



Cybersecurity operations

Kort fortalt

Deltageren kan anvende sin opnåede viden om forskellige former for netværksangreb, kryptografiske sikkerhedsalgoritmer og netværksmonitoreringsværktøjer til at foretage analyse og afværgning af netværksangreb på basis af informationer i IDS/IPS systemer.

Hold

04-11-2024

Cybersecurity operations
Hedegaardsvej 88 2300

10 dage

Daghold

24-11-2025

Cybersecurity operations
Ahorn Allé 3-5 4100

10 dage

Daghold

Kontakt

Simone K. Mathiesen
2844 2519
skm@zbc.dk

Kursusinfo

Dit udbytte af kurset
Cybersecurity operations er for dig, der bl.a.:

- Ønsker at være på forkant inden for cybercrime
- Ønsker at arbejde med sikkerhed i forbindelse med infrastruktur
- Ønsker at udfordre dig selv inden for dit fag

Læs mere om kurset i [vores brochure](#)

Fag: Cybersecurity operations

Fagnummer:

49742

Varighed

10 dage

AMU-pris:

DKK 2.080,00

Uden for målgruppe:

DKK 8.069,00

Målgruppe: Kurset henvender sig til faglærte personer, inden for det datatekniske område, og andre inden for AMU målgruppen med tilsvarende kvalifikationer, der skal eller ønsker at arbejde med sikkerhed i forbindelse med infrastruktur.

Kursuspris

AMU-målgruppe:

DKK 2.080,00

Ikke AMU-målgruppe, fremmøde:

DKK 8.069,00

Deltageren kan redegøre for Cybersikkerhedsanalytikerens rolle i virksomheden.

Deltageren kan redegøre for basale funktioner og egenskaber ved Windows operativsystemet, herunder hvorledes man monitorerer samt sikrer enheder med Windows operativsystemer.

Deltageren kan redegøre for basale funktioner og egenskaber ved Linux operativsystemet, herunder hvorledes man monitorerer samt sikrer enheder med Linux operativsystem.

Deltageren kan analysere funktionen af netværksprotokoller og -services.

Deltageren kan klassificere typerne af netværksangreb.

Deltageren kan anvende netværksmonitoreringsværktøjer til at identificere angreb mod netværksprotokoller og -tjenester.

Deltageren kan anvende metoder til at forhindre ondsindet adgang til computernetværk, værter og data.

Deltageren kan redegøre for effekten af kryptografi i forbindelse med overvågning af netværkssikkerhed.

Deltageren kan redegøre for, hvordan man undersøger endpoint svagheder og angreb.

Deltageren kan identificere advarsler om netværkssikkerhed.

Deltageren kan analysere netværkets intrusion-data for at kontrollere potentielle udnyttelser.

Deltageren kan anvende hændelsesresponsmodeller til at håndtere netværkssikkerhedshændelser.

Tilmelding

