Kurz Network Security

O kurze

Tento kurz je úvodom do kľúčových konceptov bezpečnosti a buduje zručnosti potrebné pre konfigurovanie a správu počítačových sietí ako aj zabezpečenie integrity zariadení a dát.

Výhody

Umožňuje získať praktické zručnosti a kompetencie pre návrh, implementáciu a manažment bezpečnostných sieťových systémov a zabezpečenie ich integrity.

Príprava na kariéru

- ✓ Budovanie expertízy v sieťovej bezpečnosti a ochrane dát
- ✓ Rozvoj zručností potrebných pre úspešný vstup pozícií špecialistov na sieťovú bezpečnosť na trhu práce
- ✓ Získavanie priemyslom žiadaných kompetencií korešpondujúcich s National Institute for Standards and Technology (NIST) definovaným rámcom kybernetickej bezpečnosti

Detaily kurzu

Cieľová skupina: študenti stredných a vysokých škôl

Orientačná časová dotácia kurzu: 70 hodín (výučba + samoštúdium)

Doporučené predchádzajúce kurzy: Základné porozumenie sieťových technológií (kurzy CCNA: Introduction to Networks a CCNA: Switching, Routing, and Wireless Essentials, alebo ekvivalent)

Formát kurzu: vedený inštruktorom

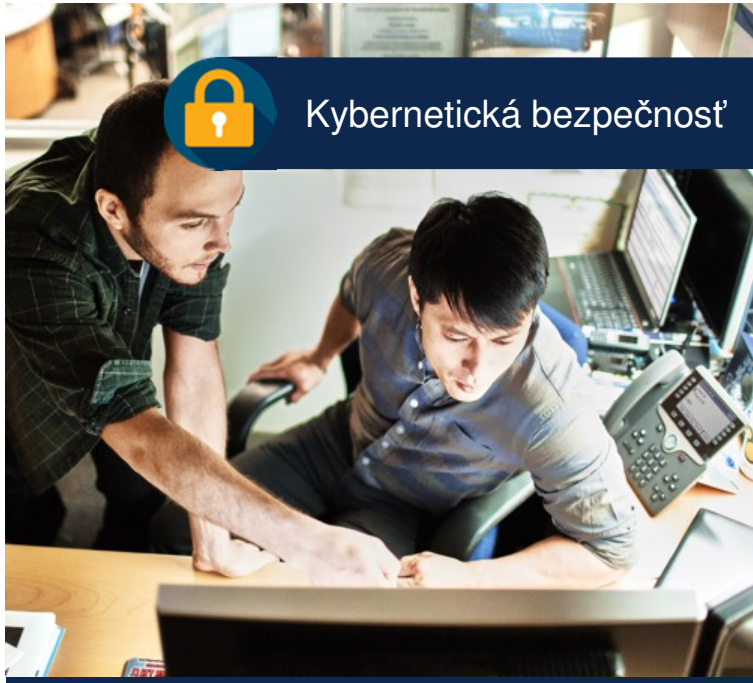
Vzdelávacie komponenty:

- ✓ 22 kapitol a 23 praktických lab cvičení
- ✓ 22 Cisco Packet Tracer aktivít
- ✓ 87+ interaktívnych aktivít, videí a kvízov
- ✓ 1 záverečná skúška

Ukončenie kurzu: Certifikát o absolvovaní, Digitálny odznak

Nasledujúce doporučené kurzy: CyberOps Associate, IoT Security

ceelabs



Požiadavky a vybavenie

- **Vzťah s podporným centrom:** Áno
- **Požadovaný tréning inštruktorov:** Áno
- **Laboratórne vybavenie:** Áno
- **Zľava na certifikáciu:** neaplikuje sa

PT **Praktické zručnosti s podporou Cisco Packet Tracer**

Formát školenia Network Security

Spôsoby organizácie:

- ✓ V laboratóriu s hardvérovým vybavením (in person)
- ✓ Prostredníctvom videokonferenčného systému Webex (remote)

Počet stretnutí:

- ✓ 5 dní/8hodín (in person)
- ✓ 10 dní/4 hodiny (remote)

Témy teoretických prednášok:

- ✓ Zabezpečenie siete, Hrozby, Riešenie hrozieb, Zabezpečenie prístupu Windows OS, Linux OS
- ✓ Administratívne roly, Monitorovanie a riadenie zariadení
- ✓ AAA, ACL
- ✓ Firewall technológie, Zone-Based Policy Firewalls
- ✓ Základy a implementácia IPS, Zabezpečenie koncových zariadení
- ✓ Zabezpečenie L2 vrstvy, Služby pre šifrovanie
- ✓ Overenie integrity a pôvodu, PKI
- ✓ VPN, IPSec
- ✓ Úvod a konfigurácia Cisco ASA Firewall

Témy praktických cvičení:

- ✓ SSH, Šifrovanie hesiel
- ✓ Konfigurácia administratívnych rôl, AutoSecure, OSPF Auth, SNMP, NTP, Syslog
- ✓ AAA Auth, Inštalácia VM, Auth Radius, ACL
- ✓ PT-konfigurácia ZPF
- ✓ SPAN
- ✓ STP, Port-Security, Šifrovanie a dešifrovanie textu
- ✓ OpenSSL - Tvorba Hash, šifrovanie a dešifrovanie, Kontrola certifikátu
- ✓ Konfigurácia IPSec Site-to-Site VNP cez CLI
- ✓ Konfigurácia ASA Firewallu cez CLI a ASDM

Spôsob ukončenia kurzu:

Teoretická záverečná skúška