrudnienia wybranego w naborze kandydata.

ODBIORCY DANYCH OSOBOWYCH

Państwa dane zostaną udostępnione Naukowej i Akademickiej Sieci Komputerowej – Państwowemu Instytutowi Badawczemu (NASK), który wspiera administratora danych w zakresie oceny merytorycznej kandydatów.

Administrator przewiduje możliwość powierzenia przetwarzania Państwa danych innym podmiotom świadczącym na jego rzecz usługi z zakresu IT.

ZAUTOMATYZOWANE PODEJMOWANIE DECYZJI

Państwa dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

PRAWA ZWIĄZANE Z PRZETWARZANIEM DANYCH OSOBOWYCH

W związku z przetwarzaniem danych osobowych przysługują Państwu następujące prawa:

- prawo dostępu do treści danych i otrzymania ich kopii, prawo do sprostowania danych, prawo do ograniczenia przetwarzania danych, prawo do usunięcia danych;
- cofnięcia zgody i usunięcia danych odnośnie do tych danych, których podanie nie jest wynika z przepisów prawa (zgoda na przetwarzanie danych osobowych może zostać cofnięta w dowolnym momencie). Wycofanie zgody nie wpływa jednak na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem;
- jeśli uznają Państwo, że przetwarzamy Państwa dane w sposób niezgodny z obowiązującymi przepisami mogą Państwo również skorzystać z prawa wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych – przed realizacją tego prawa sugerujemy kontakt z naszym IOD w celu wyjaśnienia ewentualnych wątpliwości.

Podanie przez Państwa danych osobowych, wskazanych w ogłoszeniu o naborze jako niezbędne, jest dobrowolne. Konsekwencją niepodania tych danych jest jednak uznanie Państwa aplikacji za niespełniającej wymagań formalnych i pozostawienie bez dalszego rozpoznania. Podanie danych innych niż wymagane nie ma wpływu na proces rekrutacji i nie jest niezbędne.

KONTAKT W SPRAWACH ZWIĄZANYCH Z PRZETWARZANIEM DANYCH OSOBOWYCH

Administrator wyznaczył Inspektora Ochrony Danych (dalej: IOD), z którym można skontaktować się w sprawach związanych z przetwarzaniem danych osobowych. Kontakt z IOD jest możliwy za pośrednictwem:

- adresu e-mail IOD: inspektor.RODO@mi.gov.pl,
- korespondencyjnie na adres siedziby administratora.