**Widełki wynagrodzeń dla specjalistów od cyberbezpieczeństwa wzrosły nawet o 5 tys. zł brutto od początku roku. Najnowsza analiza**

**Mediany górnych widełek wynagrodzeń oferowanych ekspertom od cyberbezpieczeństwa są obecnie najwyższe od początku 2024 roku i sięgają nawet 30,2 tys. zł netto (+ VAT) na kontrakcie B2B. Rośnie też zapotrzebowanie na specjalistów z tej branży na rynku pracy – oferty z tej kategorii stanowią już 2,5 proc. wszystkich ogłoszeń na portalu No Fluff Jobs. W wymaganiach rzadko pojawiają się kompetencje miękkie, a tylko w co 10. ofercie od kandydatów i kandydatek oczekuje się wyższego wykształcenia. Najczęściej pojawiające się wymagania to znajomość Pythona i rozwiązań chmurowych do zarządzania infrastrukturą IT.**

Rosną wynagrodzenia dla specjalistów zajmujących się cyberbezpieczeństwem. Jak wynika z **najnowszej analizy danych No Fluff Jobs**, polskiego portalu z ogłoszeniami, który od 11 lat ułatwia kandydatom i kandydatkom znalezienie pracy dopasowanej do ich oczekiwań finansowych, **mediany dolnych i górnych widełek wynagrodzeń w tej specjalizacji wynoszą obecnie**:

l **23,5-30,2 tys. zł** netto (+ VAT) na kontrakcie B2B,

l **20-25 tys. zł** brutto na umowie o pracę.

Dla porównania, na początku bieżącego roku wynosiły one 21-27 tys. zł netto (+ VAT) na kontrakcie B2B i 15-21,5 tys. zł brutto na umowie o pracę. W 2024 r. najwyższy poziom osiągnęły pod koniec drugiego kwartału: 24,2-28,5 tys. zł netto (+ VAT) na kontrakcie B2B i 18-25 tys. zł brutto na umowie o pracę.

**Ofert pracy dla ekspertów cyberbezpieczeństwa coraz więcej**

Od początku 2024 roku systematycznie rośnie **zapotrzebowanie na specjalistów zajmujących się kwestiami cyberbezpieczeństwa w firmach** – obecnie ofert pracy w tym obszarze jest dwukrotnie więcej niż jeszcze w 1. kwartale 2025 roku. Całościowo, ogłoszenia z tej kategorii stanowią 2,5 proc. wszystkich ofert opublikowanych na No Fluff Jobs.

**Najczęściej pojawiające się stanowiska to:**

l inżynier ds. bezpieczeństwa lub cyberbezpieczeństwa (Security / Cybersecurity Engineer),

l inżynier ds. bezpieczeństwa aplikacji (AppSec Engineer),

l inżynier ds. bezpieczeństwa chmury (Cloud Security Engineer),

l inżynier SecOps (Security Operations),

l analityk SOC (Security Operations Center).

*Globalny rozwój technologii sprzyja też rozwojowi zagrożeń, więc to nie przypadek, że firmy szukają fachowców od cyberbezpieczeństwa. Ma to związek z sytuacją geopolityczną na świecie – według najnowszych analiz w Europie co tydzień dochodzi do ponad 1,5 tysiąca ataków na firmy i instytucje. Polska jest na nie narażona szczególnie – według danych z pierwszego półrocza, w naszym kraju było najwięcej ataków ransomware na świecie. W kolejnych latach znaczenie stanowisk odpowiedzialnych za przeciwdziałanie zagrożeniom będzie tylko rosło, więc kluczowa będzie rekrutacja wykwalifikowanych osób* – **mówi Tomasz Bujok, CEO No Fluff Jobs**.

**Kompetencje miękkie i dyplom? Rzadko wymagane**

Stosunkowo rzadko w ogłoszeniach o pracy w sektorze cyberbezpieczeństwa wspomina się o **kompetencjach miękkich** – tylko w 12 proc. wymaga się umiejętności komunikacyjnych, w 7 proc. mówi się o zdolności zarządzania ryzykiem, a w 3 proc. o umiejętnościach analitycznych. Tylko w co 10. ofercie pracy od kandydatów i kandydatek wymaga się wyższego wykształcenia.

Praca w cyberbezpieczeństwie jest na tyle zróżnicowana, że nie występuje tu jedno kluczowe wymaganie, jak w kilku innych gałęziach IT. Najczęściej pojawia się znajomość języka Python, ale wymóg ten występuje w niecałej ⅕ ogłoszeń o pracy z tego sektora. Od kandydatów i kandydatek często oczekuje się również znajomości różnych rozwiązań chmurowych do zarządzania infrastrukturą IT, jak AWS (Amazon Web Services) czy Azure (po ok. 15 proc.). Również w 15 proc. ofert wymaga się znajomości wytycznych NIST (National Institute of Standards and Technology) – amerykańskiej agencji rządowej zajmującej się m.in. opracowywaniem standardów i wytycznych dotyczących bezpieczeństwa cybernetycznego, a co dziesiąta oferta za główne wymaganie podaje też znajomość ISO.