Wprowadzenie do Cyberbezpieczeństwa

Opis kursu

Kurs ***Wprowadzenie do Cyberbezpieczeństwa*** przedstawia trendy, zagrożenia i skuteczne metody zabezpieczeń w cyfrowym świecie - zarówno w zakresie prywatnym, jak i zawodowym.

Korzyści

Nauczysz się, jak zabezpieczać swoje dane i zachować prywatność online. Dowiesz się, jakie są trendy w tym obszarze IT oraz dlaczego rośnie deficyt specjalistów w zakresie cyberbezpieczeństwa i dlaczego większość ról zawodowych wymaga wiedzy i umiejętności w tym zakresie.

Elementy kursu

- 5 modułów
- Interaktywny model przekazywania treści
- 8 ćwiczeń oraz 7 praktycznych labów do utrwalenia wiedzy
- 4 quizy and 1 test końcowy
- Linki do dodatkowych zasobów poszerzających wiedzę

ODBIORCA: uczniowie szkół średnich, studenci, pracownicy, wszyscy zaintereowani podstawami cyberbezpieczenstwa

Wstepne wymagania: Nie ma

Model: kurs moze być prowadzony prze nauczyciela-instruktora lub oferowany do samodzielnej nauki

Czas realizacji: 15 godzin

Rekomednowany kolejny kurs: Cybersecurity Essentials (30 godz)

WWW: https://www.netacad.com/courses/security/introduction-cybersecurity

Cybersecurity Essentials

Opis kursu

Kurs Cybersecurity Essentials obejmuje fundamentalną wiedzę i najważniejsze umiejętności dla wszystkich obszarów cyberbezpieczeństwa, w tym information security, systems security, network security, ethics and laws, a także techniki obrony i ograniczania ryzyka stosowane do ochrony firm.

Korzyści

Ten kurs jest rekomendowany dla uczniów, którzy planują przystąpić do certyfikacji CCNA. Zapewnia fundamentalne umiejętności w zakresie bezpieczeństwa na stanowiska entry-level w obszarze sieci i bezpieczeństwa

Elementy kursu

- 8 modułów
- 34 praktycznych ćwiczeń, 10 ćwiczeń w Cisco Packet Tracer, 12 praktycznych labów, które wzmacniają naukę
- 8 modułowych quizów, 1 egzamin końcowy
- Linki do dodatkowych zasobów poszerzających wiedzę

Szczegóły

Odbiorca: Secondary and 2-year college vocational students

Wstępne wymagania: Introduction to Cybersecurity

Wymagana współpraca z ASC: Nie

Wymagane szkolenie wstępne: Nie

Języki:: Angielski

Model: kurs może być prowadzony przez nauczyciela-instruktora lub oferowany do samodzielnej nauki

Szacowany czas realizacji: 30 godzin

Rekomendacja następnych kursów: CCNA Cybersecurity Operations

CCNA Security

Opis kursu

Kurs CCNA Security wprowadza kluczowe koncepcje i umiejętności do rozwiązywania problemów, monitorowania sieci komputerowych i pomocy w zapewnieniu integralności urządzeń i danych.

Kurs skupia się na praktycznym wykorzystywaniu umiejętności potrzebnych do projektowania, wdrażania I zarządzania systemami bezpieczeństwa sieci.

Korzyści

Uczestnicy kursu CCNA R&S zainteresowani budowaniem fachowej wiedzy o bezpieczeństwie i ochronie danych do zawodowej certyfikacji CCNA Security i pracy jako network security specialist.

Elementy kursu

- 11 modułów, quizów i testów
- 13 ćwiczeń w Cisco Packet Tracer i1 Packet Tracer Practice Skills Based Assessment (SBA)
- 16 praktycznych labów
- Po jednym: pre-test, certification practice exam, practice final, final exam i skills-based assessment

Certification Aligned

Szczegóły

Odbiorca: 2-year and 4-year college students in Networking or Engineering programs

Wstępne wymagania: CCNAv7: ITN and SRWE (lub odpowiednik)

Wymagana współpraca z ASC: Tak

Wymagane szkolenie instruktorskie: Tak

Język: Angielski

Model: prowadzony przez nauczyciela-instruktora

Szacowany czas realizacji: 70 godzin

Rekomendacja następnych kursów: CCNP R&S ROUTE

IoT Security

Opis kursu

Nagły wzrost podłączonych urządzeń IoT umożliwia cyfryzację wielu branży, ale oznacza również większe odsłonięcie na zagrożenia bezpieczeństwa. Przed zakończeniem kursu uczniowie będą mogli przeprowadzać oceny podatności i ryzyka, a także szukać i rekomendować strategie minimalizowania ryzyka dla powszechnych zagrożeń bezpieczeństwa w systemach IoT.

Korzyści

Uczniowie chcący rozpocząć karierę w dynamicznie rozwijających się dziedzinach IoT i security poznają praktyczne narzędzia do oceny podatności na zagrożenia w rozwiązaniach IoT, przeprowadzania modelowania zagrożenia, korzystania z ram zarządzania ryzykiem do rekomendowania środków ograniczających ryzyko. Te umiejętności są ważne i IoT i innych architekturach sieci.

Elementy kursu

- Przeprowadzanie kompleksowego modelowania ryzyka i ocena zagrożeń bezpieczeństwa w rozwiązaniach IoT
- Odkrywanie i demonstrowanie podatności korzystając z prawdziwych narzędzi do penetracji jak Kali Linux
- Zdobywanie praktycznego doświadczenia z prototypami IoT korzystając z Raspberry Pi
- Zwiększanie świadomościo nowych technologiach w przestrzeni IoT Security, jak Blockchain
- Gra IoT Security

Szczegóły

Odbiorca: Vocational, 2-year and 4-year College, 4-Year University students

Wymagana współpraca z ASC: Tak

Wstępne wymagania:

- IoT Fundamentals: Connecting Things course
- Networking and security knowledge equivalent of Networking Essentials and Cybersecurity Essentials

Język: Angielski

Model: Prowadzony przez nauczyciela-instruktora

Szacowany czas realizacji: 50 godzin