Rozwiń kluczowe umiejętności cyberbezpieczeństwa

CYRUS to zestaw spersonalizowanych, dopasowanych do sektora szkoleń w miejscu pracy, zaprojektowanych dla firm z branży **transportu**, **produkcji** oraz **MŚP**. Stawiamy na realne kompetencje: krótkie bloki wiedzy + ćwiczenia, które od razu wdrożysz w swojej organizacji.

Co zyskasz jako uczestnik?

1

Praktyka ponad teorię

Ćwiczenia, scenariusze, checklisty do użycia „od dziś".

2

Konkrety dla Twojego sektora

Przykłady i rozwiązania dopasowane do transportu, produkcji i MŚP.

3

Zgodność z polskimi przepisami

m.in.
KSC i RODO.

4

Odporność organizacji

Lepsza ochrona danych i szybsza reakcja na incydenty = mniejsze ryzyko przestojów.

5

Udział bezpłatny

Dzięki współfinansowaniu ze środków UE oraz budżetu państwa.

FREE

Głos z praktyki

Świetne szkolenie! Dobre wprowadzenie i dużo realnych przykładów. Dziękuję za obszerną wiedzę! Na pewno się przyda.

— **Specjalista bezpieczeństwa informacji**

Pakiet szkoleń CYRUS

Podstawy cyberbezpieczeństwa

Dla pracowników z dostępem do sieci i danych (IT, administracja, bezpieczeństwo, zarządzanie, produkcja).

O rozpoznawaniu najczęstszych zagrożeń (phishing, ransomware, inżynieria społeczna), higienie haseł, bezpiecznym przeglądaniu i identyfikacji podejrzanych wiadomości/sprzętu.

Kluczowa korzyść: szybki wzrost świadomości i bezpiecznych nawyków w całej firmie.

Poziom: początkujący

Szyfrowanie danych

Dla osób z podstawami IT, chcących bezpiecznie chronić dane w spoczynku i w transmisji.

O podstawach kryptografii, metodach symetrycznej/asymetrycznej/hybrydowej, zarządzaniu kluczami, szyfrowaniu dysków, TLS/SSL, VPN, komunikacji end-to-end.

Kluczowa korzyść: właściwe dobranie i wdrożenie szyfrowania w procesach firmy

Poziom: średniozaawansowany

Ransomware

Dla zespołów IT/OT, administracji i bezpieczeństwa w organizacjach narażonych na ataki.

O mechanizmach infekcji (phishing, luki), modelach (w tym RaaS), zapobieganiu, kopiach zapasowych, procedurach reakcji i odzyskiwaniu danych krok po kroku.

Kluczowa korzyść: gotowe scenariusze obrony i reagowania na incydenty ransomware.

Poziom: średniozaawansowany

Polityka Bezpieczeństwa Informacji

Dla kadry zarządzającej, administracji, specjalistów IT w sektorach transportu, produkcji i MŚP

O cyklu życia polityki (analiza ryzyka, procedury, szkolenia, nadzór), klasyfikacji i obsłudze incydentów, dokumentacji i raportowaniu zgodnie z KSC/RODO (CSIRT/CERT).

Kluczowa korzyść: poukładany system bezpieczeństwa zgodny z prawem i praktyką.

Poziom: początkujący

Więcej informacji o szkoleniach