Kurz CyberOps Associate

O kurze

Tento kurz sa zameriava na základné bezpečnostné koncepcie a kompetencie pre monitorovanie, detegovanie, analýzu a odozvu na bezpečnostné udalosti. Kurz popisuje detekčné techniky a postupy v súvislosti s kyberzločinom, kyberšpionážou, vnutornými hrozbami a ďalšími problémami, ktorým môžu organizácie z hľadiska kyberbezpečnosti čeliť.

Výhody

Získanie praktických zručností a kompetencií potrebných pre správu a zaistenie prevádzkovej bezpečnosti sieťových systémov.

Príprava na kariéru

- ✓ Rozvoj zručností a príprava pre junior pozície v bezpečnostných operačných centrách (SOC)
- ✓ Príprava na certifikačnú skúšku CyberOps Associate

Detaily kurzu

Cieľová skupina: študenti stredných a vysokých škôl; budúci IT profesionáli zo zameraním na prevádzkovú bezpečnosť

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

Doporučené predchádzajúce kurzy: Introduction to Cybersecurity, Cybersecurity Essentials

Formát kurzu: vedený inštruktorom

Vzdelávacie komponenty:
- ✓ 28 kapitol a 46+ praktických lab cvičení
- ✓ 6 Cisco Packet Tracer aktivít
- ✓ 113 interaktívnych aktivít, videí a kvízov
- ✓ 1 cvičná certifikačná skúška

Ukončenie kurzu: Certifikát o absolvovaní, Digitálny odznak

Nasledujúce doporučené kurzy: CCNA Security, IoT Security

ceelabs

Požiadavky a vybavenie

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

Certification Aligned
Cisco Certified CyberOps Associate

Formát školenia CyberOps Associate

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:

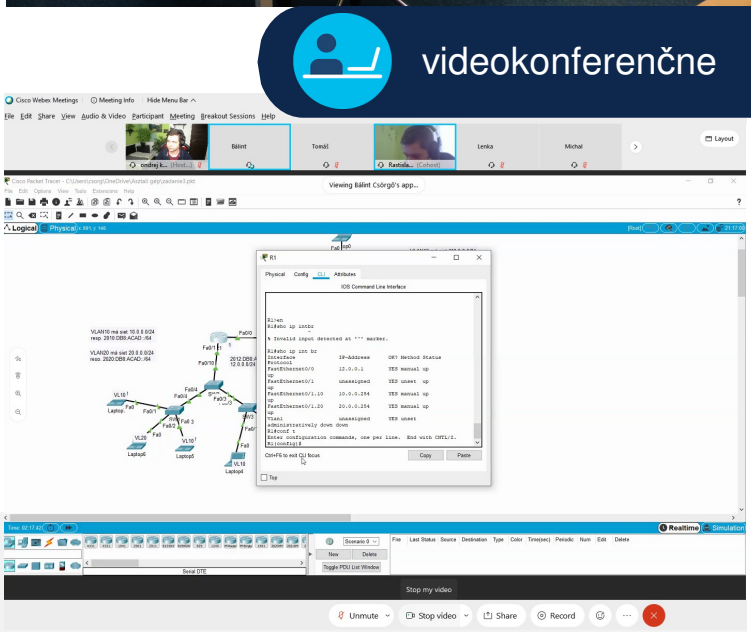
- ✓ Hrozby, Útočníci, SOC
- ✓ Windows OS, Linux OS
- ✓ Sieťové protokoly a služby
- ✓ Sieťové zariadenia a infraštruktúra
- ✓ Útoky, zraniteľnosti a monitorovanie
- ✓ Ochrana a kontrola prístupu (AAA)
- ✓ Kryptografia, Ochrana koncových zariadení
- ✓ Sieťové dáta, technológie a protokoly
- ✓ Vyhodnocovanie hlásení, Práca s dátami, Analýza incidentov

Témy praktických cvičení:

- ✓ Inštalácia VM
- ✓ Windows Task Manager, PowerShell, Linux Shell
- ✓ Wireshark + Nmap
- ✓ PT-ACL
- ✓ Wireshark, MySQL útok-pcap, Linux Log
- ✓ Hash-SHA256, Šifrovanie/Dešifrovanie-OpenSSL
- ✓ PT-Netflow, Logging
- ✓ Snort/FW pravidlá, ELK, Sguil

Spôsob ukončenia kurzu:

Teoretická záverečná skúška



ceelabs