CyberBezpieczna Infrastruktura Krytyczna

Model usługowy ComCERT:
ochrona kluczowych obszarów cyberbezpieczeństwa infrastruktury krytycznej

Energetyka | Transport | Woda i kanalizacja | Gospodarka ściekowa

comCERT
We Think Cybersecurity

Energetyka | Transport | Zaopatrzenie w wodę | Gospodarka ściekowa

Poznaj rozwiązania, które chronią ciągłość działania i bezpieczeństwo infrastruktury krytycznej.

vCISO

- Wsparcie strategiczne i operacyjne w zarządzaniu cyberbezpieczeństwem.
- Zapewnienie zgodności z wymaganiami regulacyjnymi (NIS2, uKSC, ISO 27001) w IK.
- Ekspercka wiedza ComCERT dostępna w elastycznym modelu.

Cyberhigiena

- Ukierunkowana edukacja i budowanie świadomości operatorów OT/ICS.
- Promowanie dobrych praktyk i bezpiecznych nawyków.
- Stała ocena poziomu cyberodporności pracowników.

comCERT

CyberBezpieczna Infrastruktura Krytyczna

C3TI

- Dostarcza informacji o wyciekach danych w sieci DarkWeb.
- Wspiera wczesne ostrzeganie i analizę zagrożeń.
- Dostępne w formie aplikacji webowej. Możliwość integracji poprzez API.

SOCaaS

- Monitoring 24/7 - wczesna detekcja i ciągła obserwacja systemów OT/ICS.
- Reakcja na incydenty w infrastrukturze przemysłowej w ramach 1, 2 i 3 Linii wsparcia.
- Elastyczny model świadczenia usługi – dopasowany do potrzeb Twojej organizacji.

Nasze usługi eliminują trzy kluczowe luki, które wpływają na poziom bezpieczeństwa infrastruktury krytycznej:

Luka kompetencyjna:

Brak kluczowych kompetencji z zakresu cyberbezpieczeństwa niezbędnych do rozwoju i wdrażania zmian w sektorze infrastruktury krytycznej.

Luka utylizacyjna:

Ograniczona możliwość realizacji funkcji cyberbezpieczeństwa z powodu przeciążenia zespołu innymi priorytetami – mimo posiadanych kompetencji.

Luka technologiczna:

Braki w architekturze komponentów cyberbezpieczeństwa, które uniemożliwiają wdrażanie innowacji i skuteczne spełnianie wymagań regulacyjnych.

www.comcert.pl

ComCERT

vCISO – Wirtualny Chief Information Security Officer

Usługa vCISO opiera się na trzech filarach, które wspierają budowę odpornej, zgodnej i świadomej organizacji:

Zarządzanie obszarem cyberbezpieczeństwa w środowiskach OT/ICS – wyznaczanie celów, priorytetów i kierunków działań, rekomendacje modeli organizacyjnych oraz rozwój cyberbezpieczeństwa.

Ocena stanu cyberbezpieczeństwa – przeprowadzanie analiz ryzyka, weryfikacja zgodności z regulacjami, przeglądy konfiguracji, ocena efektywności wdrożonych zabezpieczeń.

Operacyjność cyberbezpieczeństwa – wsparcie działań bieżących, zarządzanie zmianami w konfiguracji zabezpieczeń, remediacja oraz koordynacja z interesariuszami.

vCISO to dostęp do wiedzy strategicznej, technicznej i regulacyjnej – na żądanie, w modelu elastycznym, skalowalnym i dostosowanym do potrzeb Twojej infrastruktury i systemów przemysłowych.

ComCERT Cyber Threat Intelligence – C3TI

C3TI to platforma stworzona do aktywnego wspierania organizacji w identyfikacji, analizie i przeciwdziałaniu zagrożeniom cybernetycznym **w czasie rzeczywistym** w infrastrukturze krytycznej, poprzez:

Automatyczne wykrywanie zagrożeń oraz analiza danych z Dark Web i cyberforów (phishing, kampanie malware, wycieki, kompromitacje kont, błędy konfiguracyjne).

Aplikacja webowa i funkcjonalne moduły: Threat Radar, Feedy IoC, IT Visibility, Incydenty, Raporty i Statystyki. Integracja z systemami Twojej organizacji poprzez API.

Dynamiczna analiza ryzyka i wsparcie decyzyjne dla zespołów SOC/CSIRT oraz kadry zarządzającej.

C3TI wspiera wczesne wykrywanie i analizę zagrożeń – automatyzuje zbieranie i przetwarzanie informacji, zwiększając skuteczność ochrony infrastruktury.

Energetyka | Transport | Zaopatrzenie w wodę | Gospodarka ściekowa

Security Operations Center as a Service (SOCaaS)

SOC ComCERT to kompleksowa usługa monitorowania, wykrywania i reagowania na incydenty bezpieczeństwa w infrastrukturze krytycznej w całości realizowana przez doświadczony zespół analityków bezpieczeństwa.

- Monitorowanie systemów i infrastruktury IT w trybie 24/7/365. Obsługa zgłoszeń incydentów, korelacja zdarzeń i klasyfikacja zagrożeń.
- Wsparcie na poziomach L1, L2 oraz L3 – w zależności od złożoności incydentu. Koordynacja działań naprawczych i eskalacyjnych.
- Elastyczne modele usług: tryb ciągły lub dyżury.

Dzięki usłudze SOC od ComCERT Twoje systemy przemysłowe są stale monitorowane, a incydenty obsługiwane profesjonalnie, z natychmiastową reakcją i zgodnie z najlepszymi praktykami.

Cyberhigiena i budowanie świadomości

Zwiększenie poziomu bezpieczeństwa organizacji nie jest możliwe bez świadomego i przygotowanego zespołu.
Dlatego oferujemy systemowe wsparcie w kształtowaniu kultury cyberbezpieczeństwa dla zespołów OT.

- Diagnoza poziomu wiedzy i ryzyk – ocena gotowości pracowników do reagowania na zagrożenia.
- Edukacja dopasowana do roli i potrzeb – szkolenia, rekomendacje i dobre praktyki bezpieczeństwa.
- Wzmocnienie pierwszej linii obrony – świadomi operatorzy i inżynierowie wspierający politykę bezpieczeństwa organizacji.

www.comcert.pl

Energetyka | Transport | Zaopatrzenie w wodę | Gospodarka ściekowa

Kluczowe korzyści dla podmiotów infrastruktury krytycznej.

Wiedza i kompetencje na żądanie, bez stałych kosztów kadrowych.

Lepsze decyzje – oparte na danych i analizie zagrożeń.

Spójne zarządzanie ryzykiem i bezpieczeństwem w całej organizacji.

Monitoring 24/7 i szybka reakcja na incydenty.

Zgodność z regulacjami (NIS2, uKSC, KRI, ISO 27001).

Oszczędność czasu i zasobów – skupienie na głównej działalności.

Wzmocniona cyberodporność – strategiczna i operacyjna.

Zaufanie interesariuszy – potwierdzone dojrzałością bezpieczeństwa.

Czy Państwa infrastruktura jest gotowa na aktualne zagrożenia cybernetyczne?

Opowiedz mi o potrzebach swojej organizacji, przygotuję najlepsze rozwiązanie.

Skontaktuj się ze mną w celu umówienia konsultacji:

Marcin.matusiak@comcert.pl
+48 22 112 06 83
www.comcert.pl