IstroSec

Arkusz danych

Główny inspektor bezpieczeństwa teleinformatycznego (CISO) jako usługa

Jeśli w Twojej firmie nie ma głównego inspektora ds. bezpieczeństwa teleinformatycznego (CISO), który nadzoruje ogólne zarządzanie bezpieczeństwem teleinformatycznym, odpowiedzialna za bezpieczeństwo teleinformatyczne staje się inna osoba, jak np. dyrektor ds. technicznych (CTO). Problem jednak polega na tym, że głównym obowiązkiem CTO jest zapewnienie sprawnego działania całego IT w firmie. W związku z tym może nie wystarczyć czasu i zasobów na bezpieczeństwo teleinformatyczne, a w niektórych przypadkach może nawet wystąpić konflikt interesów między celami bezpieczeństwa a celami operacji IT.

Dlaczego możesz potrzebować CISO jako usługa?

- Brak zasobów do zatrudnienia pełnoetatowego CISO
- Okres przejściowy przed zatrudnieniem nowego CISO
- Doradztwo i szkolenie mniej doświadczonych CISO
- Zgodność z wymogami regulacyjnymi i normatywnymi

Dlaczego IstroSec?

Łącznie ponad 70 lat doświadczenia

Dostęp do ekspertów ze wszystkich dziedzinach bezpieczeństwa informacji, w tym testerów penetracyjnych, analityków kryminalistycznych, analityków złośliwego oprogramowania, trenerów i nie tylko

Systematyczna poprawa bezpieczeństwa informacji według frameworków wzbogaconych doświadczeniem ekspertów **Istro**Sec z zaawansowanymi incydentami bezpieczeństwa

Zapewniając zgodność z normami i przepisami bezpieczeństwa, eksperci **Istro**Sec działają zarówno w administracji publicznej (dyrektywa NIS, RODO i inne) jak i w sektorze prywatnym (ISO 27001, NIST, HIPAA i inne)

> *Skorzystaj w pełni z CISO jako usługa, dostosowując ją do swoich konkretnych potrzeb.*

IstroSec może pomóc w następujących kwestiach:

- Ogólne zarządzanie i kierowanie programem bezpieczeństwa teleinformatycznego
- Zapewnienie zgodności z wymogami regulacyjnymi, normatywnymi i umownymi
- Opracowywanie i wdrażanie procesów bezpieczeństwa, polityk, wytycznych i procedur
- Planowanie i prowadzenie programów edukacyjnych i podnoszących świadomość
- Ćwiczenia z bezpieczeństwa cybernetycznego
- Zarządzanie zasobami bezpieczeństwa teleinformatycznego
- Bezpieczeństwo fizyczne
- Zarządzanie bezpieczeństwem informacji i ryzykiem osób trzecich
- Kontrola dostępu
- Bezpieczeństwo operacji IT
- Zarządzania incydentami związanymi z bezpieczeństwem teleinformatycznym
- Testy bezpieczeństwa
- Przygotowanie do audytu wewnętrznego lub zewnętrznego
- Bezpieczeństwo w tworzeniu oprogramowania

IstroSec

Arkusz danych

Dlaczego my?

Doświadczenie i wiedza

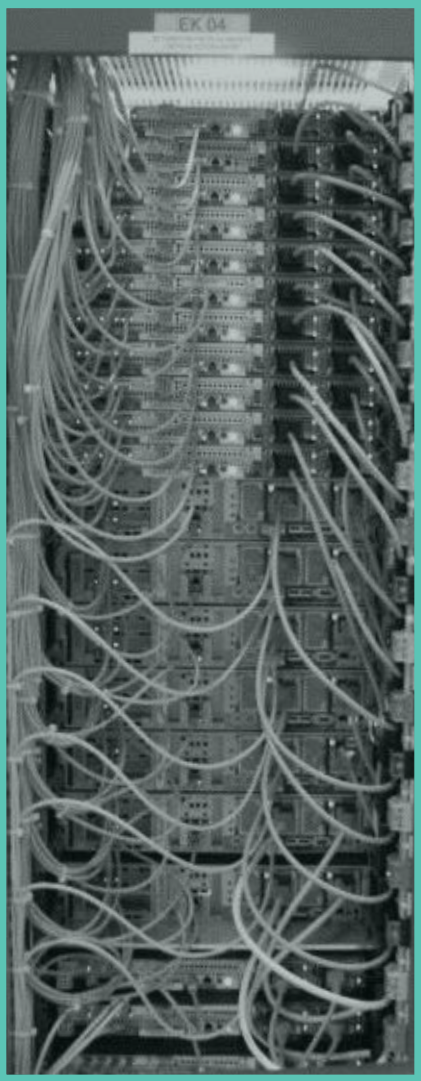
Specjaliści **Istro**Sec mają doświadczenie we wdrażaniu i zarządzaniu bezpieczeństwem informacji zgodnie z większością ram bezpieczeństwa teleinformatycznego. Znają taktykę, techniki i procedury atakujących oraz posiadają niezbędną wiedzę, aby skutecznie i płynnie wdrażać procesy bezpieczeństwa teleinformatycznego do twoich procesów biznesowych.

Specjalistyczna wiedza z zakresu zarządzania

Specjalistyczna wiedza w zakresie zarządzania bezpieczeństwem teleinformatycznym oraz wielu innych obszarach, takich jak reakcja na zdarzenia, analiza kryminalistyczna czy światowej klasy analiza złośliwego oprogramowania, którą wielokrotnie wykazali się nasi specjaliści podczas radzenia sobie z cyberatakami wspieranymi przez państwo, atakami na organizacje z listy Fortune 500, a także udział czterech ekspertów **Istro**Sec w zwycięstudniaskim zespole ćwiczenia Locked Shields 2016.

Certyfikowani profesjonaliści

Eksperci **Istro**Sec są również posiadaczami uznanych na całym świecie certyfikatów w tych dziedzinach. Posiadamy certyfikaty takie jak Certified Information Systems Security Professional (CISSP), Certified Information System Auditor (CISA), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), Certified Reverse Engineering Analyst (CREA) i inne.



Studium przypadku

Rodzaj firmy: Mała kancelaria prawna

Świadczone usługi: CISO jako usługa

Rozwiązanie: Stworzenie programu bezpieczeństwa teleinformatycznego

Klient poprosił o zaprojektowanie i wdrożenie programu bezpieczeństwa teleinformatycznego, który spełniłby wszystkie istotne zobowiązania prawne i umowne. Jako podstawowe ramy wybrano ISO 27001. Kancelaria posiadała już pewne kontrole procesów, dlatego dokonano wstępnej oceny luk w stosunku do wymagań bezpieczeństwa nałożonych na klienta. Zidentyfikowano i wdrożono brakujące kontrole. Program zarządzania ryzykiem został stworzony w celu identyfikacji i zarządzania pozostałymi zagrożeniami wraz z programem świadomości bezpieczeństwa dla pracowników.

Rodzaj firmy: Średniej wielkości organ administracji publicznej

Świadczone usługi: CISO jako usługa

Rozwiązanie: CISO klienta opuścił firmę i potrzebny był tymczasowy wirtualny CISO do sterowania programem bezpieczeństwa teleinformatycznego.

Klient przeprowadzał zmiany w swoim programie bezpieczeństwa teleinformatycznego, a CISO odszedł w trakcie tego procesu. W związku z tym zatrudniono wirtualnego CISO, aby pomóc pokierować projektem podczas przejmowania obowiązków byłego CISO. W rezultacie zrealizowano zmodernizowany program bezpieczeństwa teleinformatycznego wraz z zaktualizowanymi procesami, politykami i procedurami przy jednoczesnym zapewnieniu ciągłości działania w zakresie bezpieczeństwa teleinformatycznego. Ponadto wirtualny CISO pomógł personelowi w zatrudnieniu nowego stałego CISO, zapewnił wstępne szkolenie i przekazał zarządzanie programem.