kod szkolenia: ECIH / PL DL 3d NIS2

EC-Council Certified Incident Handler v3

Autoryzowane szkolenie EC-Council – ECIH v3 - EC-Council Certified Incident Handler

Realizowane jest w formie wykładu oraz praktycznych warsztatów.

Szkolenie EC-Council Certified Incident Handler v3 (E|CIH) to kompleksowy program na poziomie specjalistycznym, który przekazuje wiedzę i umiejętności potrzebne organizacjom do skutecznego radzenia sobie z incydentami związanymi z bezpieczeństwem informatycznym. Kurs omawia podstawowe zasady i techniki wykrywania i reagowania na obecne i nowo pojawiające się zagrożenia bezpieczeństwa komputerowego. Po ukończeniu szkolenia kursanci będą mieli okazję zapisać się na egzamin ECIH. Certyfikat ECIH jest wysoko oceniany i pomaga zwiększyć szanse zatrudnienia na stanowiskach specjalistów ds. cyberbezpieczeństwa na całym świecie.

Dyrektywa NIS2

Unijne przepisy rozszerzają zakres przepisów dotyczących cyberbezpieczeństwa. Przedsiębiorcy objęci regulacją NIS2, wynikającą z ustawy o krajowym systemie bezpieczeństwa, będą objęci obowiązkiem stosowania produktów, usług bądź procesów, objętych tymi schematami certyfikacyjnymi.

Sprawdź, czy Twoja firma będzie objęta dyrektywą NIS2

Sprawdź swoją wiedzę z zakresu:

- **CompTIA CySA+**
- **CompTIA Security+**
- **CompTIA Network+**

- **OSINT - Biały Wywiad, czyli jak dotrzeć do cennych informacji**
- **CEH - Certified Ethical Hacker**
- **ECIH - Certified Incident Handler**
- **Testy penetracyjne**

Odbiorcy szkolenia

Szkolenie skierowane jest do:

- administratorów sieci
- osób odpowiedzialnych za infrastrukturę informatyczną
- inżynierów systemowych
- audytorów VA (Vulnerability Assessment)
- osób zarządzających ryzykiem od strony IT
- inżynierów bezpieczeństwa
- analityków bezpieczeństwa
- specjalistów CFI (Cyber Forensic Investigators)
- pracowników SOC
- pracowników IT planujących podniesienie poziomu bezpieczeństwa informatycznego swojej organizacji

Dla osób nie będących specjalistami z zakresu bezpieczeństwa IT szkolenie może być zbyt intensywne ale pozwoli zwiększyć świadomość dotyczącą obsługi zdarzeń i właściwego reagowania na zagrożenia. Specjaliści ds. bezpieczeństwa informatycznego, audytorzy i analitycy bezpieczeństwa oraz pentesterzy będą mogli ugruntować, usystematyzować bądź uzupełnić swoją wiedzę.

Korzyści

Organizacje są celem nieustannych ataków a dzięki wiedzy i umiejętnościom zdobytym na kursie E|CIH, eksperci będą mogli nie tylko wykrywać incydenty, lecz także błyskawicznie nimi zarządzać, jak i całościowo na nie odpowiadać. Program szkoleniowy uczy biegłej obsługi i reakcji na takie zdarzenia jak naruszenia bezpieczeństwa sieci, infekcje złośliwym oprogramowaniem czy zagrożenia związane z atakami wewnętrznymi. Ponadto studenci poznają podstawy informatyki śledczej, jej rolę w obsłudze zdarzeń i reagowaniu na nie. Kurs omawia również pracę zespołów zarzadzania i reagowania na incydenty oraz przedstawia techniki stosowane przy przywracaniu działania firmy. Kursanci dowiedzą

się, jak radzić sobie w sytuacjach naruszenia bezpieczeństwa, poznają metody oceny ryzyka oraz różne przepisy związane z obsługą incydentów. Po ukończeniu tego kursu uczestnicy będą mogli tworzyć spójne i przemyślane zasady obsługi zdarzeń.

Uczestnicy szkolenia zrozumieją procesy obsługi i reagowania na incydenty i nauczą się :

- stosować procedury pierwszej reakcji i przygotowywać „grunt” dla informatyki śledczej
- obsługiwać incydenty i adekwatnie reagować
- obsługiwać zdarzenia związane ze złośliwym oprogramowaniem
- reagować na incydenty związane z bezpieczeństwem poczty e-mail, aplikacji internetowych
- obsługiwać i reagować na naruszenia bezpieczeństwa sieci
- radzić sobie z różnymi z incydentami związanymi z bezpieczeństwem chmury
- wykrywać i reagować na zagrożenia wewnętrzne

Program szkolenia

1. Introduction to incident handling and response.
2. Incident handling and response process.
3. First response.
4. Handling and responding to Malvere Incidents.
5. Handling and responding to Email Security Incidents.
6. Handling and responding to Network Security Incidents.
7. Handling and responding to Web Application Security Incidents.
8. Handling and responding to Coud Security Incidents.
9. Handling and responding to Insider Threats.
10. Handling and responding to Endpoint Security Incidents.

Oczekiwane przygotowanie uczestnika

Wymagana dobra znajomość systemów operacyjnych Windows oraz Linux, wiedza o protokołach i usługach sieciowych. Zalecane przynajmniej dwuletnie doświadczenie w cyberbezpieczeństwie.

Szkolenie obejmuje

- 3 dni pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Autoryzowane materiały szkoleniowe ECIH

- Voucher na egzamin
- Środowisko laboratoryjne
- Podręcznik w wersji elektronicznej
- Środowisko laboratoryjne

Metoda szkolenia

- wykład
- warsztaty

Język

- Szkolenie: polski
- Materiały: angielski

Czas trwania

3 dni / 21 godzin

Metoda egzaminacyjna

- Tytuł egzaminu: EC-Council Certified Incident Handler
- Liczba pytań: 100
- Czas trwania: 3 godziny
- Format: pytania wielokrotnego wyboru

Uwaga: Jeśli uczestnik chciałby zdawać egzamin ECIH w formule online (z dowolnego miejsca) z tzw. ochroną zdalną, obowiązuje dodatkowa opłata 100 USD netto. Koszt obejmuje wynajęcie osoby nadzorującej egzamin (tzw. proktora). Zakupu dokonujemy indywidulanie na stronie vendora: https://store.eccouncil.org/product/voucher-upgrade-rps-to-vue/