Nazwa: Specjalista do spraw cyberbezpieczeństwa

Kod: 252902

Synteza: Specjalista do spraw cybebezpieczeństwa zajmuje się zarządzaniem bezpieczeństwem systemów teleinformatycznych przez wdrażanie i rozwój zabezpieczeń technicznych i informatycznych; odpowiada za aktualizację reguł bezpieczeństwa zaimplementowanych w systemach teleinformatycznych oraz dostosowanie reguł do aktualnego stanu zagrożeń; przeprowadza analizy w zakresie bezpieczeństwa teleinformatycznego oraz zajmuje się tworzeniem, wdrożeniem i aktualizowaniem procedur dotyczących postępowania w celu zapewnienia bezpieczeństwa teleinformatycznego.

Zadania zawodowe:

- utrzymywanie i rozwój systemów bezpieczeństwa teleinformatycznego;
- formułowanie wymagań bezpieczeństwa dla projektów i rozwiązań wdrażanych w organizacji w zakresie bezpieczeństwa teleinformatycznego;
- planowanie i wdrażanie rozwiązań z zakresu cyberbezpieczeństwa;
- opracowywanie procedur awaryjnych, scenariuszy reakcji na ataki cybernetyczne;
- obsługiwanie incydentów oraz prowadzenie analizy powłamaniowej do systemów teleinformatycznych;
- tworzenie polityk, standardów i procedur bezpieczeństwa teleinformatycznego, w tym sprawowanie nadzoru nad aktualnością procedur "Disaster Recovery / Business Continuity" oraz ścisła współpraca z Pełnomocnikiem ds. Ochrony Informacji Niejawnych w zakresie aktualizacji polityki bezpieczeństwa wdrożonej w organizacji;
- programowanie systemów w językach skryptowych, tj.: perl, bash, python lub innych językach wysokiego poziomu bezpieczeństwa teleinformatycznego;
- konfigurowanie i zarządzanie bezpieczeństwem aktywnych urządzeń sieciowych, systemu pocztowego oraz stacjami roboczymi poprzez Active Directory;
- obsługa systemów bezpieczeństwa, tj.: IDS/IPS, FW, AV, SIEM, LM, NAC, FDE, DLP, protokołów sieciowych ISO1-7, serwerów Unix / Linux, Microsoft oraz tworzenie zapytań SQL;
- zarządzanie powierzonymi kluczami systemowymi bezpieczeństwa teleinformatycznego, wykonywanie backupu i archiwizacji;
- monitorowanie stanu bezpieczeństwa poszczególnych elementów systemów teleinformatycznych, w tym przeglądanie logów i informacji powstałych w narzędziach monitorujących bezpieczeństwo systemów informatycznych;
- przeprowadzanie audytów i testów bezpieczeństwa systemów teleinformatycznych;
- identyfikowanie luk w zabezpieczeniach systemów teleinformatycznych, analizowanie ryzyka i wykrywanie ataków hakerskich czy innych incydentów;

	• prowadzenie analiz i przedkładanie raportów i wniosków w zakresie bezpieczeństwa teleinformatycznego, w tym niezwłoczne raportowanie wykrytych incydentów oraz uruchamianie alertów w wypadku zidentyfikowania zagrożeń w środowisku teleinformatycznym; • opiniowanie architektury systemów ICT pod kątem bezpieczeństwa teleinformatycznego; • wspieranie innych jednostek organizacyjnych, w zakresie bezpieczeństwa teleinformatycznego poprzez m.in. udział w projektach i wdrożeniach systemów teleinformatycznych.
Dodatkowe zadania zawodowe:	• definiowanie parametrów (zmiennych systemowych) w systemach teleinformatycznych i ich implementowanie przy współpracy z administratorami systemów teleinformatycznych oraz z wykonawcami i użytkownikami oprogramowania.