TECHCOLLEGE

Undervisningsmateriale til AMU-kursus

Kursusoplysninger

Kursusnavn	Cybersecurity Operations
AMU-kursusnummer	49742
Varighed	10 dage
Målgruppe	Faglærte 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
Dato for udarbejdelse	December 2025
Udarbejdet af	Johnny Kure Jakobsen

Indhold i materialet:

Støttet af

BØRNE- OG UNDERVISNINGS-MINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET

Formål

Formålet med opgaverne er at understøtte deltagernes forståelse af operative cybersikkerhedsprocesser og træne deres evne til at analysere og reagere på sikkerhedshændelser. Deltagerne opnår praksisnær og anvendelsesorienteret viden om operative cybersikkerhedsprocesser i moderne IT-miljøer. Kurset giver deltagerne forståelse for, hvordan sikkerhedshændelser identificeres, analyseres og håndteres i mindre og mellemstore organisationer.

Opgaverne anvendes både som læringsaktiviteter og som forberedelse til den afsluttende praktiske prøve. Der arbejdes med progression fra observation og analyse til beslutning og dokumentation.

Deltagerne opnår indsigt i:

- Trusselsbilledet og angrebstyper
- Loganalyse og sikkerhedsovervågning
- SIEM-principper
- Incident Response-processer
- Endpoint-sikkerhed i Windows og Linux
- Netværksmonitorering og intrusion-analyse

Efter kurset kan deltageren bidrage aktivt til overvågning, analyse og håndtering af sikkerhedshændelser i organisationen.

Deltageren kan:

- Redegøre for cybersikkerhedsanalytikerens rolle i virksomheden
- Redegøre for basale funktioner og egenskaber ved Windows operativsystemet, herunder monitorering og sikring
- Redegøre for basale funktioner og egenskaber ved Linux operativsystemet, herunder monitorering og sikring
- Analysere funktionen af netværksprotokoller og -services
- Klassificere typer af netværksangreb
- Anvende netværksmonitoreringsværktøjer til at identificere angreb
- Anvende metoder til at forhindre ondsindet adgang
- Redegøre for effekten af kryptografi i netværkssikkerhed
- Undersøge endpoint-svagheder og angreb
- Identificere advarsler om netværkssikkerhed
- Analysere intrusion-data
- Anvende hændelsesresponsmodeller

Støttet af
BØRNE- OG UNDERVISNINGS-MINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET

Indhold

Kurset veksler mellem teori og praksis. Herunder ses indholdet på kursets ti dage.

Introduktion til Cybersecurity Operations

- Operations vs governance og compliance
- Trusselsaktører og motiver
- Angrebsfaser og kill chain

Netværkssikkerhed og angrebstyper

- Klassiske netværksangreb
- Protokolmisbrug
- Intrusion detection

Logning og overvågning

- Logtyper (Windows, Linux, netværk)
- Event correlation
- Grundlæggende SIEM-principper

Endpoint-sikkerhed

- Windows event logs
- Linux logs og journaling
- Hardening-principper

Kryptografi i praksis

- TLS, certifikater og hashing
- Krypteringens rolle i overvågning
- Incident Response

Identifikation

- Inddæmning
- Afhjælpning
- Recovery

Dokumentation

- Undervisningen tager udgangspunkt i realistiske hændelsesscenarier og praktisk analyse frem for avanceret exploit-udvikling.

Støttet af
BØRNE- OG UNDERVISNINGS-MINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET

Aktiviteter

Dag 1–2 – Trusselsforståelse og rolle

- Cybersecurity operations vs governance
- Angrebstyper
- Kill chain
- Analytikerens rolle

Dag 3–4 – Netværksanalyse

- Protokolanalyse
- Netværksangreb
- Intrusion detection
- PCAP-analyse

Dag 5 – Windows sikkerhed

- Event Viewer
- Audit policies
- Endpoint monitorering

Dag 6 – Linux sikkerhed

- Syslog
- Journalctl
- Hardening

Dag 7 – SIEM-principper

- Log correlation
- Alarmer
- False positives

Dag 8–9 – Incident Response

- Hændelsesflow
- Roller og ansvar
- Dokumentation
- Simulerede hændelser

Dag 10 – Anvendelse i praksis

- Integreret hændelsesscenarie
- Analyse
- Beslutning

Støttet af
BØRNE- OG UNDERVISNINGS-MINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET

- Dokumentation

Kurset afsluttes med opsamling på læring, fælles refleksion og evaluering. Deltagerne arbejder med at perspektivere cybersikkerhedsarbejdet til egen organisation, herunder:

- Hvordan overvågning kan forbedres
- Hvordan responstiden kan reduceres
- Hvordan dokumentation kan styrkes

Der lægges vægt på, at deltageren kan forbinde teknisk analyse med organisatorisk ansvar.

Støttet af
BØRNE- OG UNDERVISNINGS-MINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET

Konkrete produkter

a. Opgavebeskrivelser

Formålet med opgaverne er at understøtte deltagernes forståelse af operative cybersikkerhedsprocesser og træne deres evne til at analysere og reagere på sikkerhedshændelser.

Opgaverne anvendes både som læringsaktiviteter og som forberedelse til den afsluttende praktiske prøve.

Der arbejdes med progression fra observation og analyse til beslutning og dokumentation.

Opgave 1 – Trusselsanalyse (Dag 1)

- Analyse af angrebsscenarie.
  Output: Skriftlig vurdering.

Opgave 2 – Netværksangreb (Dag 3)

- Analyse af PCAP-fil.
  Output: Identifikation af angrebstype.

Opgave 3 – Windows loganalyse (Dag 5)

- Fortolkning af sikkerhedshændelser.
  Output: Hændelsesrapport.

Opgave 4 – Linux loganalyse (Dag 6)

- Analyse af login-forsøg og systemhændelser.
  Output: Loganalyse-dokumentation.

Opgave 5 – SIEM-case (Dag 7)

- Identifikation af false positive vs reel hændelse.
  Output: Beslutningsrapport.

Støttet af
BØRNE- OG UNDERVISNINGS-MINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET

Opgave 6 – Incident Response simulation (Dag 8–9)

- Håndtering af sikkerhedshændelse.
  Output: Incident-rapport.

Opgave 7 – Integreret enterprise-case (Dag 10)

- Analyse og håndtering af samlet hændelse.
  Output: Dokumentation og redegørelse.

b. Pædagogiske overvejelser

Kurset er tilrettelagt med henblik på at udvikle deltagernes analytiske og refleksive kompetencer. Da målgruppen ofte har teknisk baggrund, arbejdes der med:

- Case-baserede hændelser
- Loganalyse i praksis
- Diskussion af beslutningstagning
- Rollefordeling i hændelseshåndtering
- Der lægges vægt på metodisk tilgang frem for teknisk "trial-and-error".

c. Didaktiske overvejelser

Undervisningen er opbygget med progression fra forståelse af trusselsbilledet til praktisk håndtering af hændelser. PowerPoint anvendes til begrebsafklaring, mens hovedindlæringen sker gennem:

- Analyseøvelser
- Simulerede hændelser
- Praktiske monitoreringsopgaver
- Fælles refleksion
- Der arbejdes bevidst med at koble teknisk analyse til organisatorisk konsekvens.

d. Praktisk prøve – Procesprøve (Bestået / Ikke bestået)

Prøveform: Individuel prøve - case-baseret - praktisk analyse - mundtlig redegørelse

Opgaven består af, at deltageren skal:

- Analysere en sikkerhedshændelse
- Identificere angrebstype
- Fortolke logdata

- Beskrive containment-strategi
- Udarbejde hændelsesrapport
- Redegøre for valg af handling

Deltageren må bruge følgende hjælpemidler: Egne noter, kursusmateriale og logudtræk

Tidsforbrug:

- Analyse og dokumentation: ca. 3 timer
- Mundtlig redegørelse: 10–15 minutter

e. Bedømmelsesgrundlag (Bestået / Ikke bestået)

Deltageren vurderes på evnen til at:

- Analysere sikkerhedshændelser korrekt
- Identificere angrebstype
- Anvende hændelsesresponsmodel
- Fejlfinde metodisk
- Dokumentere sammenhængende

Vurderingsskema (intern brug)

Vurderingsområde	Opfyldt	Delvist opfyldt	Ikke opfyldt	Bemærkninger
Angreb korrekt identificeret	☐	☐	☐	
Loganalyse korrekt	☐	☐	☐	
Incident model anvendt korrekt	☐	☐	☐	
Containment korrekt foreslået	☐	☐	☐	
Dokumentation overskuelig	☐	☐	☐	
Faglig redegørelse sammenhængende	☐	☐	☐	

Støttet af
BØRNE- OG UNDERVISNINGS-MINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET

Kriterier for "bestået":

Bestået forudsætter:

- Korrekt identifikation af hændelse
- Loganalyse dokumenteret
- Incident response anvendt korrekt
- Dokumentation sammenhængende
- Deltageren kan redegøre fagligt for sin løsning

Hvis deltageren ikke kan identificere hændelsen korrekt eller ikke kan anvende hændelsesresponsmodellen, vurderes prøven som ikke bestået.

Støttet af
BØRNE- OG UNDERVISNINGS-MINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET