

# Ministerstwo Rozwoju i Technologii w Warszawie

00-507 Warszawa Plac Trzech Krzyży 3/5

Ogłoszenie nr 163992 / 15.05.2026

## główny informatyk/główna informatyczka

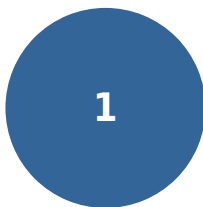
w Zespole Bezpieczeństwa i Ciągłości Działania IT w Departamencie Gospodarki Cyfrowej

#administracja publiczna #informatyzacja #IT

Pierwszeństwo dla osób z niepełnosprawnościami



Liczba stanowisk



Wymiar etatu



Status



Miejsce pracy



Ważne do



Wynagrodzenie zasadnicze



### Czym będziesz się zajmować

#### Osoba na tym stanowisku:

- Zarządza incydentami bezpieczeństwa, w tym: tworzy i doskonali proces obsługi incydentów (IRP, playbooki, RCA), identyfikuje, analizuje, eskaluje oraz koordynuje działania naprawcze, prowadzi dokumentację incydentów oraz rekomenduje działania zapobiegawcze, uczestniczy w symulacjach i testach planów reagowania.
- Monitoruje i wykrywa zagrożenia, w tym: projektuje i wdraża reguły detekcyjne w systemach SIEM, XDR, IDS/IPS, analizuje zachowania użytkowników i wykrywa techniki ataków (MITRE ATT&CK, UEBA), integruje dane telemetryczne i wzbogaca je informacjami z Threat Intelligence.
- Wdraża i utrzymuje rozwiązania bezpieczeństwa, w tym: instaluje, konfiguruje i zarządza systemami SIEM, SOAR, XDR, IDS/IPS, TIP, integruje systemy z infrastrukturą organizacji, tuninguje reguły i polityki.
- Zajmuje się automatyzacją i rozwojem narzędzi bezpieczeństwa, w tym: buduje playbooki i workflowy w systemach SOAR, współpracuje z zespołami developerskimi i DevSecOps w zakresie zabezpieczeń aplikacji.
- Bierze udział w projektach mi.in. realizowanych w ramach Funduszy Europejskich i Krajowego Planu Odbudowy.
- Bierze udział w przygotowywaniu i przeprowadzaniu postępowań o zamówienia publiczne w zakresie usług merytorycznie związanych z realizowanymi na stanowisku zadaniami.

### Kogo poszukujemy

#### Potrzebne ci będą (wymagania niezbędne)

- Wykształcenie: wyższe
- Doświadczenie zawodowe co najmniej 3 lata w obszarze cyberbezpieczeństwa lub IT (w tym w administrowaniu systemami operacyjnymi Windows/Linux i aplikacjami)

- Znajomość języka angielskiego na poziomie A2
- Posiadanie poświadczenia bezpieczeństwa do przetwarzania informacji niejawnych o klauzuli „tajne” lub zgoda na poddanie się procedurze sprawdzającej
- Znajomość zagadnień dotyczących bezpieczeństwa informacji i cyberbezpieczeństwa oraz ciągłości działania IT, w tym posiadanie wiedzy z obszaru cyberbezpieczeństwa odpowiadającego domenom wiedzy ujętym w obszarze certyfikacji CompTIA Security+
- Znajomość zagadnień w zakresie bezpieczeństwa przetwarzania i ochrony danych osobowych
- Znajomość podstawowych zagadnień z zakresu prawa zamówień publicznych
- Znajomość metodyki zarządzania projektami
- Praktyczna znajomość technik i standardów związanych z Threat Hunting
- Bardzo dobra znajomość narzędzi i technologii: SIEM, SOAR, XDR, IDS/IPS, Threat Intelligence, Deception
- Umiejętność wykorzystania języków skryptowych (Python, PowerShell) na poziomie umożliwiającym samodzielne tworzenie narzędzi automatyzujących
- Znajomość standardów i norm bezpieczeństwa m.in.: MITRE ATT&CK, OWASP, NIST 800 61 Rev. 3
- Organizacja pracy i orientacja na osiągnięcie celów, rzetelność, współpraca
- Komunikacja
- Wysoka kultura osobista
- Myślenie analityczne
- W służbie cywilnej nie może być zatrudniona osoba, która w okresie od dnia 22 lipca 1944 r. do dnia 31 lipca 1990 r. pracowała lub pełniła służbę w organach bezpieczeństwa państwa lub była 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 (nie dotyczy kandydatek/kandydatów urodzonych 1 sierpnia 1972 r. lub później). Osoba wybrana do zatrudnienia będzie musiała złożyć oświadczenie lustracyjne, jeśli urodziła się przed 1 sierpnia 1972 r.
- Posiadanie obywatelstwa polskiego
- Korzystanie z pełni praw publicznych
- Nieskazanie prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe

#### **Dodatkowym atutem będzie** (wymagania dodatkowe)

- Minimum 1 rok doświadczenia we wdrażaniu rozwiązań bezpieczeństwa na dużą skalę.
- Certyfikat z zakresu rozwiązań bezpieczeństwa w chmurze (np. AWS/Azure/GCP Security).
- Umiejętność analizy malware i digital forensics.

## **Co oferujemy**

- elastyczny czas pracy – możliwość rozpoczęcia pracy w godz. 7.00-9.00,
- częściowe wykonywanie pracy poza siedzibą urzędu (praca zdalna),
- dodatek za wysługę lat (powyżej 5 lat) od 5 do 20% wynagrodzenia w zależności od udokumentowanego stażu pracy,
- trzynaste wynagrodzenie,
- podwyższona kwota pracodawcy do Pracowniczych Planów Kapitałowych,
- przejrzyste kryteria awansowania i przyznawania nagród,
- atrakcyjny pakiet socjalny: bezzwrotna pomoc finansowa dla dzieci, dofinansowanie wypoczynku dla dzieci, dofinansowanie wypoczynku tzw. grusza, pożyczki pracownicze na preferencyjnych warunkach, dopłata do biletów na imprezy kulturalne oraz zajęcia sportowe, dofinansowanie zajęć sportowych – FitProfit oraz możliwość korzystania z systemu kafeteryjnego My Benefit,
- pakiet szkoleń adaptacyjnych dla nowych pracowników,
- gwarantowany program rozwoju zawodowego (m.in. szkolenia, dofinansowanie do nauki języków obcych i studiów podyplomowych),
- Indywidualny Program Rozwoju Zawodowego dla każdego pracownika,
- staż zagraniczny w Wydziale Ekonomiczno-Handlowym w Stałym Przedstawicielstwie RP przy UE w Brukseli,

- system poleceń pracy w MRIT z nagrodami dla zgłaszających pracowników,
- stojaki na rowery na terenie urzędu,
- stołówka pracownicza,
- praca w centrum Warszawy (w pobliżu znajduje się: stacja metra, stacja Veturilo, stacja PKP),
- możliwość wykupienia polisy na życie w preferencyjnej cenie.

## Dostępność

- Nasz urząd jest pracodawcą równych szans. Aplikacje rozważane są z równą uwagą bez względu na płeć, wiek, niepełnosprawność, rasę, narodowość, przekonania polityczne, przynależność związkową, pochodzenie etniczne, wyznanie, orientację seksualną czy też jakąkolwiek inną cechę prawnie chronioną.
- Jako osoba z niepełnosprawnością możesz skorzystać z pierwszeństwa w zatrudnieniu – złóż wówczas kopię dokumentu potwierdzającego niepełnosprawność.  
W miesiącu poprzedzającym datę upublicznienia ogłoszenia wskaźnik zatrudnienia osób niepełnosprawnych w urzędzie, w rozumieniu przepisów ustawy o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych, był mniejszy niż 6%.
- Do składania ofert zachęcamy również osoby ze szczególnymi potrzebami.
- Jako osoba ze szczególnymi potrzebami możesz je zgłosić na etapie składania dokumentów.
- Umożliwiamy osobom ze szczególnymi potrzebami korzystanie z własnych urządzeń i rozwiązań wspomagających pracę (np. pomoc asystenta lub trenera pracy).
- Dostosowujemy materiały używane podczas naboru do potrzeb osób ze szczególnymi potrzebami (np. większa czcionka w materiałach drukowanych).
- Zwiększamy czas poszczególnych metod i technik naboru dla osób ze szczególnymi potrzebami.

## Warunki pracy

Warunki dotyczące charakteru pracy na stanowisku i sposobu wykonywania zadań:

- Praca pod presją czasu
- Stres związany z koniecznością obsłużenia incydentów
- Obsługa klienta zewnętrznego
- Obsługa incydentów poza godzinami pracy urzędu - w przypadku incydentów pracownik musi być gotowy do dyżurów/pracy zdalnej lub stawienia się w urzędzie poza godzinami pracy
- Krajowe i zagraniczne wyjazdy służbowe - kilka razy w roku
- Reprezentowanie urzędu na zewnątrz

Opis dostępności budynku dla osób z niepełnosprawnością znajduje się na stronie Ministerstwa:

<https://www.gov.pl/web/rozwoj-technologie/warunki-pracy>

## Dodatkowe informacje

- Oświadczenia złóż zgodnie ze wzorem zamieszczonym na stronie:  
<https://www.gov.pl/web/rozwoj-technologie/pracuj-z-nami>
- Oświadczenia podpisz odręcznie i wstaw datę ich sporządzenia.
- Nie przesyłaj wszystkich dokumentów, które uznasz, że mogą Ci pomóc w naborze. Prześlij tylko te, których wymagamy lub zalecamy.
- Nie rozpatrzymy oferty, którą otrzymamy po terminie.
- Złóż dokumenty w języku polskim. Do dokumentów sporządzonych w języku obcym dołącz kopie ich tłumaczenia na

język polski sporządzone przez tłumacza przysięgłego.

- Dokumentem potwierdzającym wykształcenie jest kopia dyplomu lub zaświadczenie z uczelni.
- W przypadku ukończenia studiów wyższych na uczelni zagranicznej, prześlij kopię potwierdzenia uznania dyplomu przez Narodową Agencję Wymiany Akademickiej lub nostryfikacji dyplomu.
- Weryfikację wymagań formalnych przeprowadzamy na podstawie dokumentów wymienionych w części „Dokumenty i oświadczenia niezbędne”.
- Kompletna aplikacja to taka, która zawiera wszystkie wymagane dokumenty i oświadczenia.
- W swoim cv podaj numer telefonu i/lub adres poczty elektronicznej. Jeśli Twoja aplikacja spełni wymagania formalne, o kolejnym etapie naboru powiadomimy Cię telefonicznie lub mailowo.
- W CV opisz swoje doświadczenie zawodowe określając daty początkowe i końcowe oraz wykonywane czynności. Jeżeli w ogłoszeniu jest wymagana lub pożądana znajomość języka obcego określ w CV poziom jego znajomości.
- Oferty kandydatów, którzy nie zostaną zakwalifikowani z przyczyn formalnych oraz którym nie zaproponujemy zatrudnienia w danym naborze, zostaną zniszczone komisyjnie po zakończeniu rekrutacji.
- Zwróć uwagę na warunki pracy, które wskazaliśmy w ogłoszeniu – rzetelnie oceń, czy odpowiada Ci taka praca.
- W Ministerstwie Rozwoju i Technologii możesz zgłosić naruszenie prawa w trybie określonym w Wewnętrznej procedurze dokonywania zgłoszeń naruszeń prawa i podejmowania działań następczych w Ministerstwie Rozwoju i Technologii, stanowiącej Załącznik nr 1 do Zarządzenia nr 24 Ministra Rozwoju i Technologii z dnia 12 września 2024 r. w sprawie procedur zgłaszania informacji o naruszeniach prawa i podejmowania działań następczych w Ministerstwie Rozwoju i Technologii (Dz. Urz. Min. Roz. i Tech. poz. 26) Link do przepisów: <https://www.gov.pl/web/rozwoj-technologie/zglos-naruszenie-prawa>

### **Planujemy następujące metody/techniki naboru:**

1. weryfikacja formalna ofert kandydatów - etap obligatoryjny,
2. rozmowa kwalifikacyjna – etap obligatoryjny.

W zależności od wymagań określonych w ogłoszeniu możliwe są jeszcze dodatkowe etapy naboru. W procesie selekcji kandydatów stosujemy narzędzia takie jak: próbki pracy, sprawdzian wiedzy/ umiejętności w formie testu, pracy pisemnej, sprawdzian znajomości języka obcego, itp.

### **Twoja aplikacja musi zawierać (dokumenty niezbędne)**

- CV i list motywacyjny
- Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie wykształcenia
- Kopia poświadczenia bezpieczeństwa do przetwarzania informacji niejawnych o klauzuli „tajne” lub oświadczenie o wyrażeniu zgody na poddanie się procedurze sprawdzającej
- Oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych do celów rekrutacji
- 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 (nie dotyczy kandydatek/kandydatów urodzonych 1 sierpnia 1972 r. lub później)
- Oświadczenie o posiadaniu obywatelstwa polskiego
- Oświadczenie o korzystaniu z pełni praw publicznych
- Oświadczenie o nieskazaniu prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe

### **Dołącz, jeśli posiadasz (dokumenty dodatkowe)**

- Kopia dokumentu potwierdzającego niepełnosprawność - w przypadku kandydatek/kandydatów, zamierzających skorzystać z pierwszeństwa w zatrudnieniu w przypadku, gdy znajdą się w gronie najlepszych kandydatek/kandydatów
- Kopię certyfikatu z zakresu rozwiązań bezpieczeństwa w chmurze (np. AWS/Azure/GCP Security).

## Aplikuj do: 29 maja 2026

W formie papierowej w zamkniętej kopercie na adres: **Ministerstwo Rozwoju i Technologii**  
**Biuro Dyrektora Generalnego**  
**Plac Trzech Krzyży 3/5**  
**00-507 Warszawa**

**Kancelaria czynna w godz. 8.15-16.15**

**Aplikację możesz wystać też przez ePUAP lub na adres mailowy: [rekrutacja@mrit.gov.pl](mailto:rekrutacja@mrit.gov.pl) (plik nie może przekraczać 30 MB)**

**W liście motywacyjnym oraz w tytule wiadomości elektronicznej lub na kopercie wpisz numer naboru DGC-69**

Zapraszamy również do kontaktu telefonicznego: **w zakresie merytorycznym (22) 411 99 29, w zakresie procesu rekrutacyjnego (22) 411 99 48**

Więcej o pracy na stronie urzędu: <https://www.gov.pl/web/rozwoj-technologie/pracuj-z-nami>

- Dokumenty należy złożyć do: **29.05.2026**
- Decyduje data: **wpływu oferty do urzędu**
- Aplikując, oświadczasz, że znana Ci jest treść informacji na temat przetwarzania danych osobowych w naborze

### Przetwarzanie danych osobowych

#### DANE OSOBOWE - KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 Nr 119, str. 1 z późn. zm.) zwanego dalej RODO, informuję, że:

1. Administratorem Pani/Pana danych osobowych jest Minister Finansów i Gospodarki obsługiwany przez Ministerstwo Rozwoju i Technologii. Adres siedziby: Warszawa, Plac Trzech Krzyży 3/5. Kontakt do administratora: tel.: 222 500 123. Adres do doręczeń elektronicznych AE:PL-68477-29007-EFSHR-25. Adres skrytki na ePUAP: /MRPiT/SkrytkaESP.
2. Kontakt do Inspektora Ochrony Danych: [iod@mrit.gov.pl](mailto:iod@mrit.gov.pl).

Pełna informacja dotycząca zasad przetwarzania danych osobowych, w tym przysługujących kandydatom na wolne stanowiska pracy w służbie cywilnej uprawnień, dostępna jest na stronie internetowej pod adresem: <https://www.gov.pl/web/rozwoj-technologie/jak-przetwarzamy-twoje-dane-osobowe>