SOC Factory

DORA NIS2 KSC

Made in Poland

SecurityBox to kompleksowe podejście do monitorowania oraz analizy zdarzeń bezpieczeństwa IT w celu wykrywania i eliminacji zagrożeń oraz incydentów związanych z cyberbezpieczeństwem. Jest implementacją koncepcji **Security Operations Center (SOC)** rozszerzonej o badanie zgodności z regulacjami w zakresie cyberbezpieczeństwa (**Compliance**) **NIS2/DORA/ISO27001**. Rozwiązanie to wykorzystuje najnowsze narzędzia technologiczne open source oraz umożliwia właściwe zdefiniowanie krytycznych procesów organizacji.

Sankcje grożące w przypadku braku spełnienia wymagań regulacyjnych

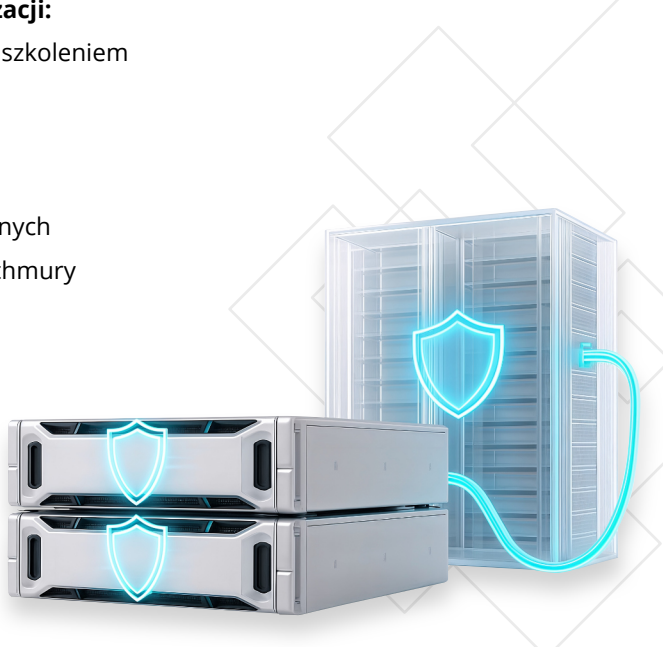
DORA – kara: 1% dziennego obrotu za dzień naruszenia (max 6 mies.); organ: KNF/inny sektorowy; sankcje: zakaz dla dostawcy ICT, obowiązkowe audyty, publiczne ogłoszenie.

NIS2 – kara: 10 mln EUR lub 2% obrotu (kluczowe) / 7 mln EUR lub 1,4% (ważne); organ: minister + CSIRT; sankcje: zawieszenie kadry, obowiązkowe dodatkowe środki.

KSC – kara: 1 mln zł (podmiot) / 200 tys. zł (kierownik); organ: minister + CSIRT; sankcje: nakaz wdrożenia środków, kontrole, zgłoszenie do prokuratury.

Najważniejsze korzyści z wdrożenia SecurityBox w Twojej organizacji:

- Zgodność z DORA / NIS2 / KSC – kompleksowe rozwiązanie wraz ze szkoleniem
- Lokalne wdrożenie on premise dostarczane razem ze sprzętem
- Operacyjna zgodność z ISO i NIST w ramach jednej platformy
- PLUG & SECURE – uruchomienie SOC nawet w ciągu 14 dni
- Jednorazowy koszt wdrożenia – zero dodatkowych kosztów licencyjnych
- Threat Inteligence jako lokalny silnik AI – bez wysyłania danych do chmury
- Wykorzystanie matryc MITRE ATT&CK
- Prioretyzacja incydentów i podatności



Jesteśmy członkiem Polskiego Klastra Cyberbezpieczeństwa

#CyberMadeInPoland

Powered by dogs.pl

SecurityBox to Security Operations Center (SOC) wzbogacony o narzędzia do zapewnienia zgodności z regulacjami NIS2 i DORA. Rozwiązanie jest modułowe i można je elastycznie dopasować do potrzeb każdej organizacji.

Oferowane pakiety

Essential

- System zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM)
- Automatyzacja (SOAR)
- Ewidencja zasobów (Digital Assets)
- Mapa sieci (Network Mapping)
- Zarządzanie ryzykiem (Risk Registry)
- Zarządzanie podatnościami (Vulnerability Platform)
- Planowanie reakcji (Mitigation Plan)

Advanced

- Matryca taktyk MITRE ATT&CK
- CTI (Threat Intelligence) zintegrowane z AI
- Zgodność z ISO/NIST
- Integracja z NASK

Pakiet wsparcia

- Wsparcie techniczne
- Konsultacje audytora
- Wsparcie merytoryczne w zakresie wypełnienia zgodności (Compliance)
- Możliwość zapewnienia vCISO (Virtual Chief Information Security Officer)
- Zewnętrzny zespół CSIRT

Realizacja usługi przebiega w trzech jasno określonych etapach:

ETAP I
Audyt infrastruktury

Audyt i zebranie informacji na temat posiadanych systemów IT

ETAP II
Implementacja

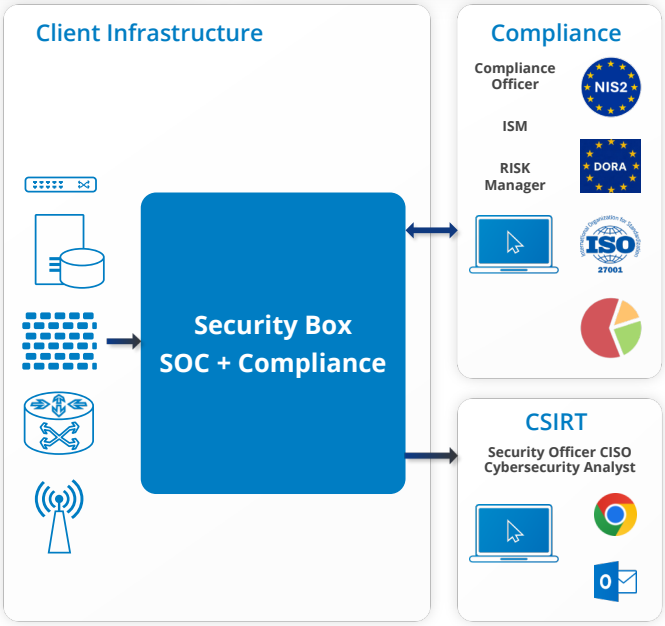
Instalacja i konfiguracja środowiska SOC

ETAP III
Szkolenie zespołu

Dokumentacja i przeszkolenie zespołu z obsługi SOC

Moduły rozwiązania

1. Monitorowanie (SIEM) - DORA (art. 8-12) i NIS2 (art. 21)
2. Automatyzacja (SOAR) - DORA (art. 11-12), NIS2 (procedur obsługi incydentów)
3. Wykrywanie i reagowanie (Threat Intelligence) DORA (art. 45)
4. Ewidencja zasobów (Asset Inventory) - DORA (art. 8)
5. Zarządzanie ryzykiem (Risk Registry)
6. Zarządzanie podatnościami (Vulnerability Platform)
7. Planowanie reakcji (Mitigation Plan)
8. Integracja z NASK CERT / CSIRT - DORA (art. 45)
9. Zautomatyzowany audyt zgodności ISO / NIST (Compliance)



www.SOCfactory.com

www.dcs.pl

Powered by dcs.pl

dcs.pl Sp. z o.o, ul. Puławska 303, 02-785 Warszawa
+48 22 5486000, info@dcs.pl, www.dcs.pl