PFR
Polski Fundusz Rozwoju

Sieć Firm Przyszłości

COMCERT

Warsztaty

CyberSec w praktyce

- Doświadcz cyberataku
- Wyciągnij wnioski
- Wprowadzaj standardy cyberbezpieczeństwa dla Twojej firmy

Co się będzie działo na warsztatach?

Symulacje

Sesje interaktywnej symulacji m.in. atak cybernetyczny

Praktyka

Analiza realnych przypadków z biznesu

Strategia

Tworzenie założeń strategii cyberbezpieczeństwa i wdrażania standardów

Wiedza

Wiedza z zakresu zarządzania ryzykiem, reagowania na incydenty i działań po atakach itp.

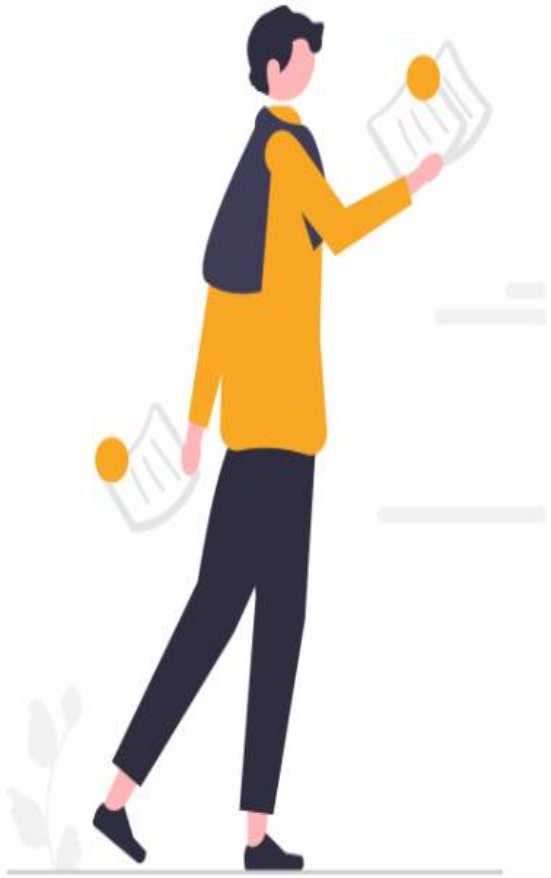
Plan warsztatów

Warsztat 1: Wprowadzenie do Cyberbezpieczeństwa

- Gra symulacyjna: atak cybernetyczny
- Podstawowe pojęcia
- Analiza decyzji i postępowania
- Analiza zagrożeń dla firm oraz najlepsze praktyki

Warsztat 2: Najlepsze praktyki i zarządzanie ryzykiem

- Gra symulacyjna: symulacja sytuacji kryzysowej związanej z cyberatakiem
- Omówienie strategii zarządzania ryzykiem
- Analiza decyzji i postępowania
- Praktyczne ćwiczenia z zarządzania ryzykiem
- Narzędzia do ograniczania ryzyka (w obszarach procesowym, technicznym i kadrowym)



Warsztat 3: Reagowanie po incydentach i odbudowa po atakach

- Gra symulacyjna: zarządzanie kryzysem
- Kluczowe strategie reagowania na incydenty
- Planowanie i przygotowanie do odbudowy
- Metody odzyskiwania działalności biznesowej po ataku

Warsztat 4: Wprowadzanie standardów cyberbezpieczeństwa

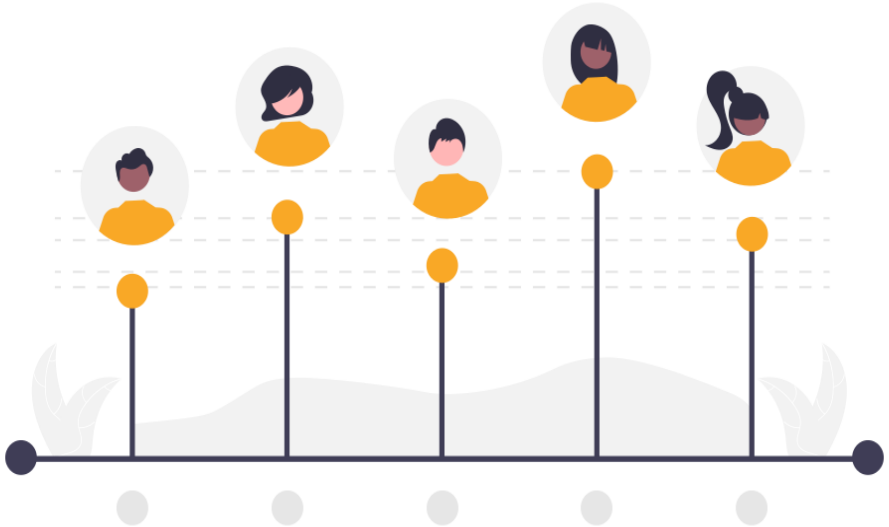
- Gra symulacyjna: poznanie standardów
- Wdrażanie standardów w praktyce
- Praktyczne zastosowanie standardów w sektorze MŚP

Co zyskasz?

1. Wiedzę jak przygotować firmę na ataki cybernetyczne
2. Opracujesz podstawy strategii cyberbezpieczeństwa firmy
3. Przygotujesz się do wdrożenia standardów cyberbezpieczeństwa
4. Zaprojektujesz scenariusze reagowania na incydenty oraz proces postępowania z incydentami

Dla kogo?

- Firmy z sektora MŚP
- Kadra zarządzająca firmą
- Osoby odpowiedzialne za cyberbezpieczeństwo
- Osoby chcące podnieść swoją świadomość nt. cyberbezpieczeństwa i zwiększyć umiejętności obrony przed cyberatakami



Platforma Cyber Twierdza Enterpise

Interakcja

Gra zespołowa polegająca na wyborze odpowiedniej strategii zapobiegania oraz reagowania na incydenty. Podczas gry uczestnicy warsztatów mogą współpracować, aby osiągnąć cel - ochrona aktywów ich organizacji.

Wiedza

Gra umożliwia lepsze zrozumienie ekosystemu cyberbezpieczeństwa jako całości oraz wzajemnych powiązań pomiędzy jego poszczególnymi komponentami.

Networking

Gra stwarza szanse na ustalenie lub utworzenie relacji pomiędzy uczestnikami, które można później wykorzystać praktycznie w rzeczywistym środowisku pracy.

Strategie

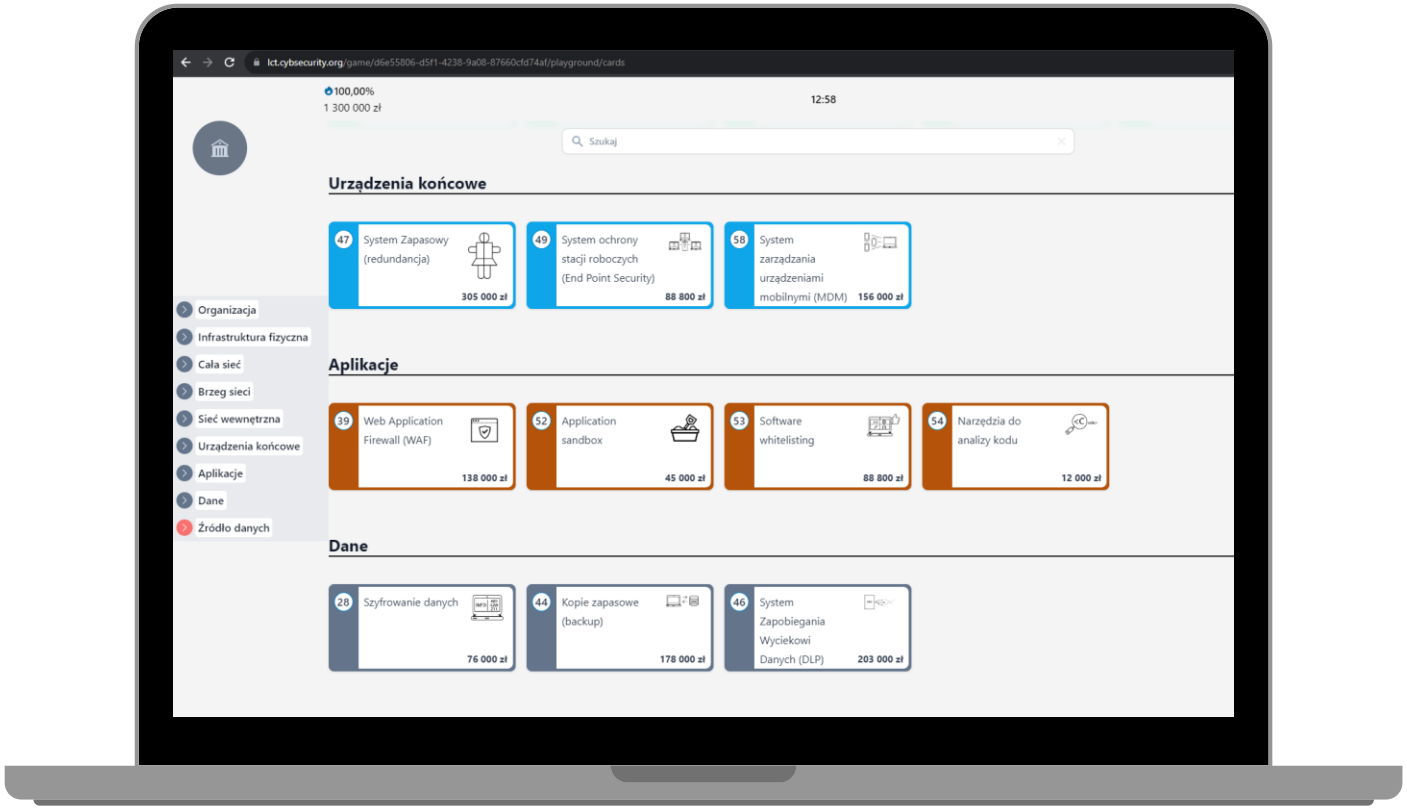
Uczestnicy mogą zrozumieć i przetestować różne strategie realizacji budżetu na cyberbezpieczeństwo, w szczególności skuteczności ich inwestycji w obszarze prewencji i reakcji na incydent.

Platforma Cyber Twierdza Enterpise

Gra bazuje na aplikacji webowej i wykorzystuje specjalnie przygotowane karty symbolizujące Zabezpieczenia z ośmiu obszarów:

- ORGANIZACJA
- INFRASTRUKTURA FIZYCZNA
- CAŁA SIEĆ
- BRZEG SIECI
- SIEĆ WEWNĘTRZNA
- HOST
- APLIKACJE
- DANE

Dziewiąty obszar – Źródła Danych – jest powiązany z wykrywaniem cyberataków. ŹRÓDŁA DANYCH

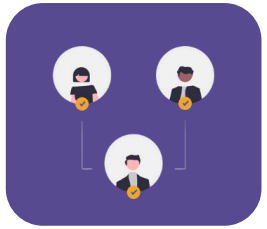


Platforma Cyber Twierdza Enterprise

Scenariusze w grze powstają na bazie wykrytych cyberataków

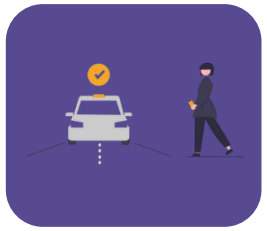
Firma konsultingowa

Atak poprzez kampanie w mediach społecznościowych (haktywizm), a następnie wykorzystanie przejętej infrastruktury firmy do przeprowadzenia dalszych cyberataków na inne cele
(~45 min)



Firma z sektora transportu

Atak mający na celu kradzież cennych danych.
(~30 min)



Firma produkcyjna

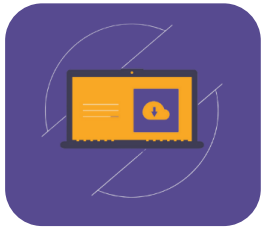
Atak przy użyciu legalnego oprogramowania (dostawca oprogramowania został skompromitowany)
(~45 min)

Przedsiębiorstwo usługowe

Atak ransomware.
(~30 min)

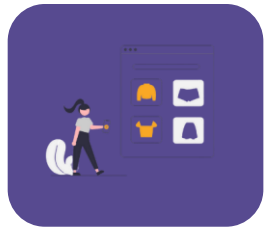
Firma korzystająca z usług chmurowych

Atak mający na celu przejęcie zasobów chmurowych.
(~30 min)



Sklep internetowy

Atak na strony WWW z wykorzystaniem podatności.
(~30 min)



PFR Polski Fundusz Rozwoju

Sieć Firm Przyszłości

comCERT

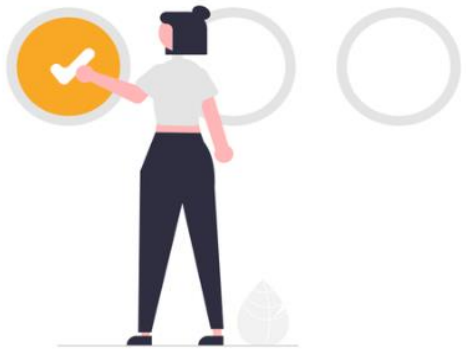
Przykładowe scenariusze symulacyjne*

1. Atak typu ransomware na systemy księgowe - Symulacja skupia się na ataku zakłócającym działanie systemów finansowych i księgowych, kluczowych dla funkcjonowania MŚP.

2. Phishing i socjotechnika skierowana na pracowników - Scenariusz przedstawiający techniki manipulacji, mające na celu wyłudzenie poufnych danych firmy.

3. Wyciek danych klientów - Symulacja koncentruje się na wycieku wrażliwych danych, analizie skutków i procesie zarządzania kryzysem.

4. Ataki DDoS na e-sklepy - Scenariusz uwzględniający ataki mające na celu uniemożliwienie działania sklepu internetowego, kluczowego dla dochodów MŚP.



*** Scenariusze zostaną dostosowane do profilu firm biorących udział w warsztacie**

Zainwestuj w przyszłość firmy

Cena obejmuje:

- Udział zespołu w spotkaniach warsztatowych
- Udział w grze symulacyjnej na platformie Cyber Twierdza Enterprise
- Dostęp do materiałów

2399 zł netto
(2950,77 zł brutto)

Cena udziału za 2 OSOBY Z FIRMY

Terminy spotkań

- Warsztat 1
  8 października, godz.10:00-13:00
- Warsztat 2
  9 października, godz.10:00:13:00
- Warsztat 3
  10 października, godz.10:00-13:00
- Warsztat 4
  11 października, godz. 10:00-13:00

Poznaj ekspertów

Piotr Kępski

Obecnie pracuje jako Cybersecurity Systems Analyst w ComCERT S.A., gdzie zajmuje się obszarem modelowania zagrożeń w cyberprzestrzeni oraz TTP (techniki, taktyki i procedury) w cyberatakach. Audytor wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji wg normy ISO/IEC 27001. Posiada doświadczenie we wdrażaniu polityki ochrony informacji z wykorzystaniem ISO/IEC 27001 oraz w planowaniu i wdrażaniu polityk bezpieczeństwa infrastruktury i informacji cyfrowej na bazie ISO/IEC 27001, 27002, 27005. Przez wiele lat związany z obszarem utrzymania systemów IT w sektorze publicznym, zarówno na poziomie technicznym jak i zarządczym. Jako członek Fundacji Bezpieczna Cyberprzestrzeń aktywnie działa na rzecz wzmacniania świadomości w obszarze zagrożeń pochodzących z cyberprzestrzeni, w tym m. in. prowadzi szkolenia, współtworzy serię podcastów Cyber, Cyber… oraz bierze udział w organizacji rozgrywek Ligi CyberTwierdza.

Marcin Fronczak

Obecnie pracuje jako Dyrektor Działu R&D w ComCERT. Certyfikowany audytor oraz ekspert w zarządzaniu ryzykiem i bezpieczeństwem IT – CISA, CIA, CRISC, ISO 27001 LA. Przez wiele lat zarządzał bezpieczeństwem IT w sektorze finansowym i ubezpieczeniowym oraz wykonywał audyty bezpieczeństwa obszaru IT/OT dla operatora infrastruktury krytycznej. Założyciel polskiego oddziału Cloud Security Alliance. Pierwszy w Polsce posiadacz certyfikatu i trener z zakresu bezpieczeństwa chmur Certified Cloud Security Knowledge (CCSK).

Partner merytoryczny

ComCERT
Jest pierwszą, niezależną firmą specjalizującą się w usługach typu CERT (Computer Emergency Response Team) na rynku przedsiębiorstw i instytucji w Polsce.
Świadczy usługi z zakresu cyberbezpieczeństwa klientom z różnych sektorów, m.in. z sektora finansowego (większość polskich banków), sektora telekomunikacyjnego (większość największych operatorów telekomunikacyjnych), przedsiębiorstw państwowych, instytucji i agencji Unii Europejskiej (ENISA, FRONTEX, Komisja Europejska), jak i dla rządów krajów pozaeuropejskich. W Republice Togijskiej zrealizowaliśmy nasz największy dotychczas kontrakt na budowę struktury cyberbezpieczeństwa „Cyber Defense Africa", na który składały się krajowy CERT oraz SOC realizujący usługi komercyjne na rynku togijskim.
Przez wiele lat ComCERT szkolił krajowe zespoły cyberbezpieczeństwa najważniejszych podmiotów w Polsce.

Zapraszam do kontaktu

Weronika Marusińska
Polski Fundusz Rozwoju

e-mail: weronika.marusinska@pfr.pl
telefon: +48 511 632 579