Górnośląskie Centrum Medyczne im. prof. Leszka Gieca Śląskiego Uniwersytetu Medycznego w Katowicach

Administrator Systemów Informatycznych w zakresie bezpieczeństwa systemów informatycznych

Zakres obowiązków:

- Określanie wymagań bezpieczeństwa dla projektowanych rozwiązań IT
- Opiniowanie nowych rozwiązań, inicjatyw oraz zmian w systemach informatycznych w zakresie bezpieczeństwa IT
- Opracowanie procesów i zaleceń w obszarze bezpieczeństwa IT
- Identyfikowanie i analizowanie zdarzeń oraz incydentów bezpieczeństwa
- Analizowanie podatności środowiska IT, w tym wspieranie procesów skanowania podatności infrastruktury oraz testów penetracyjnych
- Doradztwo w zakresie zabezpieczenia infrastruktury IT
- Monitorowanie i raportowanie stanu bezpieczeństwa zarządzanych systemów
- Współpraca z wykonawcami w zakresie cyberbezpieczeństwa
- Wdrażanie szkoleń i kampanii informacyjnych z zakresu cyberbezpieczeństwa
- Monitorowanie trendów związanych cyberbezpieczeństwem oraz identyfikacja zagrożeń
- Przeprowadzanie audytów bezpieczeństwa w organizacji (analiza, raportowanie, proponowanie rekomendacji)
- Sporządzanie i aktualizacja dokumentacji technicznej utrzymywanych i tworzonych systemów

Wymagania:

- Samodzielne, pomysłowe, sumienne i nastawione na kreatywne/ nieszablonowe rozwiązywanie problemów oraz wykazanie się doświadczeniem w jednym lub wielu z poniższych obszarów:
- Posiadanie doświadczenia lub pasjonowania się obszarem bezpieczeństwa IT;
- Posiadanie praktycznej znajomości standardów ISO w zakresie bezpieczeństwa informacji oraz utrzymywania systemów zarządzania oraz standardów cyberbezpieczeństwa
- Doświadczenie w analizie ryzyka, zagrożeń, podatności i zdarzeń

- Rozwiązywanie oraz analizowanie złożonych problemów z zakresu cyberbezpieczeństwa
- Znajomość standardów bezpiecznej konfiguracji systemów teleinformatycznych (minimum systemy operacyjne Linux/Windows, serwery WWW, bazy danych)
- Znajomość zasady działania sieci, protokołów i usług sieciowych pozwalająca na analizie zagrożeń sieciowych
- Posiadanie praktycznej znajomości mechanizmów bezpieczeństwa systemów IT, w tym systemów zabezpieczeń FW/IPS/WAF/SIEM/DLP/Antimalware
- Posiadanie wiedzy z zakresu hardeningu systemów operacyjnych i infrastruktury IT
- Znajomość popularnych ataków na aplikacje webowe, mobilne, systemy operacyjne, infrastrukturę
- Posiada umiejętność przeprowadzania testów penetracyjnych
- Znajomość języka angielskiego w mowie i piśmie mile widziane
- Certyfikaty zawodowe potrwiedzające posiadane kompetencje

Kandydaci zobowiązani są do dostarczenia następujących dokumentów:

- Życiorysu (CV);
- Listu motywacyjnego;
- Kopii dyplomów, świadectw lub innych dokumentów potwierdzających posiadane kwalifikacje;
- Podpisanego oświadczenia:
  „Zgodnie z art. 6 ust. 1 lit. a ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) wyrażam zgodę na przetwarzanie moich danych osobowych dla potrzeb aktualnej i przyszłych rekrutacji”

Ww. dokumenty należy przesłać drogą elektroniczną na adres: kadry@gcm.pl
Telefon kontaktowy: (32) 359 – 85-56
Zastrzegamy sobie prawo do kontaktu tylko z wybranymi osobami.

Klauzula informacyjna dla kandydatów do pracy

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 r. informuję, iż:

1) administratorem Pani/Pana danych jest Górnośląskie Centrum Medyczne im. prof. Leszka Gieca Śląskiego Uniwersytetu Medycznego w Katowicach (dalej „GCM"),
2) kontakt z Inspektorem Ochrony Danych – iod@gcm.pl,
3) 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.,
4) Pani/Pana dane osobowe przechowywane będą przez okres tej i przyszłych rekrutacji,
5) 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,
6) ma Pan/ Pani prawo wniesienia skargi do organu nadzorczego, posiadanie danych osobowych jest obligatoryjne w oparciu o przepisy prawa, a w pozostałym zakresie jest dobrowolne.