CyberAgent

Co-funded by the European Union

EQF NIVÅ 4-5

OPPLÆRINGSMODULER FOR YRKESUTDANNINGSSTUDENTER

CYBERAGENT 01.2025

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Finansiert av Den europeiske union. Synspunkter og meninger som kommer til uttrykk er imidlertid kun forfatterens/forfatternes og gjenspeiler ikke nødvendigvis synspunkter og meninger hos Den europeiske union eller Det europeiske utdannings- og kulturbyrået (EACEA). Verken Den europeiske union eller EACEA kan holdes ansvarlig for disse.

www.cyberagents.eu

Arbeidspakke 3: Utvikling av læringsressurser for endringsagenter innen cybersikkerhet

Leveranse 3.2: Opplæringsmoduler for yrkesfaglige studenter
Leder for 3.2 – TIMTAL (TR)

INNHOLD

LISTE OVER TABELLER

INNLEDNING

De raske endringene innen vitenskap og teknologi, endrede behov hos enkeltpersoner og samfunnet, innovasjoner og utvikling innen læring og undervisningsteorier og -tilnærminger har hatt direkte innvirkning på de rollene som forventes av enkeltpersoner. Denne endringen definerer en person som produserer kunnskap, kan bruke den funksjonelt i livet, kan løse problemer, tenke kritisk, er initiativrik, målbevisst, har kommunikasjonsevner, kan vise empati, bidrar til samfunnet og kulturen osv.

Den svimlende hastigheten som informasjonsalderen medfører, fører med seg stadig skiftende behov hos enkeltpersoner og samfunn. Innovasjoner innen læring og undervisningsteorier endrer radikalt rollene som forventes av enkeltpersoner. Nå er det ikke bare kunnskap som teller, men også ferdigheter som å kunne bruke kunnskapen funksjonelt i livet, å kunne finne løsninger på komplekse problemer, å kunne tenke kritisk, å kunne handle med entreprenørånd, å kunne kommunisere effektivt, å kunne vise empati og å kunne tilføre samfunnet verdi. Denne transformasjonen oppmuntrer enkeltpersoner til å stadig lære, tilpasse seg og forbedre seg.

I denne sammenhengen gjennomgår også yrkesopplæringen en stor transformasjon. Tradisjonelle yrker erstattes av nye, teknologifokuserte og stadig utviklende yrker. Cybersikkerhet er av avgjørende betydning i denne endringen. I den digitaliserte verden øker cybersikkerhetsrisikoen i alle sektorer og alle yrker. Cybersikkerhet spiller en viktig rolle på mange områder, fra personopplysninger til beskyttelse av bedriftshemmeligheter, fra sikkerhet i kritisk infrastruktur til sikkerhet i finansielle transaksjoner.

Betydningen av opplæring i cybersikkerhet i yrkesrettet utdanning er ikke begrenset til tekniske ferdigheter. Det omfatter også å utdanne individer som har etiske verdier, høy ansvarsfølelse, er kjent med lovbestemmelser og er åpne for kontinuerlig læring. Cybersikkerhet er nemlig ikke bare et teknisk problem, men også et samfunnsansvar. Derfor er det avgjørende for både individers og samfunnets fremtid å legge nødvendig vekt på opplæring i cybersikkerhet i yrkesrettet utdanning.

Yrkesrettet utdanning omfatter planlegging, forskning, utvikling, organisering og koordinert ledelse, tilsyn og undervisningsaktiviteter for alle yrkesrettede og tekniske utdanningstjenester sammen med landbruk, industri og tjenestesektorer innenfor utdanningssystemets integritet. Målet med disse utdanningsaktivitetene er å utdanne eksperter som vil sikre samfunnets kontinuitet og kvalifisert personell som trengs i alle ledd av produksjonen, og å legge vekt på yrkesrettet opplæring.

Cyber Agent-yrkesutdanningsprogrammet (EQF4-5) er utformet for å forberede enkeltpersoner på cybersikkerhetslivet og er basert på arbeidsmarkedets behov og jobbanalyse. Cyber Agent-læreplanen har som mål å gi kunnskap, ferdigheter, holdninger og atferd som må til for å utføre relevant arbeid og transaksjoner gjennom leksjoner og prestasjoner, mens utdanningsaktivitetene på den annen side er planlagt på en måte som vil forberede enkeltpersoner på arbeidslivet i samsvar med dette rammeverket.

1. MÅLENE MED CYBERAGENT EQF NIVÅ 4-5-PROGRAMMET

Behovet for cybersikkerhet har blitt svært viktig, spesielt i EU-landene, men også over hele verden, og har økt raskt de siste årene. Parallelt med den teknologiske utviklingen har også cyberrisikoer og -trusler endret seg i samme tempo og blitt mer komplekse. Cyberrisikoer og trusler har nådd et potensial som vil føre til mye mer omfattende og negative resultater enn fysiske angrep. Med sektorer som finans, elektronisk kommunikasjon, energi, transport og luftfart som tilbyr tjenester i et sikkert digitalt miljø, har sikring av nasjonal cybersikkerhet blitt en av de viktigste prioriteringene for vårt land. I denne sammenheng er målet å spre cybersikkerhetsopplæring i formell og uformell utdanning, og å utvikle og berike utdanningsinnholdet.

2. DEN EUROPEISKE KVALIFIKASJONSRAMMEN

EU utviklet den europeiske kvalifikasjonsrammen (EQF) som et oversettelsesverktøy for å gjøre nasjonale kvalifikasjoner lettere å forstå og mer sammenlignbare. EQF har som mål å støtte grenseoverskridende mobilitet for lærende og arbeidstakere, fremme livslang læring og profesjonell utvikling i hele Europa.

EQF er et 8-trinns rammeverk basert på læringsutbytte for alle typer kvalifikasjoner, som fungerer som et oversettelsesverktøy mellom ulike nasjonale kvalifikasjonsrammeverk. Dette rammeverket bidrar til å forbedre gjennomsiktigheten, sammenlignbarheten og overførbarheten av folks kvalifikasjoner og gjør det mulig å sammenligne kvalifikasjoner fra ulike land og institusjoner.

EQF dekker alle typer og alle nivåer av kvalifikasjoner, og bruken av læringsutbytte gjør det klart hva en person kan, forstår og er i stand til å gjøre. Nivået øker i henhold til ferdighetsnivået, hvor nivå 1 er det laveste og 8 det høyeste nivået. Det viktigste er at EQF er nært knyttet til nasjonale kvalifikasjonsrammeverk, slik at det kan gi et omfattende kart over alle typer og nivåer av kvalifikasjoner i Europa, som blir stadig mer tilgjengelige gjennom kvalifikasjonsdatabaser.

EQF ble opprettet i 2008 og senere revidert i 2017. Revideringen har beholdt kjerneformålet om å skape åpenhet og gjensidig tillit i kvalifikasjonslandskapet i Europa. Medlemsstatene forpliktet seg til å videreutvikle EQF og gjøre den mer effektiv når det gjelder å legge til rette for forståelse av nasjonale, internasjonale og tredjelands kvalifikasjoner blant arbeidsgivere, arbeidstakere og lærende.

Hvert av de åtte nivåene i EQF er definert av et sett med beskrivelser som angir læringsutbyttet som er relevant for kvalifikasjoner på det nivået i ethvert kvalifikasjonssystem. Læringsutbyttet er definert i form av:

- Kunnskap: I EQF-sammenheng beskrives kunnskap som teoretisk og/eller faktabasert.
- Ferdigheter: I EQF-sammenheng beskrives ferdigheter som kognitive (som involverer bruk av logisk, intuitiv og kreativ tenkning) og praktiske (som involverer manuell fingerferdighet og bruk av metoder, materialer, verktøy og instrumenter).
- Ansvar og autonomi: I EQF-sammenheng beskrives ansvar og autonomi som lærerens evne til å anvende kunnskap og ferdigheter selvstendig og med ansvar.

Tabell1 e læringsutbytte på EQF-nivå 4

Kunnskap	Evne	Ansvar og autonomi
Faktisk og teoretisk kunnskap i brede sammenhenger innenfor et studie- eller læringsfelt	Et sett med kognitive og praktiske ferdigheter som kreves for å finne løsninger på spesifikke problemer innen et arbeids- eller utdanningsfelt	Anvende selvledelse innenfor retningslinjene for arbeids- eller læringskontekster som generelt er forutsigbare, men som kan endres; overvåke andres rutinearbeid, ta noe ansvar for evaluering og forbedring av arbeids- eller læringsaktiviteter

3. CYBERSIKKERHET YRKESFAG STUDENTER (EQF-NIVÅ 4-5)

Cybersikkerhetsmedarbeider (nivå 4-5) er en kvalifisert fagperson som arbeider innenfor informasjonssystemer på arbeidsplassen, deltar i studier av forebyggende tiltak innen cybersikkerhet i forbindelse med sporing av sårbarheter og bevisstgjøring om cybersikkerhet, følger opp tiltak, overvåker driften og bærekraften til systemer som brukes i cybersikkerhetsanalyser, fastsetter kravene til enkle nettverk, setter opp fysiske nettverk, utfører enkle konfigurasjoner relatert til nettverksmaskinvare, sikrer nettverkssikkerhet, vedlikehold og forbedringer, gir teknisk støtte til brukere og gjennomfører faglige utviklingsstudier for å beskytte IT-infrastrukturen på arbeidsplassen mot cybertrusler innenfor rammen av kvalitetskrav ved å implementere tiltak for helse, sikkerhet og miljøvern.

3.1. CYBERAGENT LÆREPLAN FOR EQF-4-5

Yrkesfaglæreplanen (EQF 4-5) ble utviklet ved å strategisk tilpasse den omfattende høyere utdanningslæreplanen (EQF 5-6). Tilpasningsprosessen innebar å konsentrere materialet for å tilpasse det til 1 ECTS-omfang og fokusere på læringsutbyttet som er mest relevant for yrkesfaglig utdanning og SMB-er umiddelbare behov. Prioritet ble gitt til emner som vektlegger praktisk anvendelse og grunnleggende cybersikkerhetsferdigheter, mens mer dyptgående teoretiske konsepter ble strømlinjeformet for å passe til yrkesfaglig utdanning.

Tabell2 -Modul: 1

Enheter	Emner
Prosjektledelse	Prosjektplanlegging Definere prosjektmål Aktuelle cybersikkerhetstrusler (DDoS, ransomware, malware, phishing, zero-day, IoT-angrep osv.)

	Trusselmodellering og sårbarhetsanalyse Rapportering av cybersikkerhetstrusler og hendelser
Læringsutbytte • Deltakerne vil kunne definere prosjektledelsesfaser og lage en grunnleggende prosjektplan. (Anvendelse) • Deltakerne vil kunne formulere klare, målbare og oppnåelige prosjektmål. (Analyse) • Deltakerne vil identifisere, klassifisere og evaluere ulike cybersikkerhetstrusler. (Analyse) • Deltakerne vil utvikle trusselmodeller og utføre sårbarhetsanalyser for spesifikke scenarier. (Anvendelse) • Deltakerne vil utarbeide hendelsesrapporter i henhold til etablerte protokoller. (Anvendelse)	
Ressursstyring	Sikkerhetsverktøy og programvare Effektiv bruk av teknologiske ressurser
Læringsutbytte • Elevene skal demonstrere effektiv bruk av cybersikkerhetsverktøy og programvare for å oppdage og reagere på trusler. (Anvendelse) • Elevene skal optimalisere teknologiske ressurser for økt sikkerhet og effektivitet. (Anvendelse)	
Sikkerhetsmålinger	Sikkerhetsmetrikker og målingsteknikker Datainnsamling med SIEM Analyse av sikkerhetsmetrikker Prosjektoppfølging og ytelsesevaluering Rapportering av sikkerhetsmetrikker
Læringsutbytte • Deltakerne vil identifisere og anvende relevante sikkerhetsmetrikker og måleteknikker. (Anvendelse) • Deltakerne skal konfigurere og bruke SIEM-verktøy for datainnsamling og sikkerhetsovervåking. (Anvendelse) • Deltakerne skal tolke og analysere sikkerhetsmålinger for å vurdere sikkerhetssituasjonen. (Analyse) • Deltakerne skal overvåke og evaluere prosjektets ytelse ved hjelp av sikkerhetsmetrikker. (Evaluering) • Deltakerne skal sammenstille og presentere rapporter basert på analyse av sikkerhetsmetrikker. (Anvendelse)	
Kvalitetssikring og kvalitetskontroll	Kvalitetsstyring Kvalitetsstandarder innen cybersikkerhet Test- og valideringsteknikker
Læringsutbytte: • Lærerne vil implementere kvalitetsstyringspraksis i cybersikkerhetsprosjekter. (Anvendelse) • Lærerne vil identifisere og anvende relevante kvalitetsstandarder for cybersikkerhet. (Anvendelse) • Lærerne skal utvikle og gjennomføre test- og valideringsprosedyrer for cybersikkerhetsløsninger. (Anvendelse)	

Tabell3 -Modul: 2

Enheter	**Emner**
Administrasjon av operativsystemer	Operativsystemer Forholdet mellom maskinvare og programvare Binære tall, heksadesimal telling Biter og byte Kommandolinje i operativsystemet Windows- og Linux-kommandoer Windows-klient og -server Programmer, prosesser og tjenester i Windows Filtyper og filformater Registernøkler og verdier Kontrollpanelinnstillinger Brukere og grupper Domenestruktur og serveradministrator AD og GPO Linux-grensesnitt og kjernen Prosesser i Linux Navngivningskonvensjoner for filer og kataloger Linux-skall og kommandosyntaks Manipulering av filer og mapper Arbeide med kommandoer for overvåking av rør og systemer Prosessstyring og jobbkontroll Tjenestestyring
Læringsutbytte: • Lærerne skal sammenligne og kontrastere ulike operativsystemer og deres arkitekturer. • Lærerne skal forklare samspillet mellom maskinvare og programvare i et operativsystemmiljø. • Lærerne skal utføre binære og heksadesimale konverteringer og forstå datarepresentasjon. • Lærerne vil utføre grunnleggende kommandoer i Windows- og Linux-miljøer. • Lærerne skal administrere applikasjoner, tjenester og prosesser ved hjelp av systemverktøy. • Elevene skal konfigurere og administrere Active Directory og GPO-er. • Elevene skal samhandle med Linux-grensesnitt og utføre operasjoner på kjernenivå. • Elevene skal administrere tjenester og systemprosesser ved hjelp av Linux-kommandoer.	

Administrasjon av databasesystemer	Repositorier og kildelister Administrere en webserver Systemlogger og loggovervåking Planlegging av oppgaver i Linux Feilsøking av server og nettverk Sikkerhetskopiering og gjenoppretting Sikring av GRUB Brannmurer Active Directory-objekter og GPO-administrasjon DNS og DHCP Grunnleggende om PowerShell Microsoft BitLocker, AppLocker og brannmur LDAP og Kerberos NTLM Passord- og låsepolitikker Autentisering og tilgangskontroll Internet Control Message Protocol (ICMP) TCP vs UDP NetBIOS og SMB SSL og TLS Sertifikater Telnet og Secure Shell (SSH) protokoller HTTP og HTTPS E-postsystemprotokoller Domain Name System Protocol (DNS) FTP og RDP Innkapsling vs. utkapsling Nettverkssniffere og Wireshark TCP/UDP DHCP, DNS
Læringsutbytte: • Deltakerne skal konfigurere repositorier og administrere kildelister. • Deltakerne skal analysere og overvåke logger for feilsøking og sikkerhet. • Deltakerne skal utføre sikkerhetskopiering og gjenoppretting for å sikre dataintegriteten. • Deltakerne vil implementere sikkerhetstiltak, inkludert brannmurer, BitLocker og AppLocker.	
Nettverksadministrasjon	Nettverkstyper og trådløse nettverk Nettverk og topologier Enheter Identitet og tilgangsenheter Infrastruktur og sikkerhetsenheter Spesialiserte enheter og nettverksarkitektur Virtuelle nettverk Fysiske og logiske adresser OSI og nettverksmodeller Datakapsling og dekapsling Nettverksprotokoller og portnumre Nettverksmedier og kabler

	Trådløse teknologier Verktøy for nettverksadministrasjon Cisco Packet Tracer Nettverksklasser og undernett Adresseresolusjonsprotokoll (ARP) Statisk vs. dynamisk IP-adressering Nettverksadresseoversettelse (NAT) Switcher og Cisco IOS Switches port sikkerhet og rutergrensesnitt Konfigurering av VLAN-er og DTP Ruting mellom VLAN-er Introduksjon til ACL-er Feilsøking i nettverk
Læringsutbytte: • Deltakerne vil designe og administrere nettverk, forstå protokoller og topologier. • Deltakerne vil konfigurere VLAN-er, ACL-er og administrere IP-adresseringsskjemaer. • Deltakerne vil bruke verktøy som Wireshark og Cisco Packet Tracer til overvåking og feilsøking.	
Skyadministrasjon	Hypervisorer og virtuelle maskiner Containere Sikring av virtuelle miljøer Sikkerhetskopiering og gjenoppretting Skyberegning og CSP-er Hva er skytjenestemodeller Typer av skyimplementering Virtuelle nettverk AWS-databehandlingstjenester Amazon Elastic Compute Cloud (EC2) Verktøy for skymonitorering Automatiserings- og orkestreringsverktøy Sikkerhetstrusler og sårbarheter i skyen Identitets- og tilgangsstyring (IAM) Rollebasert tilgangskontroll (RBAC) Multifaktorautentisering (MFA) Kryptering av skydata Virtuell privat sky (VPC) Docker og Kubernetes
Læringsutbytte: • Deltakerne vil administrere virtuelle miljøer ved hjelp av AWS, Docker og Kubernetes. • Deltakerne vil implementere sikkerhetskontroller og identitetsadministrasjon i skyen.	
Administrasjon av cyber-fysiske systemer	Sikkerhet og tilgangskontroll Autentiseringstyper TACACS+ og RADIUS AAA-konfigurasjon Risikostyringsmål Kryptering og dekryptering Hashing og regnbuetabeller MAC-spoofing og ARP-forgiftning

	VLAN-hopping og rogue DHCP ICMP-flom TCP- og UDP-flom Sesjonskapring DNS-spoofing Defense in Depth (DID) og Zero Trust Demilitariserte soner (DMZ) Honeypots og nettverkssikring Beste praksis for et sikkert nettverk VPN SSH og VNC Stateful vs. stateless brannmurer Vertbaserte vs. nettverksbaserte Maskinvare- vs. programvarebrannmurer Webapplikasjonsbrannmur (WAF) AI i brannmurer IDS og IPS NIDS og HIDS Snort tcpdump
Læringsutbytte: • Deltakerne vil sikre nettverk ved hjelp av brannmurer, IDS/IPS og verktøy for trusseloppdagelse. • Deltakerne vil anvende krypteringsteknikker og administrere sikkerhetsprotokoller.	
Systemherding	GenAI-teknikker Kodegenerering Brukerkontoadministrasjon og tilgangskontroll Deteksjon av avvik og feilsøking Løse Apache2-tjenestefeil Patchadministrasjon og oppdateringer Automatisk sikkerhetskopiering og gjenoppretting Gjenoppretting av slettede filer med GenAI Prosedyrer for cybersikkerhet Trusseloppdagelse og analyse Truerespons og utbedring Utnyttelse av AI for trusseloppdagelse i sanntid Validering og testing av GenAI-modeller DNS-konfigurasjon og sikkerhet DHCP-konfigurasjon og sikkerhet Grunnleggende om PowerShell Sikkerhet for switch-porter Network Basic Input/Output System (NetBIOS) Server Message Block Protocol (SMB) Secure Sockets Layer (SSL) og Transport Layer Security (TLS) Sikkerhetssertifikater E-postsystemprotokoller Domain Name System Protocol (DNS) Filoverføringsprotokoll (FTP)

	Fjernskrivebordsprotokoll (RDP) Planlegging av oppgaver i Linux Feilsøking av server Feilsøking av nettverk Sikkerhetskopiering og gjenoppretting Sikring av GRUB Konfigurere og sikre brannmurer
Læringsutbytte: • Deltakerne vil anvende sikkerhetsteknikker for å forbedre systemsikkerheten. • Deltakerne vil utnytte AI til trusseloppdagelse og systemovervåking.	
Systemherding	IR vs. SOC Hendelser og incidenter Deteksjon og prioritering av varsler Dokumentasjon og rapportering Hva er nettangrep? DoS og DDoS SQL-injeksjon og XSS Kommandoinjeksjon og lokal filinkludering (LFI) Cross-Site Request Forgery (CSRF) Brute-Force og Credential Stuffing Pass the Hash og Pass the Ticket Brutt tilgangskontroll Løsepengevirus Datavirus og orm Trojaner og adware Keylogger og kryptojacking Fileløs skadelig programvare Forstå spredningen av skadelig programvare Administrere IOC-er og passordretningslinjer Retningslinjer for akseptabel bruk (AUP) Retningslinjer for bruk av egne enheter (BYOD) Retningslinjer for ekstern tilgang
Læringsutbytte: • Skille mellom de viktigste rollene og samarbeidet mellom R og SOC. • Definere forskjellen mellom sikkerhetshendelser og sikkerhetsbrudd. • Forklar kildene til sikkerhetsvarsler og triageprosesser. • Levere effektiv dokumentasjon og rapportering for sikkerhetshendelser. • Beskrive vanlige typer nettangrep (DoS/DDoS, SQL-injeksjon, XSS, kommandoinjeksjon, LFI, CSRF). • Forklar brute force- og credential stuffing-angrep og gi en oversikt over mottiltakene mot disse. • Forstå de grunnleggende prinsippene for «pass the hash»- og «pass the ticket»-angrep. • Forklar hvordan sårbarheter i brutt tilgangskontroll kan utnyttes. • Forklar ulike typer skadelig programvare (ransomware, virus, orm, trojaner, adware, keylogger, cryptojacking, fileløs skadelig programvare) og hvordan de sprer seg. • Forklar viktigheten av å håndtere indikatorer for trusselinformasjon (IOC). • Skissere nøkkelelementene i sterke passordretningslinjer og retningslinjer for akseptabel bruk (AUP).	

• Evaluer sikkerhetskonsekvensene av BYOD- og fjernadgangsretningslinjer.

Tabell4 -Modul: 3

Enheter	**Emner**
Ytelsesmålinger (metrikker)	Ytelsesmetrikker System- og nettverksovervåking Overvåking av ytelsesmetrikker Nettverkskartlegging Sårbarhetsskanning Analyse av nettverkstrafikk
Læringsutbytte: • Deltakerne skal definere ytelsesmålinger og forklare deres betydning for evaluering av system- og nettverksytelse. • Deltakerne vil demonstrere oppsett og bruk av overvåkingsverktøy for kontinuerlig vurdering av system- og nettverksytelse. • Deltakerne skal analysere og tolke ytelsesmålinger for å vurdere systemets tilstand og identifisere muligheter for optimalisering. • Deltakerne skal lage nettverkskart for å visualisere, overvåke og optimalisere nettverksstrukturer. • Deltakerne skal utføre sårbarhetsskanninger, identifisere sikkerhetsrisikoer og anbefale tiltak for å avhjelpe disse. • Elevene skal utføre nettverkstrafikanalyse for å oppdage og reagere på potensielle trusler.	
Dataanalyse	Datainnsamling Datarengjøring og forbehandling Dataanalyse Datavisualisering Analytiske verktøy Anvendelser av dataanalyse i cybersikkerhet
Læringsutbytte • Deltakerne vil samle inn relevante data fra systemer, nettverk og sikkerhetslogger for analyse. • Deltakerne vil rense og forbehandle rådata for å sikre nøyaktighet og konsistens. • Deltakerne vil anvende statistiske og analytiske teknikker for å utvinne meningsfulle innsikter fra dataene. • Deltakerne vil lage datavisualiseringer for å kommunisere analyseresultatene på en effektiv måte. • Deltakerne vil bruke verktøy som Python, R og Power BI for omfattende dataanalyse. • Elevene vil bruke dataanalyseteknikker for å oppdage, analysere og redusere cybersikkerhetstrusler.	
Sikkerhetsinformasjon	Forstå sikkerhetsinformasjon Kilder til sikkerhetsinformasjon

	Metoder for innsamling av trusselinformasjon Case-studier om sikkerhetsinformasjonsapplikasjoner
Læringsutbytte • Deltakerne skal kunne forklare betydningen av sikkerhetsinformasjon i proaktiv trusselhåndtering. • Deltakerne skal evaluere kilder til sikkerhetsinformasjon, inkludert trusselstrømmer, rapporter og åpne kildekodeverktøy. • Deltakerne skal beskrive metoder for innsamling og analyse av trusselinformasjon. • Deltakerne skal undersøke virkelige tilfeller for å forstå anvendelsen av sikkerhetsinformasjon i forebygging av cybertrusler.	

Tabell5 -Modul: 4

Enheter	**Emner**
Grunnleggende om sikkerhetsoperasjoner	Forståelse av sikkerhetsoperasjoner og SOC (Security Operations Centre) Roller og ansvar i sikkerhetsoperasjoner Oversikt over verktøy og teknologier for sikkerhetsoperasjoner Praktiske eksempler og casestudier
Læringsutbytte • Deltakerne skal kunne forklare formålet med og strukturen til et sikkerhetsoperasjonssenter og dets rolle i cybersikkerhet. • Deltakerne skal beskrive rollene og ansvaret til sikkerhetsoperasjonspersonell, inkludert håndtering av hendelser, trusseljakt og overvåking. • Deltakerne skal identifisere og demonstrere bruken av vanlige verktøy og teknologier for sikkerhetsoperasjoner. • Elevene skal analysere eksempler fra virkeligheten og casestudier for å forstå sikkerhetsoperasjoner i praksis.	
Sikkerhetskonvergens	Forstå sikkerhetskonvergens Grunnleggende om fysisk sikkerhet (prinsipper for fysisk sikkerhet, beskyttelse av fysiske eiendeler, retningslinjer) Vanlige trusler som SMB-bedrifter står overfor Casestudier som belyser konvergensproblemer
Læringsutbytte • Deltakerne skal definere sikkerhetskonvergens og forklare dens betydning for integrering av fysiske og cybersikkerhetstiltak. • Deltakerne vil anvende prinsipper for fysisk sikkerhet for å beskytte eiendeler, fasiliteter og personell. • Deltakerne skal identifisere og evaluere sikkerhetstrusler som små og mellomstore bedrifter (SMB) ofte står overfor. • Deltakerne skal undersøke case-studier for å forstå virkningen av konvergensutfordringer. • Deltakerne skal gjennomgå prosesser for sikkerhetsinformasjon og hendelsesstyring.	
Sikkerhetsinformasjon og hendelsesstyring	Gjennomgang av prinsipper for sikkerhetsovervåking (basert på andre partners moduler) Implementering av SIEM-løsninger

	Oppsett av logger og varsler Gjennomgang av trusselinformasjon og deteksjonsmetoder (basert på andre partners moduler)
Læringsutbytte: • Deltakerne vil kunne forklare prinsippene for sikkerhetsovervåking og deres anvendelse i SIEM-løsninger. • Deltakerne vil konfigurere og betjene SIEM-løsninger for effektiv trusseloppdagelse og respons. • Deltakerne vil sette opp loggførings- og varslingsmekanismer i SIEM-verktøy for å overvåke sikkerhetshendelser. • Deltakerne skal vurdere trusselinformasjon og deteksjonsmetoder for effektive sikkerhetsoperasjoner.	
Sikkerhetsoperasjonspraksis	Overholdelse og regulering Strategier for kontinuerlig forbedring av sikkerhetsoperasjoner Automatisering og koordinering Måling og rapportering
Læringsutbytte: • Deltakerne vil kunne forklare viktigheten av samsvar og regulering i sikkerhetsoperasjoner. • Deltakerne skal utforme og implementere strategier for kontinuerlig forbedring av sikkerhetsoperasjoner. • Deltakerne vil utnytte automatisering og koordinering for å øke effektiviteten i sikkerhetsoperasjoner. • Deltakerne skal utvikle og bruke sikkerhetsmålinger og rapporteringsteknikker for å kommunisere sikkerhetsstatus.	

Tabell6 -Modul: 5

Enheter	**Emner**
Organisatorisk kontekst	Utviklingen av cybersikkerhet i små og mellomstore bedrifter Aktuelle store trusler og sårbarheter Cybersikkerhetens innvirkning på forretningsstrategien Spesifikke utfordringer knyttet til cybersikkerhet i SMB-bedrifter sammenlignet med store bedrifter Forstå de regulatoriske implikasjonene av cybersikkerhetspraksis og hvordan de samsvarer med styringsstrukturer. Vanlige utfordringer knyttet til cybersikkerhet som er spesifikke for SMB-bedrifter, for eksempel begrensede budsjetter, mangel på dedikert sikkerhetspersonell og praktiske metoder for å prioritere investeringer i cybersikkerhet.
Læringsutbytte • Deltakerne vil følge utviklingen av cybersikkerhetspraksis i små og mellomstore bedrifter.	

• Deltakerne vil identifisere og evaluere de mest kritiske aktuelle truslene og sårbarhetene som påvirker SMB-bedrifter. • Deltakerne vil analysere hvordan cybersikkerhet påvirker forretningsstrategi og operasjonelle beslutninger. • Deltakerne vil sammenligne cybersikkerhetsutfordringene som SMB-bedrifter står overfor med de som større organisasjoner møter. • Deltakerne skal tolke regelverkskravene for cybersikkerhet og vurdere hvordan disse integreres i organisasjonens styring. • Deltakerne skal beskrive praktiske løsninger på vanlige cybersikkerhetsutfordringer for SMB-er, for eksempel budsjettbegrensninger og begrenset personell.	
Personvern	Personvernprinsipper i cybersikkerhet Beskyttelse av personopplysninger og GDPR Personvernets innvirkning på SMB-virksomhet Verktøy og teknikker for personvern
Læringsutbytte • Deltakerne skal kunne forklare de grunnleggende personvernprinsippene i sammenheng med cybersikkerhet. • Deltakerne vil anvende GDPR-kravene og vurdere deres innvirkning på personvernet. • Deltakerne skal vurdere hvordan personvernregelverket påvirker SMB-virksomheters daglige drift og forretningsmodeller. • Deltakerne skal bruke verktøy og implementere teknikker for å opprettholde personvernet og beskytte sensitive data.	
Lover, etikk og samsvar	Cybersikkerhetsorganisasjoner, retningslinjer og standarder Relevant nasjonal og internasjonal lovgivning Regulativ etterlevelse i SMB-bedrifter Etikk i cybersikkerhet Juridiske konsekvenser av manglende etterlevelse innen cybersikkerhet Analyse av hvordan AI-baserte verktøy kan brukes til å styrke cybersikkerhetsstyringen og sikre overholdelse gjennom kontinuerlig overvåking og automatisert trusselrespons.
Læringsutbytte • Deltakerne vil identifisere sentrale organisasjoner innen cybersikkerhet og vurdere relevante rammeverk for policyer og standarder. • Deltakerne vil oppsummere viktige lover som påvirker cybersikkerhet på nasjonalt og internasjonalt nivå. • Deltakerne vil utforme strategier for å oppnå og opprettholde regelverksetterlevelse i SMB-sammenheng. • Deltakerne vil undersøke etiske hensyn i beslutningstaking og atferd knyttet til cybersikkerhet. • Deltakerne vil evaluere de juridiske konsekvensene av å ikke overholde lovene om cybersikkerhet. • Deltakerne vil utforske hvordan AI-verktøy kan forbedre styring, automatisere overvåking og forbedre etterlevelse.	
Sikkerhetsstyring	Styringsstruktur for cybersikkerhet Roller og ansvar i sikkerhetsstyring Modeller for modenhet innen cybersikkerhet

	Forbedre evnen til å gjennomføre risikovurderinger og utarbeide strategiske beredskapsplaner under simulerte krisesituasjoner (ransomware, phishing-angrep osv.) Kommunikasjon på ledelses- og styrenivå Kommunikasjonsstrategier for cybersikkerhet Sikkerhetsrapportering til toppledelsen Kriseledelse og kommunikasjon innen cybersikkerhet Mestre krisehåndtering og beslutningstaking i stressende situasjoner som involverer AI-drevne angrep og ransomware.
Læringsutbytte • Deltakerne skal utforme og evaluere styringsstrukturer som støtter effektiv cybersikkerhetsledelse. • Deltakerne vil tildele og avklare ansvar i organisatoriske sikkerhetsrammeverk. • Deltakerne skal vurdere modenheten innen cybersikkerhet ved hjelp av etablerte modeller. • Deltakerne skal gjennomføre risikovurderinger og utvikle responsstrategier for scenarier som ransomware eller phishing. • Deltakerne skal utvikle kommunikasjonsplaner for å formidle innsikt i cybersikkerhet til ledende ansatte og styremedlemmer. • Deltakerne skal formulere effektive kommunikasjonsstrategier for interne og eksterne interessenter innen cybersikkerhet. • Deltakerne skal utarbeide rapporter som informerer toppledelsen om cybersikkerhetsprestasjoner og -risikoer. • Deltakerne vil øve seg på å håndtere og kommunisere under cybersikkerhetskriser, inkludert kriser som involverer AI-drevne angrep.	
Ledelsespolicyer	Implementering og overvåking av policy
Læringsutbytte • Deltakerne vil implementere retningslinjer for cybersikkerhet og etablere prosedyrer for løpende overvåking og håndheving.	

Tabell7 -Modul: 6

Enheter	**Emner**
Introduksjon til planlegging av cybersikkerhet: Data-, menneskelig og samfunnsmessig sikkerhet	Datasikkerhet – sikkerhet ved lagring av informasjon, etterforskningsprosess Datasikkerhet – teknikker for passordangrep Menneskelig sikkerhet – bevissthet og forståelse Samfunnssikkerhet – hva er nettkriminalitet, nettetikk Samfunnssikkerhet – cyberlovgivning – digitale bevis, digitale kontrakter, multinasjonale konvensjoner (avtaler)
Læringsutbytte • Elevene skal implementere strategier for å sikre lagret informasjon og støtte etterforskningsprosesser. • Elevene skal identifisere og analysere vanlige teknikker for passordangrep og utvikle passende mottiltak.	

<table>
<tr><td colspan="2">Elevene skal fremme bevissthet om cybersikkerhet og fremme forståelse blant ansatte og interessenter.
Elevene skal forklare de samfunnsmessige implikasjonene av cyberkriminalitet og vurdere etiske hensyn i digitale miljøer.
Deltakerne vil tolke sentrale begreper innen cyberlovgivning, inkludert digitale bevis, kontrakter og internasjonale avtaler.</td></tr>
<tr><td>Operativ og taktisk ledelse</td><td>Implementering av tilgangskontroll
Patch-administrasjon og programvareoppdateringer
Kontinuerlig systemovervåking
Opplæring i sikkerhetsbevissthet for ansatte</td></tr>
<tr><td colspan="2">Læringsutbytte:
Deltakerne skal utforme og implementere effektive tilgangskontrollmekanismer for å beskytte systemer og data.
Deltakerne vil etablere prosedyrer for rettidig patch-administrasjon og programvareoppdateringer for å redusere sårbarheter.
Deltakerne skal gjennomføre kontinuerlig overvåking av systemer for å oppdage og reagere på sikkerhetshendelser.
Deltakerne skal utvikle og gjennomføre opplæringsprogrammer i sikkerhetsbevissthet for å øke ansattes engasjement og redusere menneskelig risiko.</td></tr>
</table>

Tabell8 -Modul: 7

Enheter	**Emner**
Risikovurdering	Generelt rammeverk og prosess for risikostyring Prinsipper for risikostyring Standarder for risikostyring Praktiske eksempler og casestudier
Læringsutbytte: • Deltakerne skal kunne beskrive og anvende det generelle rammeverket og prosessen for risikostyring innen cybersikkerhet. • Deltakerne skal forklare de grunnleggende prinsippene som ligger til grunn for effektiv risikostyring innen cybersikkerhet. • Deltakerne skal identifisere og tolke allment aksepterte standarder for risikostyring. • Deltakerne skal evaluere risikoscenarier gjennom eksempler fra virkeligheten og casestudier.	
Risikoidentifisering	Konkrete og abstrakte risikokilder Årsaker og hendelser Trusler og muligheter Sårbarheter og evner Endringer i eksterne og interne forhold Indikatorer på nye risikoer Arten og verdien av eiendeler og ressurser Konsekvenser og deres innvirkning på målene Begrensninger i kunnskap og pålitelighet av informasjon Forutinntatte holdninger, antakelser og oppfatninger hos de involverte. Praktiske eksempler og casestudier.
Læringsutbytte: • Deltakerne vil kunne skille mellom konkrete og abstrakte risikokilder i cybersikkerhetsmiljøer. • Elevene skal identifisere årsaker til risiko og utløsende hendelser. • Deltakerne skal analysere cybersikkerhetstrusler og vurdere potensielle muligheter for forbedring. • Deltakerne skal evaluere sårbarheter og organisasjonens evne til å håndtere risiko. • Deltakerne skal vurdere hvordan kontekstuelle endringer påvirker cybersikkerhetsrisikoer. • Elevene skal identifisere indikatorer som signaliserer fremveksten av nye cybersikkerhetstrusler. • Elevene skal vurdere verdien av eiendeler og ressursers kritikalitet i forhold til risiko. • Elevene skal estimere potensielle konsekvenser og deres innvirkning på strategiske mål. • Elevene skal erkjenne begrensningene ved informasjon og kunnskap i risikoidentifiseringsprosessen. • Elevene skal reflektere over hvordan menneskelige faktorer påvirker risikoperception og -identifisering. • Elevene skal anvende identifiseringsteknikker gjennom realistiske scenarier.	

Interne trusler	Definisjon og typer av interne trusler Oppdage og identifisere trusler fra innsiden Praktiske eksempler og casestudier
Læringsutbytte • Deltakerne vil definere trusler fra innsiden og klassifisere de ulike typene. • Deltakerne vil utvikle ferdigheter for å oppdage og reagere på indikatorer på trusler fra innsiden. • Deltakerne skal analysere casestudier av reelle hendelser med trusler fra innsiden.	
Modeller og metoder for risikomåling og -evaluering	Kvantitative og kvalitative risikovurderingsmodeller og -metoder Sannsynligheten for hendelser og konsekvenser Konsekvensenes art og omfang Sensitivitet og konfidensnivåer. Praktiske eksempler og casestudier
Læringsutbytte: • Deltakerne skal sammenligne og anvende både kvantitative og kvalitative modeller i risikovurderinger av cybersikkerhet. • Deltakerne skal evaluere sannsynligheten for og potensielle utfall av identifiserte risikoer. • Deltakerne skal vurdere alvorlighetsgraden og omfanget av konsekvensene knyttet til cybersikkerhetsrisikoer. • Deltakerne skal fastslå nivåer av usikkerhet og sikkerhet i risikovurderinger. • Deltakerne vil implementere risikovurderingsmodeller i praktiske scenarier.	
Risikokontroll	Overvåking og gjennomgang Registrering og rapportering Praktiske eksempler og casestudier
Læringsutbytte • Deltakerne skal gjennomføre regelmessige prosesser for risikooovervåking og -gjennomgang. • Deltakerne skal dokumentere og rapportere risikokontrolltiltak på en effektiv måte. • Deltakerne vil undersøke eksempler fra virkeligheten for å forstå effektiv implementering av risikokontroll.	

Tabell9 -Modul: 8

Enheter	**Emner**
Håndtering av hendelser	Definisjon og betydning av hendelsesrespons Viktige komponenter i en effektiv beredskapsplan for hendelser Vanlige cybersikkerhetstrusler
Læringsutbytte • Deltakerne skal definere hendelseshåndtering og forklare dens betydning i cybersikkerhetsstyring. • Deltakerne skal identifisere og implementere nøkkelelementer i en strukturert beredskapsplan for hendelseshåndtering.	

• Deltakerne skal gjenkjenne og reagere på vanlige cybersikkerhetstrusler som oppstår under håndtering av hendelser.	
Gjenoppretting etter katastrofer	Forstå katastrofegjenoppretting Roller og ansvar i katastrofegjenoppretting Gjenopprettingstrinn etter katastrofe
Læringsutbytte • Deltakerne skal kunne forklare prinsippene og målene for katastrofegjenoppretting i sammenheng med cybersikkerhet. • Deltakerne skal beskrive rollene og ansvaret til teammedlemmene som er involvert i katastrofegjenoppretting. • Deltakerne skal utvikle en trinnvis plan for å gjenopprette systemer og drift etter en cyberkatastrofe.	
Forretningskontinuitet	Forståelse av forretningskontinuitet Roller og ansvar i forretningskontinuitet Analyse av forretningspåvirkning
Læringsutbytte: • Deltakerne skal kunne forklare konseptet og betydningen av planlegging av forretningskontinuitet. • Deltakerne vil identifisere roller og ansvar knyttet til å sikre forretningskontinuitet. • Deltakerne skal gjennomføre en analyse av forretningspåvirkning for å vurdere kritiske funksjoner og avhengigheter.	
Sikkerhetsbevissthet, opplæring og utdanning	Forståelse av sikkerhetsbevissthet Ansattes ansvar innen cybersikkerhet
Læringsutbytte • Deltakerne skal forklare sikkerhetsbevisstheten rolle i å redusere menneskelige cybersikkerhetsrisikoer. • Elevene vil lære om ansattes ansvar for å opprettholde protokoller og beste praksis for cybersikkerhet.	
Sikkerhetspraksis ved ansettelse	Definere krav til sikkerhetsroller Gjennomføring av bakgrunnssjekker
Læringsutbytte: • Deltakerne vil definere stillingsroller innen cybersikkerhet og formulere passende krav. • Deltakerne vil anvende beste praksis ved gjennomføring av bakgrunnssjekker for sikkerhetssensitive roller.	
Sikkerhetsopphørspraksis	Umiddelbar tilbakekalling av tilgang Varsle relevante team Juridiske og compliance-hensyn
Læringsutbytte • Deltakerne vil implementere prosedyrer for umiddelbar tilbakekalling av tilgang ved oppsigelse av ansatte. • Deltakerne vil koordinere kommunikasjonen med relevante avdelinger under avskjedsprosessen. • Deltakerne skal undersøke juridiske og compliance-krav knyttet til oppsigelse av ansettelsesforhold innen cybersikkerhet.	
Tredjepartssikkerhet	Vurdering av tredjepartsrisiko

	Implementering av kontraster og sikkerhetskrav Løpende overvåking og revisjon Håndtering av hendelser og kommunikasjon
Læringsutbytte: • Deltakerne vil vurdere sikkerhetsrisikoer knyttet til tredjepartsleverandører og partnere. • Deltakerne skal utforme og anvende kontraktsklausuler for å sikre at tredjeparter overholder sikkerhetskravene. • Deltakerne skal etablere kontinuerlige overvåkings- og revisjonsrutiner for tredjeparts sikkerhet. • Deltakerne skal koordinere med tredjeparter under hendelseshåndteringsaktiviteter.	
Sikkerhet i gjennomgangsprosesser	Inkorporering av sikkerhet i gjennomganger Sårbarhetsvurdering og penetrasjonstesting Gjennomgang etter hendelser
Læringsutbytte: • Deltakerne vil integrere sikkerhetshensyn i organisasjonens gjennomgangsprosesser. • Deltakerne vil gjennomføre sårbarhetsvurderinger og penetrasjonstester som en del av gjennomgangsaktivitetene. • Deltakerne vil gjennomføre evalueringer etter hendelser for å vurdere effektiviteten og forbedre fremtidige responser.	
Spesielle problemstillinger knyttet til personvern for ansattes personopplysninger	Begrensninger i datainnsamling Lagring og tilgangskontroll Overholdelse av personvernbestemmelser Datadeling og tredjeparter Ansattes samtykke og rettigheter
Læringsutbytte • Deltakerne vil identifisere passende grenser for innsamling av personopplysninger om ansatte. • Deltakerne vil anvende sikre lagrings- og tilgangskontrolltiltak for sensitive ansattdata. • Deltakerne skal sikre overholdelse av relevante personvernbestemmelser, for eksempel GDPR. • Deltakerne skal vurdere risikoer og regler knyttet til deling av ansattes data med tredjeparter. • Deltakerne skal forstå ansattes rettigheter og viktigheten av å innhente informert samtykke.	

KONKLUSJON

Denne rapporten presenterer læreplanen som er passende for yrkesutdanningsnivået som bør tas i betraktning for en vellykket gjennomføring av CyberAgent-opplæringen. Etter forskningen som er gjennomført siden prosjektets start for å identifisere opplæringsbehovene, beskriver dette dokumentet behovene til yrkesutdanningsstudenter for deres deltakelse.

Læreplanen utarbeidet for CyberAgent-prosjektet EQF nivå 5-6 ble brukt som referanse under utarbeidelsen av programmet. Fra denne læreplanen ble emner som passer for EQF nivå 4-5 valgt ut.

Til slutt, for å sikre at opplæringen er av høyeste kvalitet når det gjelder innhold, organisering og kompetanseutvikling, ble det stilt spørsmål knyttet til emner som ikke ble overført fra EQF nivå 5-6.

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau