Metalindustriens Uddannelsesudvalg

Undervisningsvejledning

Datatekniker med speciale i cybersikkerhed
1. juli 2025

Indhold

Undervisningsplan H1 Cybersikkerhed

Fag:

- 22848 Informations- og cybersikkerhed H1 (1 uge)

Kompetencemål: 45, 48, 49, 55

Læringsmål

- Forstå grundlæggende begreber som trusler, privacy, risikovurdering og databeskyttelse
- Udvikle en basal adgangskontrol- og passwordpolitik
- Identificere interessekonflikter og forstå deres betydning i en sikkerhedskontekst
- Få indblik i hvordan machine learning kan bruges til sikkerhedsovervågning

Undervisningsaktiviteter

Dag	Aktivitet
Mandag	Intro: Hvad er cybersikkerhed? Begreber: CIA, privacy, datatyper, trusselvektorer Workshop: Identificer trusler i dagligdagen
Tirsdag	Adgangskontrol: opbygning af adgangs- og passwordpolitikker Gruppearbejde: Lav jeres egen passwordpolitik for et fiktivt firma
Onsdag	Etik og interessekonflikter i sikkerhedsarbejde Rollespil/cases: Hvad gør man når privatliv, sikkerhed og forretning kolliderer?
Torsdag	Introduktion til risikovurdering Mini-øvelse: Vurder sikkerhedsrisici i en hverdagssituation
Fredag	Intro til machine learning i cybersikkerhed Refleksion: Hvad har jeg lært? Hvordan påvirker det mit syn på IT? Quiz eller samtale som formativ evaluering

Materialer

- Begynderkompendium om cybersikkerhed (eget eller fra CFCS)
- Slides med begrebsforklaringer og eksempler
- Case-ark til rollespil og diskussion
- Video-intro fra f.eks. OWASP, Center for Cybersikkerhed eller EU's ENISA

Værktøjer

- Kahoot eller Socrative til quiz
- Google Docs eller Padlet til gruppearbejde og refleksion
- Canva eller PowerPoint til at lave adgangskontrolpolitikker
- (Evt. simuleret adgangsstyring i f.eks. Windows/Moodle hvis tid)

Evaluering

- Formativ quiz eller samtale fredag
- Bedømmelse af elevens adgangskontrolpolitik og deltagelse i cases
- Observation af begrebsforståelse og refleksion

Undervisningsplan H2 Cybersikkerhed

Fag:

- 22849 Informations- og cybersikkerhed H2 (1,5 uge)

Kompetencemål: 44, 45, 47, 48, 51, 54

Læringsmål

- Forstå og kunne forklare formålet med ISO 27001 og 27002
- Kende centrale aktører som Center for Cybersikkerhed og CIS
- Anvende principper for multifaktorautentifikation (MFA)
- Overføre viden om fysisk adgangssikring til konkrete løsningsforslag
- Forstå begreber som compliance, regulering og beredskabsplan

Undervisningsaktiviteter

Dag	Aktivitet
Mandag	Intro til informationssikkerhed som styringsdisciplin Gennemgang af ISO 27001/27002 Gruppearbejde: Find kontroller i standarderne og forklar dem for klassen
Tirsdag	Compliance og governance: Hvad betyder det for virksomheder? Case: GDPR-krav i praksis + relation til ISO Diskussionsøvelse: Beredskabsplan – hvad skal med?
Onsdag	Multifaktorautentifikation (MFA): Teori og brugsscenarier Workshop: Opsætning af MFA i f.eks. Google/Microsoft miljø Evaluering af MFA-løsninger
Torsdag	Fysisk sikkerhed: Adgangskontrol, overvågning og implementering Designøvelse: Lav en fysisk sikringsplan for en case-virksomhed Peer-feedback på løsningsforslag
Fredag	Opsamling: Sammenhæng mellem fysisk og logisk sikkerhed Gruppearbejde: Udarbejd sikkerhedspolitik med både ISO, MFA og fysisk sikring Fremlæggelse og refleksion

Materialer

- Introduktion til ISO 27001/27002 (uddrag eller oversigtsdokumenter)
- CFCS materiale om fysisk sikkerhed

- MFA-dokumentation fra f.eks. Microsoft eller Google
- Case-beskrivelser af fiktive virksomheder

Værktøjer

- Canva / Google Slides til planlægning og visualisering
- Google/Microsoft-konti til MFA-øvelser
- Draw.io eller papir til fysisk sikkerhedsdesign
- Quizværktøjer (Socrative / Kahoot)

Evaluering

- Produkt: Politisk dokument eller fysisk sikringsplan
- Mundtlig: Fremlæggelse og begrundelser
- Observation og samtaler i løbet af ugen
- (Evt. quiz om compliance og MFA-principper)

Undervisningsplan H3 Cybersikkerhed

Tema 1: Infrastruktur og netværkssikkerhed

Kompetencemål: 48, 49, 50, 51, 52

Fag:
- 22865 Network Security 1 (2 uger)
- 22850 Informations- og cybersikkerhed H3 (delvis, 1 uge)

Læringsmål:
- Implementere sikkerhed på netværksenheder
- IDS/IPS, logning, segmentering og topologier
- Forstå sikkerhed i IT/OT kontekst og risikovurdering
- Forstå cloud-baseret sikkerhed og proaktive strategier

Aktiviteter:
- Konfigurere routere, switche og firewalls i virtualiseret lab (f.eks. Cisco Packet Tracer eller GNS3)
- Simulere og analysere netværksangreb (f.eks. DoS, ARP-spoofing)
- Udarbejde fysisk og logisk netværksdiagram med sikkerhedsannotering
- Udarbejde en risikovurdering og mitigeringsplan for en fiktiv virksomhed

Evaluering:
- Praktisk test (opsætning og konfiguration)
- Skriftlig opgave: netværkssikkerhedsdesign
- Mundtlig fremlæggelse af risikovurdering

Materialer:
- Cisco Networking Academy (moduler om routing, switching og netværkssikkerhed)
- **Kursusbog**: "Network Security Essentials" af Stallings eller lignende dansk oversættelse
- OWASP Network Security Cheat Sheets
- ISO 27001 / 27002 uddrag (på dansk hvis muligt)
- Artikler/cases fra *Center for Cybersikkerhed (CFCS)*
- "Cyber Kill Chain" og MITRE ATT&CK framework (introduktion)

Værktøjer:
- **Cisco Packet Tracer** *(gratis via Cisco NetAcad for skoler)*
- **GNS3** *(open source netværkssimulator – kræver lokal opsætning)*
- **Wireshark** *(gratis netværkssniffer)*
- **pfSense** *(open source firewall-løsning)*
- **Security Onion** *(open source IDS/IPS og SIEM-pakke)*

- **Draw.io / Diagrams.net** *(gratis online værktøj til netværksdiagrammer)*

Tema 2: Databeskyttelse og informationssikkerhed

Kompetencemål: 44, 45, 48, 49, 56, 62

Fag:
- 22857 Data Security 1 (1 uge)
- 22850 Informations- og cybersikkerhed H3 (delvis, 1 uge)

Læringsmål:
- Anvende datasikkerhedsprincipper (klassifikation, adgangskontrol, backup)
- Forstå og arbejde med GDPR og compliance
- Forstå DRP, IRP og BCP
- Kommunikere sikkerhedspolitikker

Aktiviteter:
- Klassificering af data i case-virksomhed
- Udarbejde backupstrategi baseret på 3-2-1-1-0 modellen
- Workshop i GDPR og incident response
- Design af awareness-kampagne

Evaluering:
- Skriftlig prøve i GDPR og datasikkerhedsprincipper
- Fremlæggelse af sikkerhedsstrategi og politik for ledelsen i case

Materialer:
- Datatilsynets vejledninger og GDPR-forståelse for IT-fagpersoner
- *NIS2-direktivet* i praksis – uddrag og konsekvenser
- Artikler fra Dansk IT om *compliance og governance*
- *Backup & Restore* whitepapers fra Veeam eller Acronis
- Vejledning i risikovurdering fra ISO 27005 eller CIS Controls

Værktøjer:
- **Threat Dragon (OWASP)** *(open source threat modeling tool)*
- **Veeam Community Edition** *(gratis til test og backup-simulationer)*
- **Canva Education / Google Slides** *(gratis til awareness-kampagner – kræver login)*
- **Helk** (Elastic stack til analyse – alternativ hvis Splunk ikke bruges)

Tema 3: Endpoints og applikationssikkerhed

Kompetencemål: 47, 48, 49, 50, 51, 52, 53, 56, 57, 59

Fag:
- 22862 Endpoint Security 1 (2 uger)
- 22854 Application Security 1 (1 uge)

Læringsmål:
- Identificere trusler mod endpoints og sikre disse
- Anvende og forklare EDR, SIEM og SOC
- Implementere inputvalidering og sikker kodning
- Forstå patch management og OWASP

Aktiviteter:
- Opsætning af endpoint-sikkerhed i lab (EDR, AV, BYOD-politik)
- Analyse af logfiler og SIEM-opsætning
- Workshop i OWASP Top 10 og sikring mod XSS/SQLi
- Kodesprint: rette usikre kodeeksempler

Evaluering:
- Praktisk case: sikre endpoints og dokumentere politik
- Skriftlig test i applikationssikkerhed
- Gruppefremlæggelse: sikkerhedsanalyse af en webapplikation

Materialer:
- OWASP Top 10 dokumentation og cheat sheets
- Eksempler på sårbar kode (f.eks. deliberately vulnerable web apps som DVWA eller Juice Shop)
- Artikler: "Endpoint Security Explained", “BYOD Security Guidelines”
- NIST SP 800-53 og SP 800-171 (uddrag for endpoint og applikation)

Værktøjer:
- **OWASP Juice Shop**, **DVWA**, **WebGoat** *(alle open source og designet til undervisning)*
- **Burp Suite Community Edition** *(gratis version til sårbarhedsanalyse)*
- **OpenEDR** *(open source endpoint detection tool fra Comodo)*
- **Wazuh** *(open source SIEM/EDR platform – kræver lidt opsætning)*
- **ClamAV** *(gratis antivirus, til demonstration og forståelse)*
- **Visual Studio Code** *(gratis editor)*

Afslutning af H3-forløbet – Cybersikkerhed

Samlet evaluering:

- **Portfolio**: Eleverne samler centrale produkter fra forløbet, fx netværkstopologier, backupplaner, EDR-konfigurationer, loganalyser og opgaver i sikker kodning.
- **Afsluttende øvelse**: Eleverne arbejder i små grupper med en tværgående opgave, hvor de skal analysere sikkerhedsbehov for en fiktiv virksomhed og foreslå konkrete løsninger på netværks-, data- og endpoint-niveau.
- **Mundtlig fremlæggelse**: Grupperne fremlægger deres løsning med fokus på trusselsbillede, valg af teknologier, anvendte principper (f.eks. CIA, Zero Trust) og dokumentation.
- **Feedback**: Læreren giver både faglig og formativ feedback med fokus på styrker, læringspotentiale og samarbejde.

Formål:
Afslutningen skal:

- Give eleverne mulighed for at integrere og anvende det lærte i praksis
- Understøtte mundtlig og skriftlig formidling af cybersikkerhedsfaglige beslutninger
- Forberede eleven på mere selvstændige og komplekse opgaver i H4

Undervisningsplan H4 Cybersikkerhed

Tema 1: Applikationssikkerhed og softwarearkitektur

Fag:
- 22855 Application Security 2 (2 uger)

Kompetencemål: 44, 47, 48, 49, 51, 57

Læringsmål:
- Anvende sikker udvikling og autentifikation
- Implementere OWASP principper og patch management
- Forstå og anvende kryptografi og API-sikkerhed
- Udføre sikkerhedstest i SDLC

Aktiviteter:
- Gennemgang af OWASP Top 10 og Secure Coding Guidelines
- Øvelse i inputvalidering og sikring af formularer (XSS, SQLi)
- Konfiguration af API-sikkerhed med tokens
- Trusselsmodellering i OWASP Threat Dragon
- Introduktion til penetrationstest i Juice Shop

Evaluering:
- Opgave: Sikkerhedsrevision af en demoapplikation
- Praktisk: Implementere sikker inputvalidering
- Fremlæggelse: Trusselsmodel og mitigeringstiltag

Materialer:
- OWASP Cheat Sheets
- Introduktion til SDLC og DevSecOps
- Introduktion til moderne API sikkerhed

Værktøjer:
- OWASP Juice Shop
- OWASP Threat Dragon
- Burp Suite Community
- Visual Studio Code
- GitHub

Tema 2: Endpoint- og datasikkerhed

Fag:
- 22863 Endpoint Security 2 (1 uge)
- 22858 Data Security 2 (1 uge)

Kompetencemål: 43, 44, 47, 48, 49, 51, 52, 56, 62

Læringsmål:
- Udføre patch management og EDR-konfiguration
- Planlægge og dokumentere backup- og gendannelsesstrategier
- Implementere compliance og databeskyttelse
- Anvende risikovurdering og formidle sikkerhedsstrategier

Aktiviteter:
- Konfigurere endpointbeskyttelse i Wazuh eller OpenEDR
- Scanning og patching med OpenVAS
- Øvelse i at udarbejde backupstrategi (3-2-1-1-0)
- Workshop i GDPR og NIS2: "Compliance i praksis"
- Simulering: analyse af databrud og kommunikation til ledelse

Evaluering:
- Rapport: Backup- og gendannelsesstrategi
- Mundtlig: Compliance review og præsentation
- Praktisk: Opsætning af EDR + risikovurdering

Materialer:
- Datatilsynets vejledninger
- NIS2-overblik
- ISO 27001 principper

Værktøjer:
- Wazuh / OpenEDR
- Veeam CE (eller simulering)
- OpenVAS
- Canva / Google Slides
- Excel / skabeloner til risikovurdering

Tema 3: Netværkssikkerhed og segmentering

Fag:
- 22866 Network Security 2 (1 uge)
- 22851 Informations- og cybersikkerhed H4 (delvis 1 uge)

Kompetencemål: 43, 44, 45, 47, 48, 49, 51, 56

Læringsmål:
- Implementere VPN, IDS/IPS og microsegmentering
- Anvende firewall- og adgangskontrolprincipper
- Vurdere behovet for logning og alarmer
- Forstå cloud-infrastruktur og livscyklus

Aktiviteter:
- Opsætning af pfSense firewall og IDS/IPS
- Simulering af fjernadgang med VPN-konfiguration
- Workshop: Zero Trust og microsegmentering
- Analyse af netværkstrafik og alarmer med Wireshark
- Dokumentere netværksdesign i Draw.io

Evaluering:
- Praktisk prøve: Konfiguration af firewall + segmentering
- Skriftlig rapport: Netværkssikkerhedsdesign
- Gruppearbejde: Netværksovervågning og analyse

Materialer:
- Cisco sikkerhedsvejledninger
- OWASP Network Security dokumentation
- ITIL Change Management overblik

Værktøjer:
- pfSense
- Wireshark
- GNS3
- Draw.io

Tema 4: Detektion, respons og SOC-arbejde

Fag:
- 22860 Detektion & Respons 1 (1 uge)
- 22851 Informations- og cybersikkerhed H4 (delvis 1 uge)

Kompetencemål: 43, 44, 45, 47, 49, 51, 52

Læringsmål:
- Anvende SOC-principper og SIEM
- Forstå incident response og analyse
- Implementere overvågning og alarmstrukturer
- Sammenkoble logkilder og vurdere hændelser

Aktiviteter:
- Konfiguration af Security Onion med logkilder
- Øvelse: Identifikation af indikatorer på kompromittering
- Workshop: SOC-roller og logflow
- Mini-forensic analyse med brug af SIEM
- Refleksionsopgave: SOC-arkitektur og best practice

Evaluering:
- Loganalyse: Hændelsesbeskrivelse og rapport

- Opgave: Design af SOC-light løsning for SME
- Fremlæggelse: Incident-håndteringsplan

Materialer:
- MITRE ATT&CK Framework
- NIST Incident Response Guide
- SOC2 og ISO relateret teori

Værktøjer:
- Security Onion
- ELK Stack
- SIEM simulatorer (f.eks. Splunk Free, Wazuh)
- Event logs (simulerede eller reelle)

Afslutning af H4-forløbet – Cybersikkerhed

Samlet evaluering:
- **Faglig portfolio**: Eleverne samler og afleverer dokumentation for arbejdet gennem forløbet – herunder risikovurderinger, sikkerhedskonfigurationer, backupstrategier, logging-analyser og projektresultater.
- **Afsluttende mini-projekt**: I grupper eller individuelt arbejder eleverne med en afsluttende case (fx "Sikkerhedsstrategi for en mindre virksomhed"), hvor de integrerer læring fra temaerne: netværk, endpoints, data og compliance.
- **Mundtlig fremlæggelse**: Eleverne præsenterer deres projektløsning og begrunder valg af teknologier, metoder og prioriteter – med fokus på hvordan de opfylder konkrete sikkerhedsbehov og overholder lovgivning.
- **Refleksion**: Eleverne skriver kort refleksion over deres egen faglige progression, samarbejde og nye erkendelser.

Formål:
Afslutningen skal styrke:
- Sammenhæng mellem teori og praksis
- Elevens evne til at analysere og formidle sikkerhedsfaglige løsninger
- Klarhed over egne kompetencer og områder for videre udvikling

Undervisningsplan – H5 Cybersikkerhed (8 uger)

Tema 1: Avanceret netværkssikkerhed og penetrationstest

Fag:
- 22867 Network Security 3 (2 uger)

Kompetencemål: 43, 44, 47, 49, 56, 57

Læringsmål:
- Evaluere netværk via scanning og sårbarhedstest
- Designe planer for hændelseshåndtering
- Udføre kontrollerede tests (blackbox/whitebox)
- Dokumentere og formidle tekniske fund

Aktiviteter:
- Planlægning og udførelse af sårbarhedsscanning og sikkerhedstest på virtuel infrastruktur
- Workshop i trusselsanalyse og netværkshærdning
- Udarbejdelse af teknisk rapport og forbedringsforslag
- Øvelse i at analysere angrebsvektorer og foreslå mitigerende tiltag

Evaluering:
- Praktisk: Scanning og netværksgennemgang
- Skriftlig: Sikkerhedsstrategi og dokumentation
- Fremlæggelse: Resultater og forslag

Materialer:
- MITRE ATT&CK + OWASP Testing Guide
- Eksempler på sikkerhedsrapporter
- Dokumentation for netværksarkitektur og hændelser

Værktøjer:
- Kali Linux
- Nmap / Wireshark / OpenVAS
- OWASP ZAP
- Draw.io / GitHub

Tema 2: Applikationssikkerhed og dokumentation

Fag:
- 22856 Application Security 3 (1 uger)

Kompetencemål: 42, 44, 47, 51, 56, 57

Læringsmål:
- Anvende og vurdere sikkerhedspolitikker
- Udføre logging, penetrationstest og white/blackbox test
- Dokumentere løsninger og forklare SBOM og DLP
- Identificere AI-relaterede risici

Aktiviteter:
- Gennemføre whitebox/blackbox test på webapplikation
- Udarbejde SBOM og dokumentere afhængigheder
- Workshop: AI-sikkerhed og undtagelseshåndtering
- Simulere DLP-politikker i case

Evaluering:
- Skriftlig opgave: Anvendelse af sikkerhedsarkitektur
- Præsentation: AI i sikkerhedsdesign
- Praktisk: Analyse af logging og undtagelser

Materialer:
- OWASP SBOM-retningslinjer
- DLP-principper og cases
- Vejledninger til AI i cybersikkerhed

Værktøjer:
- OWASP Juice Shop
- GitHub + SBOM-generator
- Logindsamling via Elastic eller Wazuh
- Burp Suite

Tema 3: Detektion, respons og analyse

Fag:
- 22861 Detektion & Respons 2 (1 uge)
- 22852 Informations- og cybersikkerhed H5 (1 uger)

Kompetencemål: 45, 49, 52, 56, 60

Læringsmål:
- Udføre forensic analyser
- Implementere automatiseret incident response
- Eskalere og dokumentere hændelser
- Analysere trusselsdata og logmønstre

Aktiviteter:
- Loganalyse og forensic case (eks. fra kompromitteret endpoint)
- Arbejde med SIEM, EDR og eskalationsplaner

- Opbygge og afprøve incident response procedure
- Træning i tværfaglig kommunikation

Evaluering:
- Praktisk analyse: Forensic & logdata
- Mundtlig evaluering af incident respons
- Opgave: Dokumenteret hændelseshåndtering

Materialer:
- NIST IR-planer
- MITRE logkæder og angrebsflows
- Eskalations- og kommunikationsskemaer

Værktøjer:
- Security Onion
- Wazuh / ELK
- Velociraptor / Autopsy (open source forensic tools)
- SIEM-simulator

Tema 4: Strategisk datasikkerhed og forberedelse til specialisering

Fag:
- 22859 Data Security 3 (1 uge)
- 22864 Endpoint Security 3 (2 uger)

Kompetencemål: 44, 45, 46, 47, 48, 49, 51, 52, 55, 56, 58

Læringsmål:
- Udvikle incident response og strategisk dokumentation
- Evaluere og implementere IoT- og BYOD-sikring
- Planlægge træningsinitiativer og awareness
- Bidrage til organisations datasikkerhedsstrategi

Aktiviteter:
- Udarbejde backup- og DLP-strategi
- Dokumentere sikkerhedshændelser og udarbejde awareness materiale
- Planlægge sikkerhedstræning for medarbejdere
- Afsluttende projekt med præsentation for “ledelse”

Evaluering:
- Projekt: Dokumenteret strategi og træning
- Praktisk: Endpoint sikring og DLP-simulering
- Præsentation og portfolio-gennemgang

Materialer:

- ISO 27001 skabeloner
- Awareness kampagner (eksempler fra Erhvervsstyrelsen)
- Artikler om BYOD og fremtidens sikkerhed

Værktøjer:

- Canva / Google Sites
- Wazuh / MDM-simulator
- Autopsy / SIEM-loganalyser

Afslutning af H5-forløbet – Cybersikkerhed

Samlet evaluering:

- **Faglig portfolio**: Eleven afleverer en samlet dokumentation med løbende arbejdspapirer, rapporter og refleksioner fra hele H5-forløbet.
- **Afsluttende opgave/case**: Eleven udvælger en central opgave (fx pentest, incident response, datasikkerhedsstrategi), som uddybes og præsenteres med fokus på metode, resultater og læring.
- **Mundtlig fremlæggelse**: Eleven præsenterer sit afsluttende arbejde, herunder sikkerhedsfaglige overvejelser, anvendte værktøjer og egne refleksioner om rollen som cybersikkerhedsmedarbejder.
- **Feedback og vejledning**: Læreren giver individuel feedback, og eleven reflekterer over sin udvikling og fremtidige faglige retning.

Formål:

Afslutningen skal understøtte:

- Eleven i at skabe sammenhæng i sin læring
- Dokumentation af opnåede kompetencer
- Forberedelse til specialisering og svendeprøve

Undervisningsplan – H6 Cybersikkerhed

Titel: *"Cybersikkerhedsløsning til en virksomhed – fra risiko til respons"*

Dette undervisningsforløb i H6-modulet sigter mod at samle og anvende elevernes faglige og praktiske kompetencer inden for cybersikkerhed. Forløbet strækker sig over fem uger og kombinerer teoretisk indsigt med anvendelsesorienterede aktiviteter, som leder frem mod svendeprøven.

I den første uge arbejder eleverne med grundlæggende teorier og begreber inden for informations- og cybersikkerhed. De introduceres til risikovurdering, adgangskontrol, etik og machine learning i sikkerhedskonteksten. Målet er at etablere et fælles begrebsapparat og et analytisk udgangspunkt, som resten af forløbet bygger videre på.

De efterfølgende fire uger er projektbaserede og tager udgangspunkt i en realistisk case, hvor eleverne i grupper skal designe og implementere en komplet cybersikkerhedsløsning til en fiktiv virksomhed. Projektet omfatter både teori og og fysisk opsætning, herunder netværksdesign, endpoint- og applikationssikkerhed, backupstrategi og detektion/respons. Et centralt element er, at eleverne ikke kun teoretiserer, men også konfigurerer, scanner og tester konkrete systemer og dokumenterer resultaterne.

Forløbet lægger vægt på at udvikle elevernes evne til at arbejde struktureret med komplekse problemstillinger, kombinere tekniske og organisatoriske tiltag og formidle deres løsninger professionelt – både teknisk og forretningsmæssigt.

Ved afslutningen af forløbet skal eleverne kunne demonstrere, at de behersker de færdigheder og den helhedsforståelse, der forventes af en datatekniker med speciale i cybersikkerhed.

Uge 1: Informations- og cybersikkerhed (Opstart og teori)

Fag:

- 22853 Informations- og cybersikkerhed H6 (1 uger)

Fagligt fokus:

- Grundbegreber: privacy, trusselvektorer, risikovurdering
- Adgangskontrol, passwordpolitikker
- Interessekonflikter og etisk beslutningstagning
- Introduktion til machine learning i sikkerhed

Læringsmål:

- Eleven kan udføre og dokumentere risikovurderinger og foreslå mitigeringsstrategier

- Eleven forstår grundlæggende sikkerhedskomponenter i IT/OT og designprincippers betydning
- Eleven kan identificere sikkerhedskomponenter i automatiseringsløsninger

Undervisningsaktiviteter:

- Casebaseret risikovurdering af fiktiv virksomhed
- Udarbejdelse af adgangskontrolpolitik
- Diskussionsøvelse: etiske dilemmaer i cybersikkerhed
- Workshop i brugen af SIEM-data til detektionsformål

Uge 2-5: Svendeprøveprojekt

Projektformål

Eleverne skal i grupper designe, implementere og dokumentere en realistisk **cybersikkerhedsløsning** til en fiktiv virksomhed. Projektet skal vise, at eleverne:

- Behersker teoretiske og praktiske færdigheder inden for netværk, data, endpoints og applikationer.
- Kan gennemføre risikovurdering, design og tests af løsninger
- Kan integrere lovgivning, compliance og anbefalinger
- Kan dokumentere og formidle deres arbejde til både tekniske og ikke-tekniske modtagere

Projektindhold

Gruppen skal:

1. **Analyse & Planlægning**
    - Udføre risikovurdering af virksomhedens IT- og OT-miljø
    - Identificere relevante trusler og sårbarheder
    - Udforme en overordnet cybersikkerhedsstrategi
    - Udarbejde trusselsmodeller og prioritering

2. **Design & Implementering**
    - Fysisk opsætning af netværk og udstyr i lab:
        - Implementering af netværk med routere, switche og firewall (f.eks. pfSense)
        - Segmentering af netværket og brug af VLAN
        - Opsætning af endpoint-sikkerhed (klienter, BYOD mv.)
    - Implementering af:
        - Applikationssikkerhed med sikre kodestumper (f.eks. Juice Shop + inputvalidering)
        - Backupstrategi (f.eks. 3-2-1-1-0-modellen)

- Logning og SIEM-løsning (f.eks. Wazuh/Elastic Stack)
- Incident Response Plan (IRP) og eskalationsflow

3. **Test & Validering**
    - Praktiske øvelser:
        - Sårbarhedsscanning (OpenVAS, Nmap)
        - Penetrationstest mod egne systemer
        - Dokumentation og evaluering af fund
        - Anbefaling af mitigeringsforanstaltninger

4. **Dokumentation & Formidling**
    - Udarbejdelse af:
        - Teknisk dokumentation og netværkstopologi
        - Cybersikkerhedspolitik og awareness-materiale
        - Forretningsrettet oversigt til "ledelsen" (ikke-teknisk målgruppe)
    - Mundtlig præsentation med visning af fysisk opsætning og testresultater