Stanowisko:

analityk/analityczka cyberbezpieczeństwa – junior (2 etaty)

w Sektorowym Zespole Reagowania na Incydenty Bezpieczeństwa Komputerowego

CSIRT INFRASTRUKTURA w Biurze Zarządzania Kryzysowego

w Ministerstwie Infrastruktury

Miejsce pracy: Warszawa, ul. Chałubińskiego 4/6

Twój zakres obowiązków:

1) 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.
2) Pozyskuje i analizuje informacje o zagrożeniach cyberbezpieczeństwa, w szczególności monitoruje otwarte i zamknięte źródła threat intelligence, systemy monitorujące, kanały wymiany informacji oraz partnerów krajowych i międzynarodowych
3) Selekcjonuje, weryfikuje i interpretuje dane o zagrożeniach, w szczególności ocenia wiarygodność źródeł, identyfikuje luki informacyjne, analizuje taktyki, techniki i procedury (TTP) wykorzystywane przez atakujące grupy
4) Dystrybuuje informacje o zagrożeniach do podmiotów sektora, w szczególności przygotowuje treści komunikatów i alertów oraz identyfikuje adresatów
5) Identyfikuje i analizuje podatności, w szczególności ocenia ich wpływ na bezpieczeństwo systemów i usług sektora, opracowuje scenariusze potencjalnego wykorzystania oraz rekomendacje środków zaradczych
6) Wspiera analizę incydentów bezpieczeństwa, w szczególności współpracuje z zespołem reagowania w zakresie korelacji zdarzeń, identyfikacji wzorców ataku oraz oceny wpływu incydentów na sektor
7) Współtworzy rekomendacje prewencyjne i dobre praktyki
8) Świadczy doradztwo techniczne, w szczególności wspiera podmioty sektora w zakresie analizy zagrożeń, oceny ryzyka i doboru środków ochrony, uczestniczy w grupach roboczych i konsultacjach eksperckich

Potrzebne ci będą (wymagania niezbędne):

- Wykształcenie: wyższe na kierunku informatyka lub telekomunikacja lub automatyka lub cyberbezpieczeństwo lub pokrewne
- Doświadczenie zawodowe co najmniej 1 rok na stanowisku związanym z analizą zagrożeń, incydentów lub podatności w zespołach typu CSIRT/SOC, threat intelligence lub informatyki śledczej.
- 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
- Znajomość przepisów ustawy o krajowym systemie cyberbezpieczeństwa oraz dyrektywy NIS 2

- Znajomość technicznych aspektów działania sieci komputerowych, w tym protokołów, architektury i mechanizmów komunikacji.
- Wiedza z zakresu cyberzagrożeń i technik ataku, w tym TTP (tactics, techniques, procedures) oraz faz ataku.
- 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)

- Posiadanie co najmniej jednego z certyfikatów: CTIA (EC), CTIA (Mile2), CompTIA CySA+, GCTI, BTL2.
- Znajomość języka rosyjskiego na poziomie B1. Alternatywnie: znajomość języka rosyjskiego w zakresie umożliwiającym posługiwanie się dokumentacją techniczną i prowadzenie korespondencji.
- Umiejętność prowadzenia badań i wyszukiwania informacji o zagrożeniach w otwartych i zamkniętych źródłach z zachowaniem zasad bezpieczeństwa operacyjnego.
- Umiejętność analizy zbiorów danych, w tym ruchu sieciowego, maili w formacie eml oraz logów z maszyn i korelacji informacji z różnych źródeł.
- Znajomość przepisów RODO, rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności.

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,
- udogodnienia dla rowerzystów - stojaki na rowery pod zadaszeniem na terenie ministerstwa, prysznic,
- preferencyjne ceny posiłków w kantynie znajdującej się na terenie Ministerstwa.

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
- Kopie dokumentów potwierdzających posiadanie poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych o klauzuli POUFNE lub wyżej lub zgoda na poddanie się procedurze sprawdzającej
- 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.
- Dołącz, jeśli posiadasz: kopie certyfikatów: CTIA (EC), CTIA (Mile2), CompTIA CySA+, GCTI, BTL2.

Aplikuj mailowo na adres: rekrutacja@mi.gov.pl , w temacie wpisz: **„CSIRT-5/25”**
lub w formie papierowej **w zamkniętej kopercie** z dopiskiem: **"CSIRT-5/25"**
na adres:
Ministerstwo Infrastruktury
ul. Chałubińskiego 4/6; 00-928 Warszawa

Termin składania dokumentów: Termin składania dokumentów: 11.01.2026 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

DANE OSOBOWE - KLAUZULA INFORMACYJNA

(Aplikując, oświadczasz, że znana Ci jest treść informacji na temat przetwarzania danych osobowych w naborze)

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, z późn. zm.), informuję, że:

1) administratorem Pani/Pana danych osobowych jest Minister Infrastruktury z siedzibą w Warszawie, przy ul. Chałubińskiego 4/6, zwany dalej „Administratorem danych";
2) Pani/Pana dane osobowe przetwarzane są w celu przeprowadzenia naboru na wolne stanowisko pracy w Ministerstwie Infrastruktury;
3) podstawą przetwarzania Pani/Pana danych osobowych jest ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2025 r. poz. 277), ustawa z dnia 16 września 1982 o pracownikach urzędów państwowych (Dz. U. z 2023 r. poz. 1917, z późn.zm.) oraz udzielona przez Panią/Pana zgoda;
4) w zakresie informacji wskazanych w ogłoszeniu o naborze jako niezbędne, podanie danych jest wymagane do udziału w procesie naboru przez wskazane w klauzuli przepisy prawa. Ich niepodanie może uniemożliwić udział w procesie rekrutacji; Podanie danych innych niż wymagane, nie ma wpływu na proces rekrutacji i nie jest niezbędne;
5) Administrator danych przewiduje możliwość powierzenia przetwarzania danych innym podmiotom świadczącym na rzecz Administratora danych usługi z zakresu IT;
6) posiada Pani/Pan prawo do:
   - żądania dostępu do treści swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania,

- wniesienia sprzeciwu wobec przetwarzania danych osobowych w zakresie w jakim przetwarzanie nie wynika z obowiązku prawnego ciążącego na Administratorze danych,
- wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych;

7) Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu;
8) Pani/Pana dane osobowe będą przechowywane:
   a) 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);
   b) w przypadku złożenia aplikacji do naboru i nie wybrania Pani/Pana do zatrudnienia lub wygrania naboru, ale nie podjęcia zatrudnienia w MI, 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.
9) dane kontaktowe do Inspektora ochrony danych w Ministerstwie Infrastruktury: Inspektor ochrony danych, Ministerstwo Infrastruktury, ul. Chałubińskiego 4/6, 00-928 Warszawa, adres e-mail: inspektor.RODO@mi.gov.pl. Z Inspektorem ochrony danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania przez Administratora danych Pani danych osobowych oraz korzystania z praw związanych z tym przetwarzaniem danych.