Szkolenia on-line
z zakresu Cyberbezpieczeństwa dla trzech grup odbiorców:

1 "Cyberbezpieczny pracownik" (phishing, ransomware)

(szkolenie dedykowane wszystkim pracownikom z krótkim egzaminem na zakończenie)

Czas trwania: 2h

Cena: 159 zł netto

Terminy:

24.03.2025 - *Zapisz się on-line*

04.04.2025 - *Zapisz się on-line*

2 "Cyberbezpieczny VIP" (phishing, ransomware, TOP zagrożenia)

(szkolenie dedykowane dla kadry kierowniczej oraz zarządu banku)

Czas trwania: 2h

Cena: 299 zł netto

Terminy:

10.03.2025 - *Zapisz się on-line*

18.03.2025 - *Zapisz się on-line*

3 "Cyberbezpieczny bank" *(ofensywne szkolenie dla pracowników IT banku)*

Czas trwania: 2h

Cena: 299 zł netto

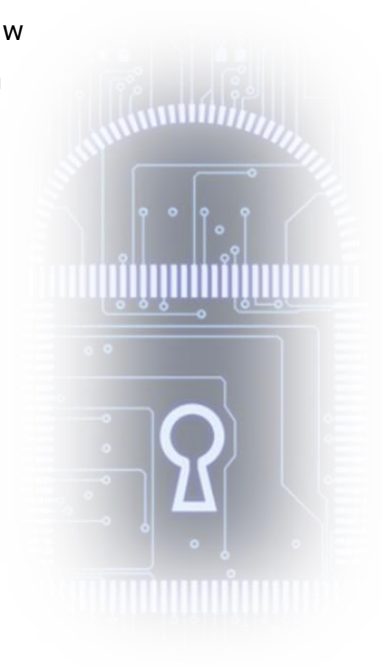
Terminy:

19.03.2025 - *Zapisz się on-line*

01.04.2025 - *Zapisz się on-line*

Cyber Security - SZKOLENIA

Celem tej propozycji szkoleniowej jest przekazanie Państwu kompleksowej wiedzy w zakresie bezpieczeństwa technologii informatycznych.



Przede wszystkim dostarczenie praktycznych informacji, które pomogą w zidentyfikowaniu, zrozumieniu i przeciwdziałaniu zagrożeniom związanym z cyberprzestrzenią.

Podczas szkoleń prowadzący przedstawią zagadnienia związane bezpieczeństwem systemów oraz aplikacji, ochroną sieci informatycznej, urządzeń, programów i danych przed atakami, uszkodzeniami lub nieautoryzowanym dostępem.

Prawidłowa reakcja na cyberatak czy wyciek danych jest priorytetowa, stąd szkolenia z przykładami i we współpracy z profesjonalistami w tym obszarze.

Metodyka: Szkolenia on-line, prowadzone za pośrednictwem Internetu przy użyciu platformy do zdalnego kształcenia.

Ewaluacja: Szkolenie dla pracowników zakończone krótkim egzaminem w formie quizu, w pozostałych wykorzystana będzie ankieta oceny szkolenia.

Sylwetka trenera:

Michał Wnękowicz

- Prowadzi szkolenia z zakresu Cyber Awareness oraz wykłady z wielu różnych dziedzin bezpieczeństwa.
- Konsultant d/s bezpieczeństwa oraz Security Research Manager dla research.securitum.com.
- Na co dzień realizuje testy bezpieczeństwa w Securitum, jest również autorem artykułów na Sekurak.pl (m.in. serii o Rekonesansie).
- Prelegent na konferencjach MEGA SHP, Sekurak Awareness, PLNOG 21.

Zachęcamy do udziału, a przede wszystkich do skorzystania z możliwości czerpania wiedzy i umiejętności od profesjonalistów w tym zakresie!

PROGRAMY SZKOLENIOWE:

Cyberbezpieczny pracownik (phishing, ransomware)

MODUŁ I: WYCIEK DANYCH I HASŁA

1. Kluczowe dobre praktyki.

MODUŁ II: ATAKI I METODY OBRONY

1. Phishing – definicja, rozpoznawanie e-maili i domen phishingowych, techniki obrony.
2. Atak homograficzny – mechanizm działania i sposoby ochrony.
3. Ataki w mediach społecznościowych i komunikatorach – analiza i metody obrony.
4. Smishing & Vishing – sposoby oszustw telefonicznych, prezentacja metod takich jak „na wnuczka”, „na hakera”, „na amerykańskiego żołnierza” itp.

MODUŁ III: ATAKI I METODY OBRONY

1. Bezpieczne korzystanie z internetu – znaczenie certyfikatów, analiza adresów, blokery reklam.
2. Bezpieczna poczta e-mail – nagłówki, filtrowanie, szyfrowanie i zabezpieczanie załączników.
3. Zaawansowane ataki – rekrutacja, fałszywe inwestycje, spear-phishing, ataki browser-in-the-browser.
4. Ataki fizyczne – pokaz na żywo zagrożeń takich jak magiczne kable, Flipper Zero, niebezpieczne pendrive'y.
5. Podsumowanie i Q&A.

Cyberbezpieczny bank - szkolenie dla IT

MODUŁ I: BEZPIECZEŃSTWO APLIKACJI WEBOWYCH

1. Typowe ataki – XSS, SQL Injection, XXE, Path Traversal, Broken Authentication, RCE, SSTI, deserializacja – demonstracje na żywo.
2. Atakowanie kontenerów Docker – omówienie zagrożeń i pokaz praktyczny.

MODUŁ II: BEZPIECZEŃSTWO INFRASTRUKTURY

1. Ransomware i MITM – mechanizmy działania i konsekwencje.
2. Ataki na protokoły sieciowe – ARP, DNS, DHCP i ich podatności.
3. Dobre praktyki obronne & Q&A.

"Bezpieczny VIP" (phishing, ransomware, TOP zagrożenia)

MODUŁ I: BEZPIECZEŃSTWO KADRY ZARZĄDZAJĄCEJ, SPRZĘTU I PRACY ZDALNEJ

1. Gromadzenie danych do ataku – metody pozyskiwania informacji i fałszywa tożsamość.
2. Ochrona danych i bliskich – zabezpieczenia informacji prywatnych i firmowych.
3. Zagrożenia technologiczne – ataki na Wi-Fi, smartfony, sprzęt prywatny i służbowy.
4. Ataki fizyczne – magiczny kabel, Flipper Zero, złośliwe pendrive'y (pokazy na żywo).
5. Higiena pracy zdalnej – bezpieczny dostęp, zagrożenia chmury, ochrona przed podglądaniem.
6. Szyfrowanie i usuwanie danych – praktyczne demonstracje.

MODUŁ II: NAJWIĘKSZE ZAGROŻENIE DLA BANKU – RANSOMWARE

1. Ransomware – definicja i metody rekonesansu (social media, skanery IoT).
2. Realne przypadki wycieków danych i decyzji PUODO.
3. Pokaz ataku end-to-end – od phishingu do przejęcia infrastruktury.
4. Uprawnienia użytkowników i administratorów – wpływ na bezpieczeństwo.
5. Znaczenie kopii zapasowych i aktualizacji.
6. Podatności CVE i uzyskanie webshella – pokaz na żywo.
7. Podsumowanie i sesja Q&A.

Przykłady prezentowane podczas szkoleń aktualizowane są na bieżąco.

Cena obejmuje:

- ✓ Dostęp do e-szkolenia
- ✓ Materiały szkoleniowe w PDF
- ✓ Sesja Q&A z ekspertem
- ✓ Egzamin przy szkoleniu dla pracowników
- ✓ E-certyfikat ukończenia szkolenia, który przekażemy Państwu w formie elektronicznej za pomocą poczty e-mail,
- ✓ Opieka moderatora.

Zgłoszenia prosimy nadsyłać najpóźniej 5 dni przed szkoleniem.

Informacja z dostępem do szkolenia zostanie rozesłana dzień przed szkleniem do godz.14:00

Podstawowe wymagania techniczne dla osób biorących udział w sesji on-line:

1. komputer wyposażony w głośniki lub słuchawki, z podłączeniem do Internetu i prawidłowo działającą przeglądarką internetową: Firefox, Edge lub Chrome (polecana),
2. przepustowość łącza - minimalnie 512Kb/s (także połączenie wifi).

Zgłoszenia przyjmuje i informacji udziela:

Iryna Lutska
Specjalista ds. szkoleń
M. +48 505 459 553
E. i.lutska@bodie.pl

Nota prawna: