CyberAgent

Co-funded by the European Union

SME CYBER SECURITY CHANGE AGENTS LÆRINGSVEISSTRUKTUR

CYBER-AGENT 06.2024

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

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Arbeidspakke 2: CyberAgent tilnærming og strukturdesign

Levering 2.3: SME Cyber Security Change Agents læringsveis struktur

Leder av WP2 – Olemisen Balanssia ry
Leder av leveranse 2.3 – Universitetet i Vilnius

INNHOLD

FORKORTELSER

CBL – Utfordringsbasert læringsmodell

CL – Kooperativ læringsmodell

EF – Europakommisjonen

ECTS - Europeisk kredittoverførings- og akkumuleringssystem

EQF – Det europeiske kvalifikasjonsrammeverket

GICL - Guidet forespørsel Collaborative Learning Model

HEI - Høyere utdanningsinstitusjoner

PBL – prosjektbasert læringsmodell

POGIL - Prosessorientert Guidet Inquiry Learning Model

SMB – små og mellomstore bedrifter

VET – yrkesfaglige utdanningsinstitusjoner

LISTE OVER FIGURER

LISTE OVER TABELLER

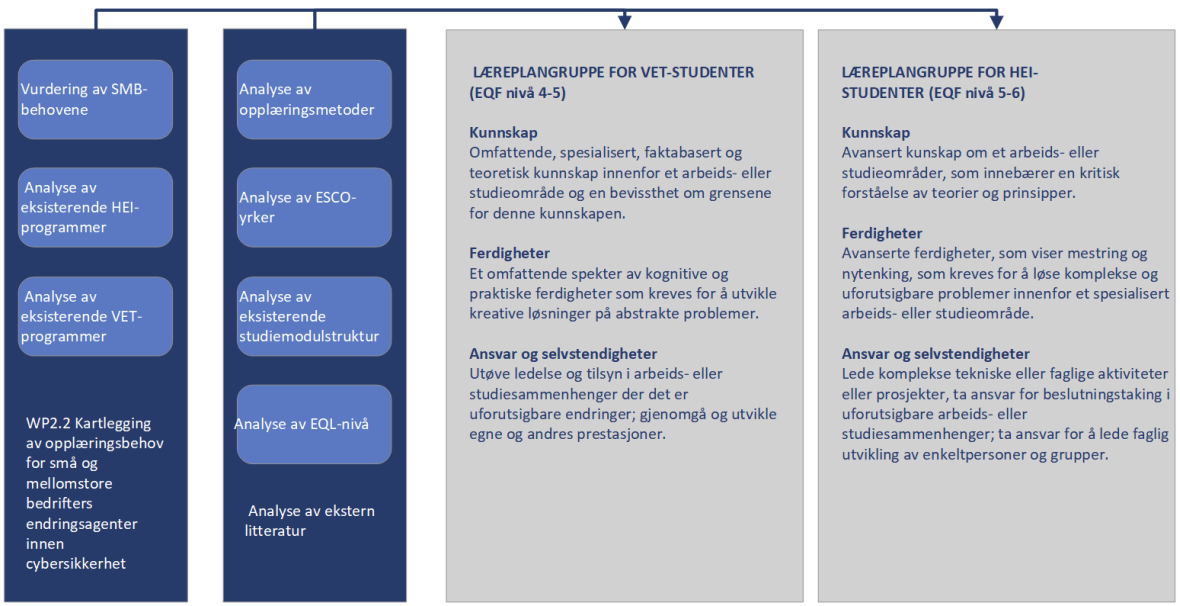
INTRODUKSJON

Det generelle målet med denne rapporten er å utvikle og beskrive nye profesjonelle læringsveier for kompetanseheving av cybersikkerhetsferdigheter blant europeiske SMB-ansatte (små og mellomstore bedrifter).

Basert på funnene fra kartleggingen av opplæringsbehovene for SMB Cyber Security Change Agents, ble ekstern ressursanalyse av læringsutbyttet i form av kunnskap, ferdigheter og kompetanse identifisert. Etter analysen av det identifiserte læringsutbyttet, gir denne rapporten veiledning om to typer opplæringsplaner fra EQF (European Qualifications Framework) nivå 4 til 6 for å dekke omfanget av ferdigheter og kunnskap som kreves for prosjektets målgrupper, SMB-ansatte og studenter, og tilpasse opplæringsresultatene til de ulike bakgrunnene og profilene til traineene.

- EQF nivå 4-5 vil bli implementert for SMB-ansatte som ikke har HEI-bakgrunn, samt yrkesopplæringsstudier. Dette nivået vil gi grunnleggende ferdigheter og kunnskaper innen cybersikkerhet med lett spesialisering i enkelte moduler.
- EQF nivå 5-6 som vil være et tilbud for SMB-ansatte som også har tilstrekkelig bakgrunn til å følge den og HEI (Higher Education Institutions) studenter. På dette nivået vil det bli gjennomført mer avanserte og komplekse opplæringsaktiviteter.

Det ble besluttet å oppdatere EQF-nivåene til 4-6, ikke bare for å dekke et bredt spekter av læringsutbytte som tidligere nevnt, men også for å muliggjøre en bro mellom opplæringens læreplaner som en videreopplæringsvei for studenter og ansatte på nivå 4 for å nå nivå 6.



Figur 1. Et illustrerende diagram, som følger EF-retningslinjene, viser de åtte EQF-nivåene, og gir en visuell fremstilling av utdanningsrammen.[1]

[1] https://europa.eu/europass/en/description-eight-eqf-levels

Læreplanen tar for seg læringsutbyttet og behovet for opplæring av SMB-ansatte for å kvalifisere seg for å fylle rollen som SME Cyber Security Change Agents og utdanne HEI- og VET-studenter til å fylle rollen etter studiet. Hver læreplan består av åtte moduler som dekker fire underemner:

- Tekniske ferdigheter - Oppdatert kunnskap om cybersikkerhetstrusler og relaterte juridiske problemstillinger - Praktisk kunnskap om hvordan man skal håndtere cybersikkerhetstrusler.
- Analytiske ferdigheter - Kritisk tenkning tankesett - Evne til å analysere og forstå lokale trusler, hvordan de skjer, mennesker i fare, etc.
- Risikostyring - Lær å gi og beskrive SMB-arbeidsplasser med cybersikkerhetsrutiner - Lag din egen arbeidsplass SMB-håndbok for cybersikkerhet og hvordan du følger den opp.
- Organisatoriske ferdigheter - Hvordan implementere nye rutiner og måter å jobbe med cybersikkerhet på SMB-arbeidsplasser; Gjennomføring av lederstøtte innen cybersikkerhet.

I tillegg er en sentral del av å skape læringsveier for kompetanseheving av cybersikkerhetsferdigheter blant europeiske små og mellomstore bedrifter hvordan microcredentials skal implementeres. De må referere til læringsutbytte (kunnskap, ferdigheter og kompetanse), kursinnhold, opplæring (kunnskap, ferdigheter og kompetanse), gamification-elementer, varighet og antall studiepoeng (European Credit Transfer and Accumulation System). For å passe formålet må de leveres gjennom etablering av partnerskap mellom HEI-ene med VET-leverandører og private bedrifter fra cybersikkerhetssektoren.

Mikroseksjoner gir elevene større frihet til å velge moduler eller deler av moduler og bestemme hvilket sertifikatnivå de trenger: deltakerbevis eller kursbevis med sertifiseringstest, dvs. bevis på at kurset er fullført med oppnåelse av en bestemt kompetanse. Kursbevis utstedes for å bestå den endelige testen med en poengsum på minst 75%, og sertifikater for deltakelse utstedes for å delta ansikt til ansikt, blandet læring eller online opplæring i bestemte emner / moduler. Denne praksisen øker ikke bare anvendeligheten og effektiviteten av opplæringen, men stimulerer også motivasjon for læring, og gir et klart verdiperspektiv for deltakernes karriere og videre utvikling.

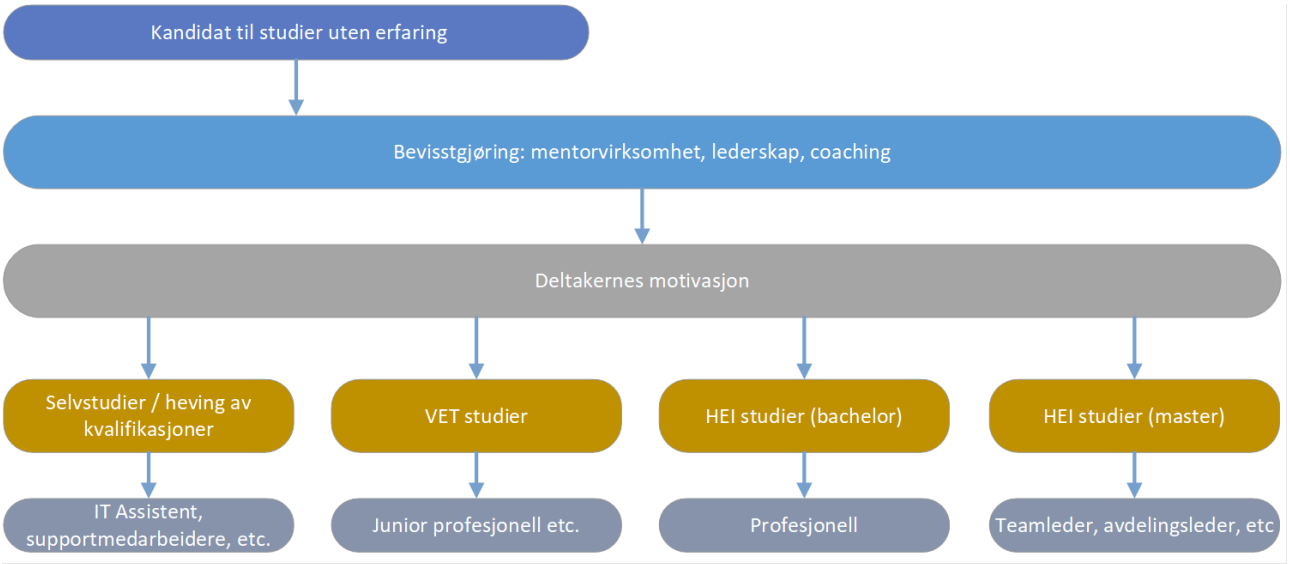
Samlet sett skisserer denne rapporten detaljerte veiledninger for utvikling av CyberAgent-moduler, inkludert innholdsoversikten over studie- og transportørveier, opplærings- og vurderingsmetoder og veikart for læreplanbygging.

1. STUDIEFORLØP

Et læringsforløp er en hel reise som deltakeren tar fra det øyeblikket de innser at de trenger å forbedre ferdigheter, starte og fullføre opplæring, til det øyeblikket de er ferdig med å lære og begynne å anvende mottatt kunnskap. Det er 3 trinn i en læringsvei:

- Før læring,
- Læring
- Etter læring.

Forlæringsfasen er illustrert i figuren nedenfor.



Figur 2. Læringsløp før studiestart

I sammenheng med små og mellomstore bedrifter kan denne lærings- / studieveien forfølges. I figuren bestemmer deltakeren seg enten for å trene seg selv eller blir påvirket av en holdningsskapende kampanje og får en forståelse av fordelene med treningen, mulighetene og karrierene som kan tilegnes etter treningen.

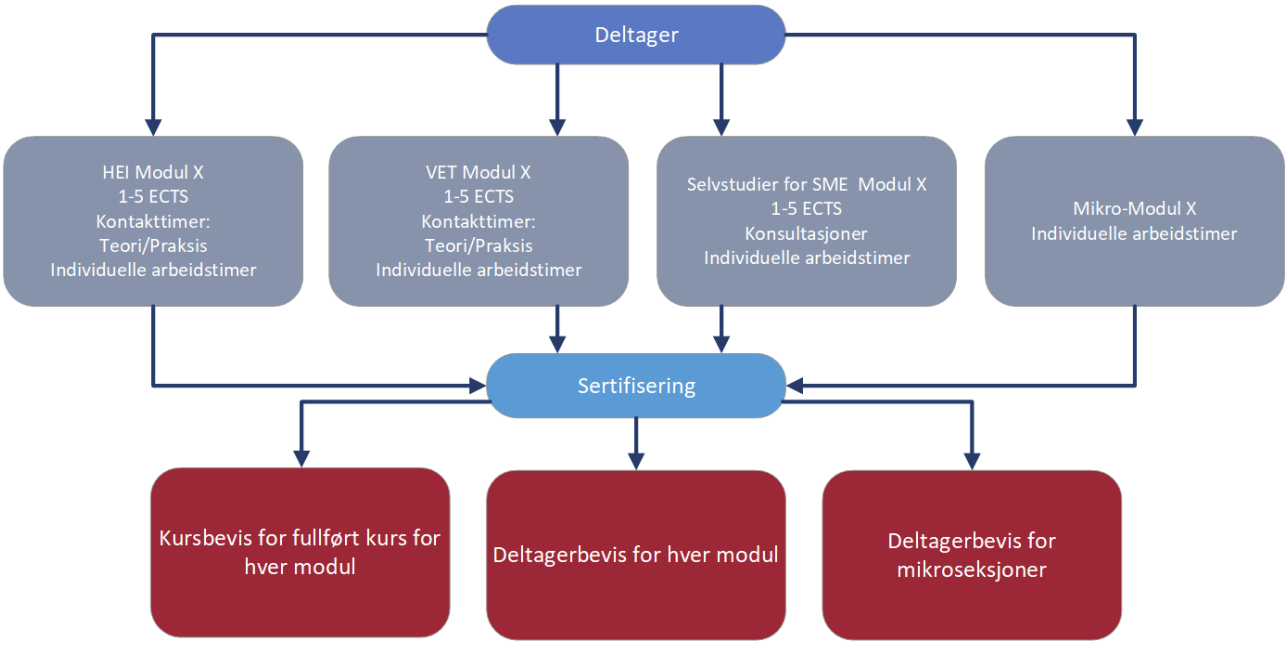
Det er også foreslått læringsforløp som typisk modul via OLE-struktur (Online Learning Environment). Etter en litteraturanalyse og flere prosjekter som anvender mikrocreditprinsippet[2],[3],[4] foreslås hver CyberAgent-modul å være 1-5 studiepoeng (hver studiepoeng er 25-30 timers arbeidsbelastning) og starter med en introduksjon og deles deretter inn i temaer, som er underemner.

[2] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Fremover og videre i utdanning: Begrepet fleksible læringsveier. I KTU leidykla "Technologija" ebøker. https://doi.org/10.5755/e01.9786090218204

[3] https://arqus-alliance.eu/call/arqus-microcredential-development-f2f-workshop/

[4] https://www.youtube.com/watch?v=ECH0VvHIyRI, https://ndma.lt/alta2023/

På slutten av emnene blir det gitt en egenvurderingstest bestående av flere spørsmål. Opplæringsmateriellet til modulen skal støtte studiet av 6-8 emner, i hver av dem er det 4-6 underemner. Emnet kan avsluttes med en kunnskapstest, som ikke er obligatorisk. Dette gir SMB-ansatte og studenter ved opplæringsinstitusjoner muligheten til å tilegne seg og demonstrere kompetansen som læres i en bestemt modul eller del av opplæringen.



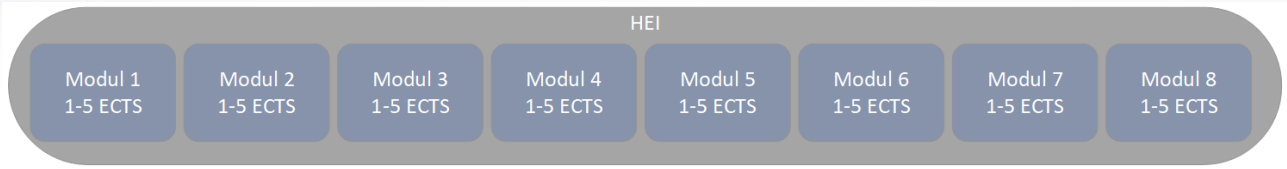
Figur 3. Studier struktur

Mikrocredits er integrert i læringsprosessen gjennom følgende nøkkelaktiviteter:

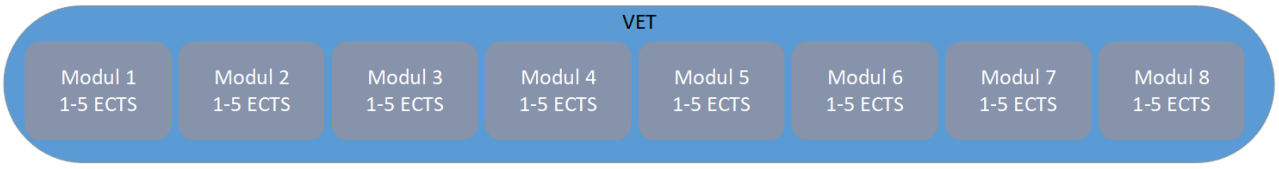
- Utvikling av opplæringsmoduler: Hver modul må være nøye formulert med hensyn til den spesifikke kunnskapen og ferdighetene som kreves i SMB-sektoren, med klare mål, læringsutbytte, undervisnings- og læringsmetoder, kursvarighet.
- Praktiske oppgaver og prosjekter: Elevene gjennomfører praktiske oppgaver og utvikler prosjekter som vurderes og gir tydelig bevis på ferdighetene som er oppnådd.
- Klart beskrevet kunnskapsvurderingsstrategi og evalueringskriterier: På slutten av hver modul organiseres en kunnskapsvurdering for å avgjøre om deltakeren har oppnådd de nødvendige læringsutbyttene og om de er kvalifisert for et sertifikat for å bevise det.

Siden målgruppen for prosjektet er SMB-ansatte, HEI- og VET-studenter, er fire typer studier tilgjengelige, i henhold til elevenes muligheter og behov:

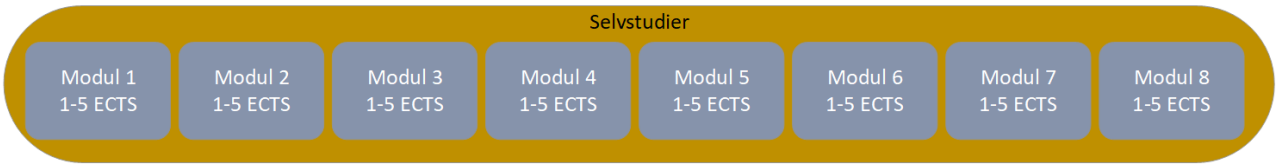
- HEI-studier: 8 moduler, hver 1-5 studiepoeng, hvor det er kontakttimer (teori og praksis) og individuell arbeidstid;
- VET-studier: 8 moduler, hver 1-5 studiepoeng, hvor det er kontakttimer (teori og praksis) og individuell arbeidstid;
- Selvstudier (for små og mellomstore bedrifter): 8 moduler, hver 1-5 studiepoeng, hvor det er konsultasjoner (om nødvendig) og individuell arbeidstid;
- Mikromoduler: individuell arbeidstid avhengig av antall valgte emner.



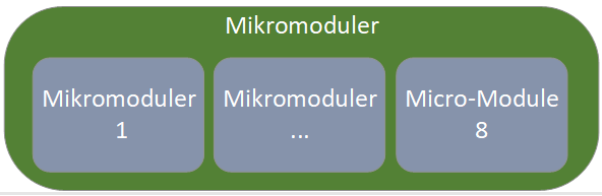
Figur 4. Studiestruktur for HEI



Figur 5. Studiestruktur for yrkesrettet utdanning

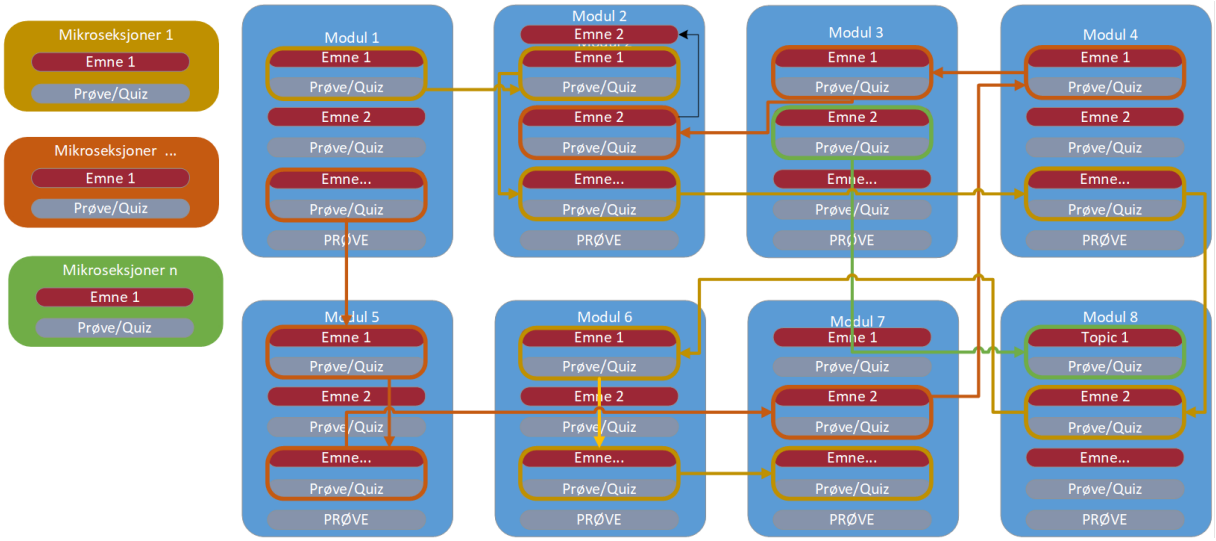


Figur 6. Studiestruktur for selvstudier



Figur 7. Studerer strukturen til mikromodulen

HEI- og VET-studenter vil kunne studere en modul på 1-5 studiepoeng hver. SMB vil kunne ta en modul om gangen, eller vi kan kanskje tilby mikroseksjoner som en del av kurset.



Figur 8. Sammenhenger mellom læringsstier

I alle tre (HEI, VET, SMB) læringstyper, studentstudier 8 moduler. I tilfelle mikromoduler velger studenten moduler etter eget valg. Esc

Mikromoduler er korte eller lange åpent vurderte læringsopplevelser. De tas av deltakeren sammen med utfordringen eller separat. Hver mikromodul er verdsatt med en annen mengde læringsbelastningsmål (for eksempel ECTS) og avsluttes med vurdering. Vellykket gjennomføring av mikromodulvurdering belønner elever med mikrocredits.

Forslaget er at hver modul fra HEI-programmet kan modulariseres i en mikromodul, hver med spesialiserte oppgaver og en detaljert plan for implementering. Testresultatene kan vurderes gjennom merker, som er bildebaserte og universelt lesbare av datamaskiner. Disse bildene bygger inn metadata som beskriver kompetansene knyttet til hvert merke og informasjon om deltakeren som har det.

Mikrocredits betyr registreringen av læringsutbyttet som en deltaker har oppnådd etter et lite læringsvolum. Dette læringsutbyttet vil være vurdert opp mot utvetydige og klart definerte kriterier. Læringsopplevelser som fører til mikrocredits er utformet for å gi deltakeren spesifikk kunnskap, ferdigheter og kompetanse som reagerer på samfunnsmessige, personlige, kulturelle eller arbeidsmarkedsbehov[5,6].

[5] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Fremover og videre i utdanning: Begrepet fleksible læringsveier. I KTU leidykla "Technologija" ebøker. https://doi.org/10.5755/e01.9786090218204

[6] Rådsrekommandasjon av 16. juni 2022 om en europeisk tilnærming til mikrocredits for livslang læring og ansettelsesevne.» Den europeiske unions tidende, vol. 2022/C, 16. juni 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022H0627(02)&from=EN

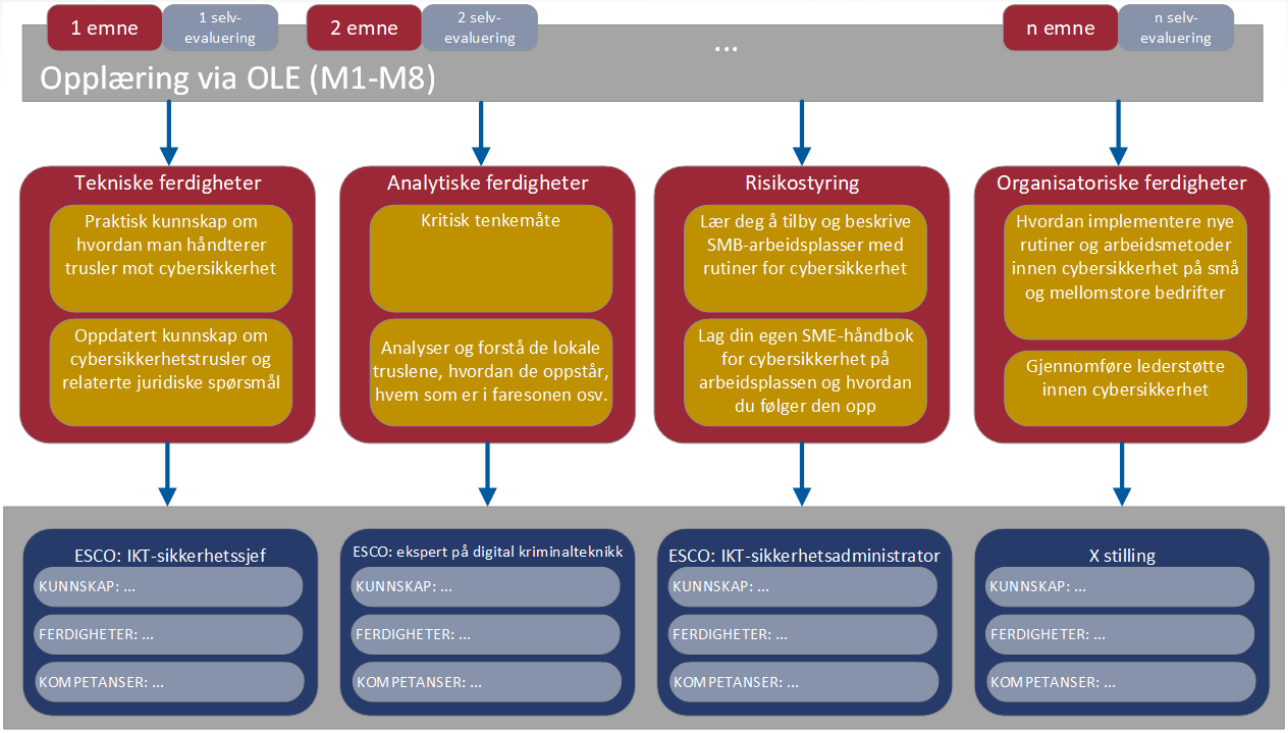
2. KARRIEREFORLØP

Aktiviteter etter læringsforøpet kan kalles karriere-forløpet. I begynnelsen av prosjektet ble forskningsanalysen av ESCO-yrker (beskrevet i rapporten: D2.2 - The SME Cyber Security Change Agents Training needs mapping report) gjort. Analysen som ble gjennomført i tre faser hadde som mål å undersøke ulike cybersikkerhetsyrker som er oppført innenfor ESCO-rammeverket. I den første fasen ble yrker relatert til cybersikkerhet identifisert og dokumentert fra **ESCO-portalen**, og fremhevet deres respektive ferdigheter, kompetanser og kunnskaper. Disse yrkene inkluderte roller som IKT-sikkerhetsansvarlig, digital etterforskningsekspert, embedded-systemsikkerhetsingeniør, etisk hacker, leder for motstandsdyktighet i IKT, IKT-sikkerhetsadministrator, IKT-sikkerhetsingeniør, IKT-sikkerhetsleder og kunnskapsingeniør. Hver yrkesgruppe ble definert av sine spesifikke ansvarsområder og fokusområder innen cybersikkerhet, alt fra bedriftssikkerhetsfunksjoner til digital etterforskning, etisk hacking og motstandsdyktighetsplanlegging.

I den andre fasen ble det fylt ut en tabell for hver gjennomgått ESCO-yrke, med detaljer om tittel og kjerneansvar. Disse inkluderte oppgaver som planlegging og implementering av sikkerhetstiltak, gjennomføring av sårbarhetsvurderinger, utvikling av modeller for motstandskraft og katastrofegjenoppretting, og integrering av kunnskap i datasystemer.

I tillegg involverte den tredje fasen kartlegging av ESCO-yrkene med tilhørende læringsutbytte, kategorisering av dem i kunnskap, ferdigheter og kompetanse. Denne prosessen la til rette for en omfattende forståelse av utdanningskravene og forventede ferdigheter for hver cybersikkerhetsrolle, og sikret tilpasning til bransjestandarder og beste praksis. Gjennom disse fasene ga analysen verdifull innsikt for den videre forskningen.

Figur 9. ESCO-yrker definert i forrige rapport



Figur 10. Mulige post-læringsveier

Figur 10 illustrerer mulige karriereveier som kan forfølges etter fullført studier via OLE (Online læringsmiljø) (HEI, VET, SME) og tilegnelse av ferdigheter, i tråd med ESCO-yrker.

Med en klarere forståelse av karrieremuligheter vil HEI- og VET-studenter som studerer cybersikkerhet få en klarere forståelse av karrieremuligheter og kunne velge et videre fagområde eller jobbe i selskaper i bestemte stillinger, mens IT og andre studenter vil kunne velge CyberAgent-moduler som individuelle studiemoduler, og dermed forbedre deres fagkompetanse, som organisatoriske og risikostyringsevner etc.

Ansatte i små og mellomstore bedrifter vil få mulighet til å heve kompetansen og utvikle kompetansen på arbeidsplassen. Basert på karriereveien som er utviklet og med klare karrieremuligheter, vil andre SMB-ansatte kunne omskolere seg innen cybersikkerhet.

Økt involvering av både studenter og SMB-ansatte er planlagt gjennom integrering av mentorordninger, organisering av formidlingsarrangementer, workshops (prosjektet inkluderer 6 felles workshops organisert av alle partnere, samt formidlingskampanjer organisert av hver partner), invitere forretnings- og cybersikkerhetsrepresentanter, samarbeid med sosiale partnere og CyberAgent-nettverket, som tilbyr praksisplasser til studenter, etc. Videre har våre mangfoldsinitiativer, inkludert målrettede oppsøkende og støtteprogrammer, som mål å styrke kvinners deltakelse og fremme en inkluderende arbeidsstyrke innen cybersikkerhet.

Ved å samkjøre ESCO-yrker til våre CyberAgent-treningsmoduler, kan deltakerne sømløst gå fra læringsmiljøer til innflytelsesrike roller innen cybersikkerhet. For å følge karriereutviklingen til CyberAgent-traineer, er det planlagt å organisere undersøkelser før opplæring, etter opplæring og 3 måneder etter trening for å finne ut hvordan ferdighetene deres bidrar til cybersikkerheten

til organisasjonene de jobber i. Undersøkelsene vil bli integrert i opplæringsplattformen og vil bli tilbudt automatisk til traineene før kursstart, på slutten av kurset for å måle fremgang og evaluere kurset og kvaliteten på opplæringen. En tredje undersøkelse vil bli brukt til å finne ut om det har skjedd noen endringer i deltakernes karriere.

3. UNDERVISNINGS- OG LÆRINGSFORMER

Analysen av de pedagogiske metodene til informasjonssystemene og Cyber Security studiet av Vilnius University (VU), Timtal og Moisil Buzau studieprogrammer og ekstern litteratur gjør oss i stand til å anbefale flere innovative kombinasjoner av undervisningsmetoder. Disse kombinasjonene kan inkluderes i studiemodulene, med tanke på strukturen til hver modul.[7]

Tabell 1. Anbefalte undervisningsmetoder

Kategori	Detaljert informasjon
Forelesing og direkte instruksjon	- **Teoretiske forelesinger:** Grunnleggende konsepter og teorier. - **Gjesteforelesere** ((sertifiserte spesialister med: Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), CompTIA Security+, Certified Ethical Hacker (CEH), GIAC Security Essentials Certification (GSEC), Systems Security Certified Practitioner (SSCP), CompTIA Advanced Security Practitioner (CASP+), GIAC Certified Incident Handler (GCIH), Offensive Security Certified Professional (OSCP))).

Praktisk og hands-on læring	- **Praktiske oppgaver/Labber:** hands-on eksperimenter og praktiske øvelser.
	- **Hands-On Aktiviteter**: Praktiske anvendelser og interaktive oppgaver.
	- **Teknisk videoanalyse:** Analyse av videoinnhold for læring av tekniske ferdigheter.
	- **Simulated Environments**:
	  o Vertsbaserte maskiner for skymiljø.
	  o Start angrep på en målmaskin.
	  o Maskin for planlegging og gjennomføring av angrep – en angrepsboks.

Vurdering og evaluering	- **Spørrekonkurranser, spill, gjør og ikke gjør** – engasjerende og interaktive vurderinger.

[7] Undervisning i cybersikkerhet: En prosjektbasert læring og veiledet forespørsel samarbeidslæringstilnærming https://scholar.utc.edu/cgi/viewcontent.cgi?article=1945&context=theses

Kategori	Detaljert informasjon
	- **Selvvurderingstester**: For elevens egenevaluering på slutten av emner.
Selvstudier	- **Selvstyrt læring:** Denne metoden støtter personlige læringsbaner og kan forbedres med digitale ressurser og modulært innhold som studentene kan få tilgang til etter behov.
Samarbeid og fagfellelæring	- **Samarbeidslæring, teamarbeid**: gruppeprosjekter og samarbeidsoppgaver. - **Peer-to-Peer undervisning og læring**: elevene lærer og lærer av hverandre. - **Gruppeveiledning og/eller individuell veiledning**: veiledning gitt av mer erfarne personer.
Teknologiforbedret læring	- **Bruk av spillifisert læringsplattform for cybersikkerhet**: engasjerende elever gjennom spilllignende elementer i læringsplattformer. - **Fang flaggkonkurransene**: konkurransedyktige arrangementer for å forbedre cybersikkerhetsferdighetene. - **Konkurranser**: konkurranser tester studentenes ferdigheter og kunnskaper i en praktisk, anvendt setting og gir et mål på deres kompetanse i et konkurransedyktig format.
Fellesskap og offentlig engasjement	- **Utdanningsarrangementer:** spesielle arrangementer under initiativer som Cybersecurity Month. - **Offentlige presentasjoner**: seminarer, konferanser og webinarer. - **Sosiale nettverk**: Bruk av sosiale medier og nettverk for læring og engasjement. - **Day Campus**: innebærer vanligvis engasjerende, campusbaserte arrangementer som kan inkludere workshops, forelesninger og nettverksmuligheter

Kategori	Detaljert informasjon
Innovative læringsmodeller	- **BSCS 5E Instructional Model (5Es)** - 5Es fokuserer på følgende faser som består av: Engasjement, utforskning, forklaring, utarbeidelse, evaluering. (Engagement, Exploration, Explanation, Elaboration, Evaluation) - **Utfordringsbasert læringsmodell (CBL) -** en tidlig implementering av CBL gir et rammeverk som består av seks faser: Beskriv utfordringen, Generering og brainstorming av ideer, gjennomgå flere perspektiver som stiller spørsmål og støtter, Forskning og revidere for beste løsninger, Test hypotese, Del funnene og konklusjonene. - **Samarbeidsbasert Læringsmodell (CL) -** I likhet med 5Es- og CBL-modellene, fremmer samarbeidsbasert læring aktiv læring i små grupper, og studentene mottar en belønning basert på deres prestasjoner som kan inkludere en karakter, en konkret belønning som et sertifikat eller stipend, eller godkjenning fra en lærer. - **Prosjektbasert læringsmodell (PBL) -** prosjektbasert læring og problembasert læring bruker samme forkortelse for PBL og er begge fokusert på å forbedre problemløsing, kritisk tenkning, samarbeid, kommunikasjon og kreative ferdigheter; men de består av ulike faser., Uavhengig og gruppeforskning, Utvikle og presentere, Analyser og evaluer prosess. - **Process Oriented Guided Inquiry Learning Model (POGIL) -** denne tilnærmingen guider elevene gjennom utforskningen av et konsept; etterfulgt av konseptoppfinnelse der elevene syntetiserer og forklarer konseptet; og lukker læringssyklusen med anvendelse av det teoretiske konseptet. - **Guided Inquiry Collaborative Learning Model (GICL) –** dette er en ny tilnærming som i stor grad er basert på POGIL-modellen.

For å sikre at de ulike opplæringsstrategiene som tilbys har best mulig effekt, vil hver tilnærming bli valgt og justert med de spesifikke læringsmålene for cybersecurity-modulene i utviklingen av et omfattende modulpensum og opplæringsmateriell. Ytterligere metoder kan også velges av foreleserne / mentorene som skal levere CyberAgent-opplæringen. I utviklingsfasen av opplæringsmateriellet vil opplæring bli gitt til instruktørene av pilotopplæringene for å informere dem om målene, prosessen og ansvarene i opplæringen, og for å forberede dem til effektivt å undervise i CyberAgent-læreplanen. Pilotopplæringsprosessen omfatter også innsamling av tilbakemeldinger fra elever og instruktører for å overvåke effektiviteten av opplæringsmetodene som brukes, og for å foreta justeringer der det er nødvendig.

Modulene vil bli holdt i ulike undervisningsformater:

- i **fjernlæringsformat**,
- i **synkron læring** (full støtte fra læreren),
- og i **asynkron læring** (støtte av lærer når det trengs), blandet læring og selvlæring.

Ettersom det er tenkt forskjellige måter å gjennomføre opplæringen på, presenteres treningsmetodene på dette stadiet som retningslinjer.

4. MODUL STRUKTUR

Analysen av modulstrukturen til VU Cyber Security studieprogrammet, analysen av modulstrukturen til internasjonale prosjekter (**CyberPhish**, **FuseIT**, **dComFra**), og analysen av modulstrukturen til kommersielle plattformer, som f.eks. **Udemy** og **Coursera**, har ført til etableringen av en typisk modulstruktur som kan brukes på både HEI- og VET-moduler.

Hovedmålet er å utvikle 8 moduler, hvor 8 moduler vil være for HEI-studenter (EQF nivå 5-6-), for VET-studenter og små og mellomstore bedrifter (EQF nivå 4-5) og mikromoduler for alle typer studenter.

Figur 11. Modul Struktur

* Det anbefales at hvert undertema etterfølges av selvtestspørsmål (selvrefleksjon). Men på modulutviklingsstadiet kan en annen vurderingsmetode eller alternativ velges avhengig av hvilken type studie som er valgt, for eksempel kan studentene få praktiske øvelser, simuleringer, etc., mens selvtestspørsmål tilbys til uavhengige elever.

** En kunnskapsvurderingstest er valgfri. Hvis eleven ønsker å få et kursbevis for å verifisere kunnskapen som er oppnådd, er denne testen obligatorisk. Eleven har imidlertid muligheten til

å skaffe seg et kursbevis for å bevise at han / hun har deltatt i opplæringen, i så fall er denne testen valgfri.

For å sikre at hver opplæringsmodul er direkte knyttet til praktisk anvendelighet, vil beskrivelsen av hver modul gi klare eksempler på hvordan teorien anvendes i praksis. Dette inkluderer ikke bare detaljerte scenarier for anvendelsen av modulene, men også spesifikke oppgaver som studentene skal gjennomføre for å konsolidere den teoretiske kunnskapen i virkelige cybersikkerhetssituasjoner.

Hver modul skal gi tekniske ferdigheter, analytiske ferdigheter, risikostyringsferdigheter, organisatoriske ferdigheter med ulike proporsjoner. Selvvurderingstesten er gitt for å teste elevenes kunnskap på slutten av hvilken som helst del av modulen (emnet). Dette tillater ikke bare vurdering eller evaluering av kunnskapen som er oppnådd, men også elevens fremgang registreres og deltakeren samler poeng og merker, noe som gjør at deltakeren kan være mer involvert i læringsprosessen.

Etter ECTS formaliteter hvor hvert studiepoeng er 25-30 timers arbeidsmengde. I henhold til dette kan hver modul være lik 5 studiepoeng. Arbeidsmengden kan fordeles slik:

Tabell 2. Timer med arbeidsmengde

	Antall moduler	Totalt antall studiepoeng	Timer fjernlæring for teoretiske ferdigheter	Timer fjernlæring for praktiske ferdigheter	Individuell arbeidstid	Arbeidsmengde totalt
Moduler for HEI-studenter (EQF nivå 5-6)	8	8-40	20%	20%	60%	200-1200
Moduler for VET-studenter (EQF nivå 4-5)	8	8-40	15%	25%	60%	200-1200
Selvstudier (blended learning)	8	8-40	10%		90%	2000-1080
Selvstudier (nettbasert)	8	8-40				200-1200
Mikromoduler	1-8	1-40				25-1200

Tabell 3. Arbeidsmengde for anbefalte moduler

Modul	ECTS	Totalt antall timer	Kontakt timer	Kontakt timer (teori)	Kontakt timer (praksis)	Individuell arbeidstid
HEI Modul tittel	1-5	25-150	40%	20%	20%	60%
VET Modul tittel	1-5	25-150	40%	15%	25%	60%
Selvstudier (blended learning)	1-5	25-150	10%			90%
Selvstudier (nettbasert)	1-5	25-150				100%
Mikro-seksjoner						10%-100%

Hver modul skal ha sin egen beskrivelse. Etter analyse av VU, Timtal og andre programmer som buker mikrocredits, foreslås en typisk modulstruktur for hver CyberAgent-modul (et eksempel på en typisk modulstruktur er gitt i vedlegg 1).

Tabell 4. Typisk struktur for CyberAgent moduler

Kategori	Detaljert informasjon
Modulidentifikasjon (grunnleggende informasjon om modulen)	- Modulens tittel - Modul kode - Foreleser - Institusjon eller avdeling der modulen leveres - Modell for levering - Språk - Forutsetninger
Modulens varighet og arbeidsmengde (tydelig tidsforpliktelse og strukturoppbygning)	- Total varighet (antall studiepoeng) - Studentens arbeidsmengde i timer - Kontakt arbeidstid - Individuell arbeidstid

Læringsmål og læringsutbytte (detaljer om hva modulen tar sikte på å oppnå og hva studentene skal lære)	- Formål og resultater av modulen
	- Læringsutbytte
	  o Tekniske ferdgheter
	  o Analytiske ferdigheter
	  o Risiko ferdigheter
	  o Organisatoriske ferdigheter

Undervisnings- og læringsmetoder	- Undervisning- og læringsmetoder
Vurdering og evaluering (forklaring på hvordan studentene skal vurderes)	- Vurderingsformer - Oppgaver (laboratorier, prosjekter, presentasjoner, rapporter, etc.) - Vurderingsstrategi, vurderingskriterier
Tilrettelegge for ressurser	- Utstyr, programvare og teknologi
Kursets innhold	- Modulemner og underemner
Ressurser	- Liste over kilder - Flere kilder

Hver ECTS regnes som 25-30 timer (kontakt eller online timer + individuell studie).

Modulen må ha minst et hierarki med to nivåer:

- **Det første nivået i hierarkiet** – emner. På dette nivået kan hovedelementene i modulen være introduksjon, inngangstest, sluttprøve og basiselementet - emne.
- **Det andre nivået i hierarkiet** – under-emne, de viktigste pedagogiske elementene i modulen.

Hver modul på første nivå i hierarkiet skal inneholde:

- **INTRODUKSJON** til modulen (tekstbeskrivelse, videointroduksjon): relevans og fordeler med modul, grunnleggende mål og resultater av modulen, nødvendig programvare og maskinvare, krav til deltakerne.
- **EMNER** – hovedtema i emnet, teoretisk materiale og teoretiske undervisningsmetoder.
- **UNDEREMNE** – underemne for hvert tema, praktisk, analytisk analyse og oppgaver, praktiske og analytiske undervisningsmetoder. Emner og underemner kan omfatte tekstinformasjon, videoer, lydklipp, presentasjoner, lenker til videre lesing.
- **MODUL Introtest** (om nødvendig). Introtesten på mellomliggende og avansert nivå skal bekrefte at søkeren har mestret nok kunnskaper og ferdigheter på tidligere nivåer.
- **MODUL anerkjennelsestester**. Bekreftelsestest skal gi objektiv verifisering av studentens ferdigheter og demonstrere deres kompetanse til modulkravene.
- **RETNINGSLINJER for mentorer/lærere**. Dette dokumentet skal inneholde metodiske anbefalinger for mentorer / lærere om bruk av modulpedagogiske elementer.

Hvert emne på andre nivå i hierarkiet bør inneholde:

- **INTRODUKSJON** til temaet mål og resultater, kort innhold.
- **UNDEREMNE:** alle nødvendige pedagogiske elementer for å støtte studenten til å mestre relevante ferdigheter.
- **EMNE-testen**: Korte anbefalinger til mentorer/lærere om modulimplementering og anvendelse. Hvert UNDEREMNE skal bestå av pedagogiske elementer, hvis innhold tilsvarer oppgavene til modulbeskrivelsen. Hvert underemne kan (bør) inneholde en underemne som bekrefter at studenten behersker relevante ferdigheter på et høyt nok nivå.

Opplæringsmateriellet til modulen skal støtte studiet av 6-8 emner, i hver av dem er det 4-6 underemner og som minimum en emneprøve. Så modulen skal inneholde (omtrentlig) 30-40 pedagogiske elementer (metoder beskrevet i seksjonsundervisningsmetoder) og 6-8 tester og en modul endelig bekreftelsestest.

5. CYBERAGENT LÆREPLAN OG OPPLÆRINGSPROGRAM

Veikart for bygging av læreplaner

CyberAgent Curriculum og et opplæringsprogram følger læreplanretningslinjer for post-sekundære gradsprogrammer i cybersikkerhet, utviklet av den felles arbeidsgruppen til ACM, IEEE, AIS SIGSEC og IFIP (2017)[8] (heretter - **Retningslinjer**). Mer spesifikt, siden det generelle fokuset på CyberAgent-prosjektet er å øke interne cybersikkerhetskompetanser hos europeiske små og mellomstore bedrifter, følger læreplanen rammeverket for organisatorisk sikkerhetskunnskapsområde, som anbefalinger fra disse retningslinjene.

Når det er sagt, er det første trinnet i læreplanbygging å kartlegge forhåndsdefinerte underemner og moduler i CyberAgent-prosjektet med kunnskapsenhetene og sentrale emner, anbefalt og beskrevet av retningslinjene (s. 59-70). Kartleggingen er basert på den logiske sammenhengen mellom disse to pilarene, som diskutert og avtalt av prosjektpartnerne.

Det andre trinnet er å tildele spesifikke læringsutbytter, identifisert og beskrevet fra T2.2 "Mapping the training needs for SME Cyber Security Change Agents" med kunnskapsenheten og sentrale emner, kartlagt ovenfor. Det skal her bemerkes at ulike yrker knyttet til cybersikkerhet kan ha en rekke forskjellige kunnskaper, ferdigheter og kompetanser, som velformulert i ovennevnte T2.2-leveranse. Forslaget nedenfor gjenspeiler imidlertid CyberAgents forventede sett med kunnskaper, ferdigheter og kompetanser, som kan tilpasses de spesifikke behovene til spesifikke yrker eller traineegrupper.

Når det er sagt, er resultatene av denne læreplanbyggingsøvelsen gitt i tabell 5 nedenfor.

[8] Joint Task Force on Cybersecurity Education. (2017). Læreplanretningslinjer for post-videregående studieprogrammer i cybersikkerhet: En rapport i Computing Curricula Series. Association for Computing Machinery, 31. desember 2017. Tilgjengelig på: **https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf** [Besøkt 3. mars 2024]

Tabell 5. plan for utvikling av læreplan

Underemner og moduler	Kunnskapsenhet og sentrale temaer	Læringsutbytte HEI	Læringsutbytte VET
Tekniske ferdigheter			
- **Oppdatert kunnskap om cybersikkerhetstrusler og relaterte juridiske problemstillinger**	**Administrasjon av sikkerhetsprogram** - Prosjektledelse - Ressursforvaltning - Sikkerhetsmålinger - Kvalitetssikring og kvalitetskontroll	**Kunnskap**: Elevene vil få forhåndskunnskap om avanserte cybersikkerhetsprinsipper, inkludert sofistikerte cybertrusler og angrepsvektorer, nasjonal og internasjonal lovgivning om cybersikkerhet, standarder og samsvarskrav som er relevante for deres bransje. **Ferdigheter**: Elevene vil være dyktige til å designe og implementere avanserte risikovurderings- og styringsstrategier for å redusere identifiserte risikoer, ved hjelp av avanserte metoder og verktøy. **Kompetanse**: Elevene vil være kompetente til å lede og administrere cybersikkerhetsprosjekter og team som implementerer strategiske retningslinjer og rammer for cybersikkerhet i tråd med organisasjonens mål og overholdelsesforpliktelser.	**Kunnskap**: Elevene vil få praktisk kunnskap om de nyeste cybersikkerhetstruslene, inkludert phishing, ransomware og DDoS-angrep, og hvordan man håndterer disse gjennom effektiv prosjekt- og ressursstyring, og implementering av kvalitetssikrings- og kontrolltiltak. **Ferdigheter**: Elevene vil være dyktige til å bruke verktøy og programvare for beskyttelse mot utviklende cybertrusler, og anvende robuste sikkerhetspraksis i prosjekt- og ressursstyring for å forbedre de generelle sikkerhetsmålingene og kvalitetskontrollen i organisasjonene. **Kompetanse: Elevene** vil være kompetente til å vurdere og redusere potensielle sikkerhetstrusler, effektivt kommunisere cybersikkerhetsproblemer og nøyaktig rapportere trusler og brudd gjennom de aktuelle kanalene i organisasjonen.

- **Praktisk kunnskap for hvordan man skal håndtere cybersikkerhetstrusler**	**Systemadministrasjon** - Administrasjon av operativsystem - Administrasjon av databasesystem - Administrasjon av nettverk - Administrasjon i skyen - Cyber-fysisk systemadministrasjon - Forsterket system - Tilgjengelighet	**Kunnskap**: Elevene vil få avansert kunnskap innen drift, database, nettverk, sky og cyber-fysisk systemadministrasjon og andre områder, slik at de effektivt kan herde systemer og sikre tilgjengelighet mens de bruker de nyeste forsvarsmekanismene for cybersikkerhet. **Ferdigheter**: Elevene vil være dyktige til å bruke avanserte metoder og verktøy for å designe og implementere sikre systemarkitekturer - inkludert operativsystemer, databaser, nettverk og skyinfrastrukturer **Kompetanse: Elevene** vil være kompetente til å utvikle og implementere strategiske cybersikkerhetsrammer for systemadministrasjon, lede prosjekter og team for å forbedre systemherding og tilgjengelighet, og ta etiske beslutninger for å opprettholde robust cybersikkerhetspraksis på tvers av ulike administrative domener.	**Kunnskap**: Elevene vil få praktisk kunnskap om hvordan man administrerer og sikrer operativsystemer, databaser, nettverk, skyer og cyber-fysiske systemer mot vanlige cybertrusler som phishing, ransomware og DDoS-angrep, samtidig som effektive risikostyringspolicyer implementeres. **Ferdigheter**: Elevene vil være dyktige til å identifisere potensielle cybersikkerhetsrisikoer og sårbarheter på tvers av ulike systemplattformer, ved hjelp av spesialiserte verktøy og programvare for å forbedre systemherding og tilgjengelighet, og implementere grunnleggende cybersikkerhetspraksis som sikker passordoppretting, sikker surfing og sikker håndtering av sensitive data. **Kompetanse: Elevene** vil være kompetente til å vurdere og redusere sikkerhetstrusler innen systemadministrasjon, effektivt kommunisere cybersikkerhetsproblemer og raskt rapportere eventuelle trusler og brudd til de aktuelle organisatoriske kanaler.

Analystiske ferdigheter			
- **Kritisk tenkning tankesett**	**Analytiske verktøy** - Ytelsesmålinger (måleparametere) - Analyse av data - Sikkerhetsetterretning	**Kunnskap**: Elevene vil få forhåndskunnskap om nasjonal og internasjonal lovgivning, standarder og krav til overholdelse av cybersikkerhet, og andre som er relevante for deres spesifikke bransje. **Ferdigheter**: Elevene vil være dyktige til å bruke ytelsesmålinger, dataanalyse og sikkerhetsetterretning for å designe og implementere effektive risikostyringsstrategier. **Kompetanse**: Elevene vil være kompetente til å bruke analytiske verktøy for å utvikle strategiske retningslinjer for cybersikkerhet med ett kritisk tenkning tankesett, og ta beslutninger i cybersikkerhetspraksis i tråd med organisatoriske mål og overholdelsesforpliktelser.	**Kunnskap**: Elevene vil få praktisk kunnskap om hvordan man bruker ytelsesmålinger, dataanalyse og sikkerhetsetterretning for å beskytte organisatoriske eiendeler. **Ferdigheter**: Elevene vil være dyktige i å bruke analytiske verktøy for å identifisere potensielle cybersikkerhetsrisikoer og sårbarheter, anvende datadrevet innsikt for å styrke cybersikkerhetspraksis og utnytte ytelsesmålinger for å evaluere og forbedre sikkerheten til passord, surfing, e-post og datahåndtering. **Kompetanse**: Elevene vil være kompetente til å vurdere og redusere potensielle sikkerhetstrusler ved hjelp av analytiske verktøy, nøyaktig rapportere trusler og brudd til de aktuelle kanalene i organisasjonen.
- **Analysere og forstå de lokale truslene, hvordan de oppstår, mennesker i risiko etc.**	**Sikkerhetsoperasjoner** - Sikkerhetskonvergens	**Kunnskap**: Elevene vil få forhåndskunnskap i lokale cybertrusler, ved hjelp av innsikt fra globale sikkerhetsoperasjonssentre og	**Kunnskap**: Elevene vil få praktisk kunnskap om lokale cybertrusler og deres opprinnelse, vurdere hvordan disse truslene påvirker organisatoriske eiendeler.

	- Globale sikkerhetsoperasjonssentre (GSOC)	nåværende trender innen forsvarsstrategier for cybersikkerhet. **Ferdigheter**: Elevene vil være dyktige til å utnytte avanserte metoder og verktøy innen globale sikkerhetsoperasjonssentre for å utforme effektive risikostyringsstrategier, og utvikle planer for å redusere lokale cybersikkerhetstrusler effektivt. **Kompetanse**: Elevene vil være kompetente i å utvikle og implementere strategiske retningslinjer for cybersikkerhet som adresserer lokale trusler gjennom bruk av globale sikkerhetsoperasjonssentre.	**Ferdigheter**: Elevene vil være dyktige til å identifisere lokale cybersikkerhetsrisikoer og sårbarheter, ved hjelp av verktøy og programvare som sikker passordoppretting, sikker surfing og sikker datahåndtering skreddersydd for deres spesifikke miljøer. **Kompetanse:** Elevene vil være kompetente til å vurdere og redusere lokale sikkerhetstrusler ved hjelp av innsikt fra globale sikkerhetsoperasjonssentre, effektivt kommunisere cybersikkerhetsproblemer og nøyaktig rapportere trusler og brudd til de aktuelle kanalene i organisasjonen.
Risikostyring			
- **Lær å tilby og beskrive cybersikkerhetsrutiner til SMB-arbeidsplassen**	**Risikostyring** - Risk identification - Risk assessment and analysis - Insider threats - Risk measurement and evaluation models and methodologies - Risk control	**Kunnskap**: Elevene vil få avansert kunnskap om risikostyringsprosesser, inkludert risikoidentifikasjon, vurdering og kontroll, slik at de kan etablere og beskrive effektive cybersikkerhetsrutiner skreddersydd for de spesifikke behovene til SMB-arbeidsplasser i samsvar med nasjonale og internasjonale standarder. **Ferdigheter**: Elevene vil være dyktige til å anvende avanserte metoder og	**Kunnskap**: Elevene vil få praktisk kunnskap i prosessene for risikoidentifikasjon, vurdering og kontroll, og risikostyringsstrategier for å beskytte SMB-arbeidsplasser effektivt. **Ferdigheter**: Elevene vil være dyktige i å identifisere og analysere potensielle cybersikkerhetsrisikoer i SMB-miljøer, bruke passende verktøy og programvare for trusselreduksjon, og fremme og implementere viktige

		verktøy for å gjennomføre omfattende risikovurderinger, designe og implementere effektive risikostyringsstrategier, og utvikle robuste cybersikkerhetsrutiner spesielt skreddersydd for SMB-arbeidsplasser. **Kompetanse**: Elevene vil være kompetente i å utvikle og implementere strategiske retningslinjer for cybersikkerhet for SMB-arbeidsplasser.	cybersikkerhetspraksis, inkludert sikker passordoppretting, sikker surfing og sikker håndtering av sensitive data. **Kompetanse:** Elevene vil ha kompetanse til å vurdere og redusere sikkerhetstrusler på SMB-arbeidsplasser, effektivt kommunisere cybersikkerhetsproblemer og prosedyrer, og nøyaktig rapportere relevante trusler og brudd til passende organisatoriske kanaler.
- **Lag egen SMB-håndbok for cybersikkerhet og hvordan du kan følge den opp**	**Forretningskontinuitet, nødgjenoppretting og hendelseshåndtering og personalsikkerhet** - Respons på hendelser - Disaster recovery - Kontinuitet i virksomheten - Sikkerhetsbevissthet, opplæring og utdanning - Praksis for sikkerhetsansettelser - Praksis for oppsigelse av sikkerhet - Tredjeparts sikkerhet - Sikkerhet i vurderingsprosesser	**Kunnskap**: Elevene vil få forhåndskunnskap om hvordan man oppretter og implementerer en omfattende SMB-cybersikkerhetshåndbok på arbeidsplassen, som inneholder avanserte cybersikkerhetsprinsipper, de nyeste forsvarsmekanismene og overholdelse av nasjonal og internasjonal lovgivning og standarder innen hendelseshåndtering, forretningskontinuitet og personellsikkerhet. **Ferdigheter**: Elevene vil være dyktige til å lage og vedlikeholde en SMB-håndbok for cybersikkerhet på arbeidsplassen, ved hjelp av avanserte metoder for å vurdere risiko, utforme	**Kunnskap**: Elevene vil få praktisk kunnskap om hvordan man lager en omfattende SMB-håndbok for cybersikkerhet på arbeidsplassen som inkorporerer strategier for hendelsesrespons, katastrofegjenoppretting, forretningskontinuitet og personellsikkerhet, og beskytter organisatoriske eiendeler og sensitive data. **Ferdigheter**: Elevene vil være dyktige til å identifisere potensielle cybersikkerhetsrisikoer, bruke verktøy og programvare for å beskytte mot trusler, og anvende beste praksis innen cybersikkerhet for å utvikle og vedlikeholde en SMB-håndbok som

	- Spesialproblem om personvern for ansattes personlige opplysninger	effektive risikostyrings- og hendelsesresponsstrategier, og utvikle omfattende forretningskontinuitetsplaner skreddersydd for organisasjonens behov. **Kompetanse:** Elevene vil være kompetente i å utvikle og implementere en cybersikkerhetshåndbok for små og mellomstore bedrifter, lede sikkerhetsprosjekter og team effektivt, og sikre tilpasning til organisatoriske mål og overholdelsesforpliktelser.	adresserer sikker passordoppretting, surfing, e-postsikkerhet og databeskyttelse. **Kompetanse:** Elevene vil være kompetente til å vurdere og redusere sikkerhetstrusler, effektivt kommunisere retningslinjer og praksis for cybersikkerhet, og systematisk rapportere sikkerhetshendelser i SMB-en, som beskrevet i deres tilpassede cybersikkerhetshåndbok.
Organisatoriske ferdigheter			
- **Hvordan gjennomføre implementering av nye rutiner og arbeidsmåter innen cybersikkerhet på SMB-arbeidsplasser**	**Sikkerhetsstyring og -policy** - Organisatorisk kontekst - Personvern - Lover, etikk og samsvar - Styring av sikkerhet - Kommunikasjon på leder- og styrenivå - Ledelsesmessige retningslinjer	**Kunnskap**: Elevene vil få avansert kunnskap om hvordan man implementerer nye cybersikkerhetsrutiner og arbeidsflyter på SMB-arbeidsplasser, som inkorporerer gjeldende cybersikkerhetsprinsipper, trender og overholdelse av nasjonal og internasjonal lovgivning som er relevant for deres bransje. **Ferdigheter**: Elevene vil være dyktige i å bruke avanserte metoder for å gjennomføre risikovurderinger, designe	**Kunnskap**: Elevene vil få praktisk kunnskap om hvordan man integrerer nye cybersikkerhetsrutiner og praksiser på SMB-arbeidsplasser, i samsvar med lovgivning, standarder, strategier og retningslinjer for informasjonssikkerhet, risikostyring og databeskyttelse. **Ferdigheter**: Elevene vil være dyktige i å bruke cybersikkerhetsverktøy og programvare for å implementere nye sikkerhetsrutiner, identifisere og redusere risiko, og fremme viktige cybersikkerhetspraksis som sikker

		og implementere nye cybersikkerhetsrutiner, og utarbeide responsstrategier, noe som sikrer effektiv styring og overholdelse på SMB-arbeidsplasser. **Kompetanse**: Elevene vil være kompetente i å utvikle og implementere strategiske retningslinjer for cybersikkerhet, lede initiativer for å etablere nye rutiner og arbeidsflyter på SMB-arbeidsplasser, og ta etiske beslutninger som samsvarer med organisatoriske mål og samsvarskrav.	passordoppretting, surfing og datahåndtering innenfor styringsrammen for SMB-arbeidsplasser. **Kompetanse:** Elevene vil være kompetente til å vurdere og redusere potensielle sikkerhetstrusler, effektivt kommunisere cybersikkerhetsendringer og retningslinjer, og nøyaktig rapportere sikkerhetshendelser i små og mellomstore bedrifter i henhold til styrings- og samsvarskrav.
-**Gjennomføre lederstøtte innen cybersecurity-feltet.**	**Planlegging av cybersikkerhet** - Strategisk planlegging - Operativ og taktisk ledelse	**Kunnskap**: Elevene vil få avansert kunnskap om hvordan man integrerer avanserte cybersikkerhetsprinsipper og dagens trender i strategisk planlegging og operativ ledelse. **Ferdigheter**: Elevene vil være dyktige i strategisk planlegging og operativ ledelse, slik at de effektivt kan utforme og implementere cybersikkerhetsstrategier som adresserer nye risikoer og sikrer robuste taktiske svar. **Kompetanse**: Elevene vil være kompetente i å utvikle og implementere strategiske	**Kunnskap**: Elevene vil få praktisk kunnskap om hvordan man integrerer strategisk planlegging og operativ ledelse i cybersikkerhet for å beskytte organisatoriske verdier, overholde relevant lovgivning og standarder, og implementere effektive informasjonssikkerhetsstrategier og risikostyringspolitikk. **Ferdigheter**: Elevene vil være dyktige i å identifisere cybersikkerhetsrisiko, bruke strategisk planlegging og operasjonelle styringsverktøy for å beskytte mot trusler, og fremme implementeringen av grunnleggende cybersikkerhetspraksis innenfor deres lederstøtteroller.

		cybersikkerhetsrammer, lede og administrere cybersikkerhetsinitiativer.	**Kompetanse:** Elevene vil være kompetente i å vurdere og redusere sikkerhetstrusler, effektivt kommunisere cybersikkerhetsstrategier og problemer, og pålitelig rapportere hendelser og sårbarheter til de aktuelle kanalene i deres organisasjoner.

6. STRATEGI FOR EVALUERING AV KURS

Evaluering av kunnskap er en integrert del av læringsprosessen og fremmer dypere læring. Dette kapittelet beskriver tilnærmingen til kursvurdering som er nødvendig for å sikre at alle deltakere i CyberAgent-kurs oppnår de nødvendige læringsutbyttene og kompetansene. Vurderingsprosessen i kurset er delt inn i to hoveddeler: egenvurdering og kunnskapsvurderingstester, som er skreddersydd for både høyere utdanning (HEI) og yrkesopplæring (VET) studenter, og tar hensyn til deres ulike behov og læringsmål.

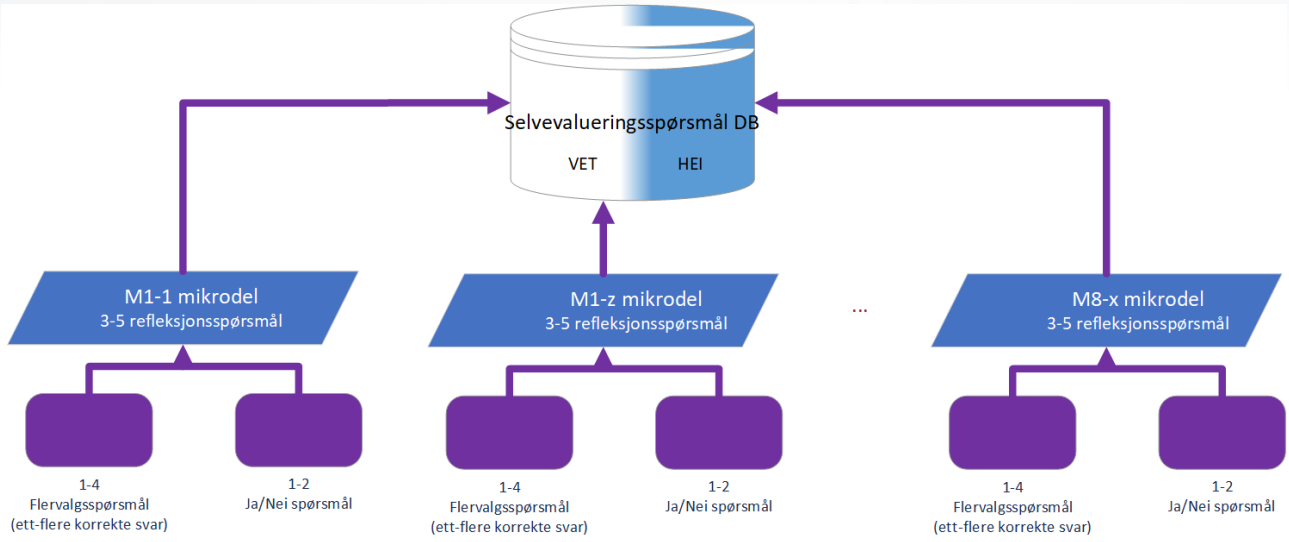
Siden temaene i modulene kan være de samme for både HEI og VET, kan noen av spørsmålene være egnet for både HEI- og VET-kurs. Ved utformingen av spørsmålene vil det derfor være mulig å spesifisere om spørsmålet bare er ment for VET eller HEI, eller for begge deler. Denne måten å markere på vil bare bli brukt ved utforming av spørsmålene, da det vil lette utformingen av spørsmålene. Når spørsmålene er importert til plattformen, vil databasene være forskjellige for VET og HEI.

Figur 12. Databaser for selvevaluering og kunnskapsevaluering

1. Egenvurderingstester: Etter å ha fullført hvert tema i kurset, skal studentene gjennomføre selvvurderingstester. Disse vurderingene er utformet for å gi umiddelbar tilbakemelding, og for å hjelpe elevene til å måle deres forståelse av det nylig gjennomgåtte materialet. Dette stadiet oppmuntrer til selvrefleksjon og hjelper til med å styrke læringsmålene for hvert emne. I tillegg tillater det elevene å identifisere områder der de kan trenge videre studier eller avklaring, og fremme en proaktiv tilnærming til læringsreisen.

Ved å bruke egenvurderingstester kan deltakerne identifisere det innledende kunnskapsnivået og kontrollere fremgangen etter hvert opplæringsemne.

En selvvurderingsquiz med 3-5 spørsmål, med en blanding av sant-usant, eller lignende, og/eller flervalgsspørsmål anbefales. Et annet emne skal låses opp først etter at alle spørsmålene er besvart riktig. Det skal ikke være noen tidsbegrensninger eller begrensninger på forsøk. Forsøk bør tilfeldig velge spørsmål fra i henhold til databasen.



Figur 13. Datadatabasestruktur for selvevaluering

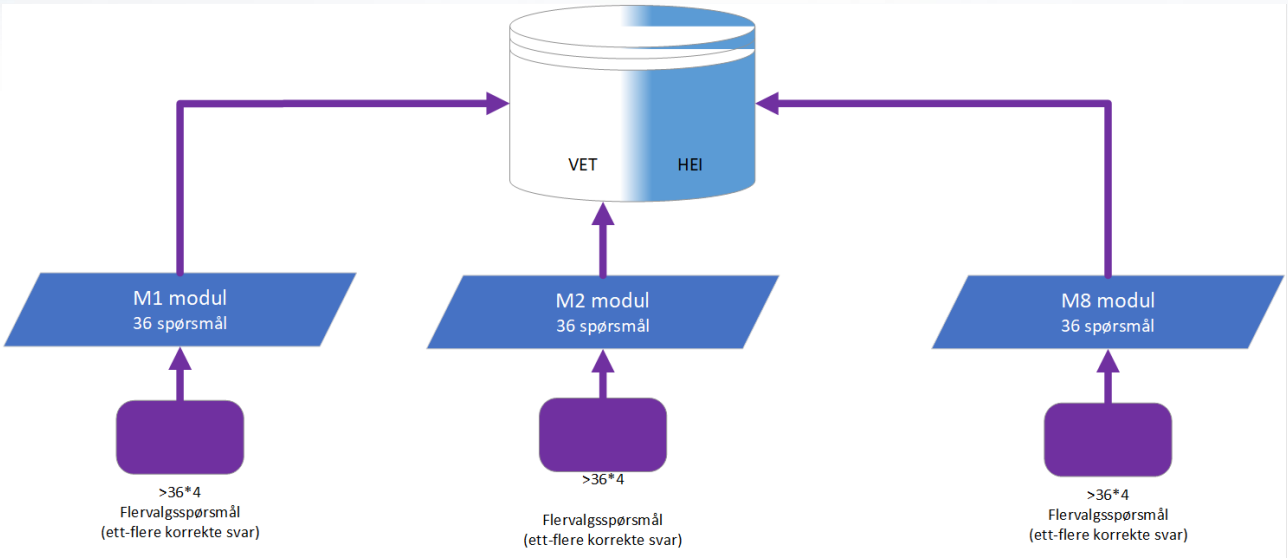
2. Kunnskapsvurderingstest*: Etter å ha fullført alle emner i kurset, vil studentene bli pålagt å ta en avsluttende test for å få kursbevis. Denne omfattende vurderingen evaluerer deres generelle forståelse og mestring av kursinnholdet. Den endelige testen vurderer studentenes oppbevaring av materialet og identifiserer hvor godt de kan bruke sin kunnskap i en bredere sammenheng.

* Under utviklingen av læreplanen og materialene vil andre metoder for å vurdere gjennomføringen av kurset og vurderingen av kunnskap bli vurdert, for eksempel case-studier, praktiske øvelser og reflekterende rapporter, noe som vil muliggjøre en mer omfattende vurdering av deltakernes analytiske og kritiske tenkning ferdigheter. Denne tilnærmingen vil også være tilgjengelig for forelesere for HEI- og VET-studenter i kursgjennomføringen.

Ved å bruke kunnskapsvurderingstestkurs kan deltakerne identifisere sitt endelige kunnskapsnivå, og hvis bestått – motta et fullføringsmerke (sertifikat).

En kunnskapsvurderingstest på 36 spørsmål, med en blanding av sant/usant eller lignende og flervalgsspørsmål anbefales. Det skal være en tidsbegrensning på 45 minutter, og bare ett forsøk tillatt. Testen bør administreres ved tilfeldig valg av spørsmål fra en database.

I tillegg bør vurderingen også vurdere forebygging av fusk, og derfor bør det utvikles omtrent fire sett med spørsmål. Noen av kunnskapstestspørsmålene for både VET og HEI kan overlappe, så vi vil ha tre attributter på utviklingstidspunktet: VET, HEI eller VET og HEI.



Figur 14. Struktur i databasen for kunnskapsevaluering

Denne to-trinns vurderingsstrategien støtter ikke bare effektiv læring ved å gi flere tilbakemeldingssløyfer, men gir også elevene mulighet til å ta en aktiv rolle i opplæringen.

Egenvurderingstester og tester for kunnskapsvurdering vil bli utviklet etter pensum i emnene og på grunnlag av resultater og anbefalinger utviklet i dette prosjektet.

SAMMENSETNING AV SPØRSMÅLSDATABASE

For å sikre en tilstrekkelig stor og balansert spørsmålsbase, vil det bli opprettet minst 5 sanne/falske eller matchende spørsmål og 5 flervalgsspørsmål for hvert emne i VET- eller HEI-kurset.

Forutsatt at det vil være minst 10 emner i hvert kurs, bør samlet grunnlag for hvert VET- eller HEI-kurs inneholde minst 10-20% sant/usant eller lignende, og 90-80% flervalgsspørsmål. Dette er en generell retningslinje, men læreren vil ha mulighet til å velge strukturen på spørsmålene i henhold til kursets emne.

Med tanke på forskjeller i yrkesfaglige/HEI læringsmål og resultater, bør den samlede sammensetningen av spørsmålsdatabasen for et enkelt kurs inneholde som det er vist i tabellen nedenfor.

Tabell 5. Spørsmålstyper

	Sanne/falske eller samsvarende spørsmål	Flervalgsspørsmål
Generell del av kurset	20%	80%
VET-spesifikke del av kurset	20%	80%
HEI-spesifikke del av kurset	20%	80%
Totalen for et VET og HEI-kurs	20%	80%

RETNINGSLINJER FOR SPØRSMÅLSKONSTRUKSJON

Spørsmål til egenvurdering og kunnskapsvurderingstester må utarbeides på engelsk og deretter lokaliseres til partnerspråk.

Når du utvikler testspørsmål for både egenvurdering og kunnskapsvurdering i kurset, er det viktig å sikre at spørsmålene er klare, tydelige og tilgjengelige for alle kandidater, uavhengig av bakgrunn. Denne tilnærmingen sikrer at vurderingene nøyaktig gjenspeiler elevenes forståelse av kursinnholdet og deres evne til å oppfylle de oppgitte ferdighetene og målene som er skissert i kursplanene.

Generelle retningslinjer for spørsmålskonstruksjon:

Klare retningslinjer vil bli brukt i utviklingen av testspørsmålene: spørsmålene må være forståelige og direkte relatert til læringsmålene for kurset, uten bruk av kompleks terminologi eller forvirrende formulering. Kulturspesifikke eller forvirrende spørsmål vil også unngås for å sikre rettferdighet og tilgjengelighet for alle kursdeltakere. Ytterligere veiledning om utformingen av spørsmålene er gitt nedenfor.

Klarhet og enkelhet: Spørsmålene må være enkle, unngå bruk av komplekst språk eller sjargong som kan forvirre eller villede kandidatene. Målet er å vurdere kandidatenes kunnskap og forståelse av fagstoffet, ikke deres evne til å tyde kompliserte spørsmål.

Direktehet og relevans: Hvert spørsmål skal direkte forholde seg til de viktigste ferdighetene og målene for kursplanene. Irrelevant eller tangentielt innhold bør unngås for å opprettholde fokus på vurdering av tiltenkt læringsutbytte.

Kultur- og bakgrunnssensitivitet: Sørg for at spørsmålene ikke forutsetter spesifikk kulturell kunnskap eller erfaringer, noe som gjør dem tilgjengelige og rettferdige for kandidater med ulik bakgrunn.

Ingen lure spørsmål: hensikten med hvert spørsmål bør være klar, uten forsøk på å villede eller lure kandidatene. Spørsmål som er utformet for å 'ta' kandidater eller for å teste deres evne til å oppdage lureri, vurderer ikke effektivt deres forståelse av emnet.

Entydig og kortfattet presentasjon: Spørsmål bør formuleres på en måte som ikke gir rom for tolkning, slik at alle kandidater forstår spørsmålet på samme måte. Hold spørsmålene tydelige, unngå unødvendig lengde som kan skjule hovedpoenget.

Positiv formulering: unngå å bruke negativ frasering i spørsmål (f.eks. "Hvilket av følgende er IKKE ..."). Negativ formulering kan føre til forvirring og feiltolkning, spesielt under eksamensforhold. I stedet ramme alle spørsmål positivt for å fremme klarhet.

Spesifikke retningslinjer for spørsmålskonstruksjon:

Flervalgsspørsmål: Sørg for at alle alternativene er plausible og relevante for spørsmålet. Det riktige svaret bør være udiskutabelt riktig, mens distraktorene skal være klart feil for noen som forstår materialet.

Sant/usant spørsmål: Presenter klare, saklige utsagn som er direkte relatert til kursinnholdet, slik at det ikke er tvetydighet om deres sannhetsverdi.

Samsvarende spørsmål: Sørg for at begge listene (f.eks. termer på den ene siden og definisjoner på den andre) er tydelig relatert og at det er et enkelt grunnlag for å gjøre hver kamp. Unngå ujevne lister der antall elementer ikke justeres med mindre det er uttrykkelig angitt at enkelte elementer ikke vil bli brukt eller kan brukes flere ganger.

Pilotopplæringen vil analysere informasjon om kunnskapsvurderingsmetoder og vurderingsprosessen ved å samle tilbakemeldinger fra både elever og instruktører. Dette vil gjøre det mulig å vurdere hensiktsmessigheten av kunnskapsvurderingsmetodene og, om nødvendig, å utfylle eller forbedre vurderingsmetoden.

GAMIFICATION

Denne delen introduserer beskrivelsen av gamification-elementene implementert i CyberAgent-kurs. Gamification er prosessen med å inkorporere gamification-prinsipper i tradisjonelle læringsaktiviteter for å øke motivasjonen og engasjementet til deltakerne. Disse elementene er valgt på grunnlag av den nyeste forskningen om pedagogisk teknologi, som viser at spillifisering kan forbedre læringsytelsen betydelig, øke studentenes motivasjon til å lære og forbedre deres engasjement i læringsprosessen.

Gamification-elementene som vil bli integrert i kursene inkluderer merker, poeng, rangeringer og fargekodede kallenavn som gjenspeiler deltakerens erfaring og prestasjoner.

- Det tildeles merker for:

- **Gjennomføring av modulen**.
- **For å bestå en test basert på beståttprosenten**. For eksempel vil en deltaker bli tildelt et bronsemerke for en minimum bestått poengsum på den endelige testen, et sølvmerke for en minimum bestått poengsum på 75%, et gullmerke for en bestått poengsum på 76% - 90% og et platinamerke for en bestått poengsum på 90% -100%. I dette tilfellet kan en deltaker ha 8 merker av denne typen.

- **Fullfører emnet**.
- **Logger på systemet hver dag i ti dager**.
- **Et spesielt aktivitetsmerke** for hvert tema vil også bli tildelt av kursets mentor/instruktør.

- **Poeng og score** beregnet på grunnlag av egenvurderingstestresultater + endelige testresultater med multiplikator.

Deltakerne på CyberAgent-kurset vil ikke kunne se fremgangen sin individuelt, men vil kunne konkurrere med andre deltakere i grupper eller lag (basert på det høyeste antall poeng som er scoret, men også basert på flest merker). Dette oppmuntrer ikke bare til individuell, men også lagkonkurranse og samarbeid, noe som er viktig for å utvikle samarbeidsevner.

Hver deltaker vil se sitt kallenavn når han/hun logger inn på kurset, som vil bli fargekodet i henhold til kursprogresjonen og erfaringen som er samlet inn (kurs gjennomført/registrert).

Dette vil hjelpe kursdeltakerne til å involvere seg bedre i opplæringsprosessen. Kursdeltakere kan gjenta den samme testen flere ganger for å forbedre poengsummen sin (poeng tildeles for det høyeste antallet egenvurderingstester som er tatt riktig).

En spesiell algoritme vil beregne hver deltakers poengsum ved å ta hensyn til tiden det tar å svare, antall ganger testen gjentas og andre parametere, og dermed minimere muligheten for juks.

Alle gamification-regler vil bli tydelig beskrevet og kommunisert til deltakerne, slik at alle enkelt kan forstå hvordan de forskjellige gamification-nivåene kan oppnås og hvordan de beregnes.

7. CYBERAGENT LÆRINGS-/UNDERVISNINGSPROSESS

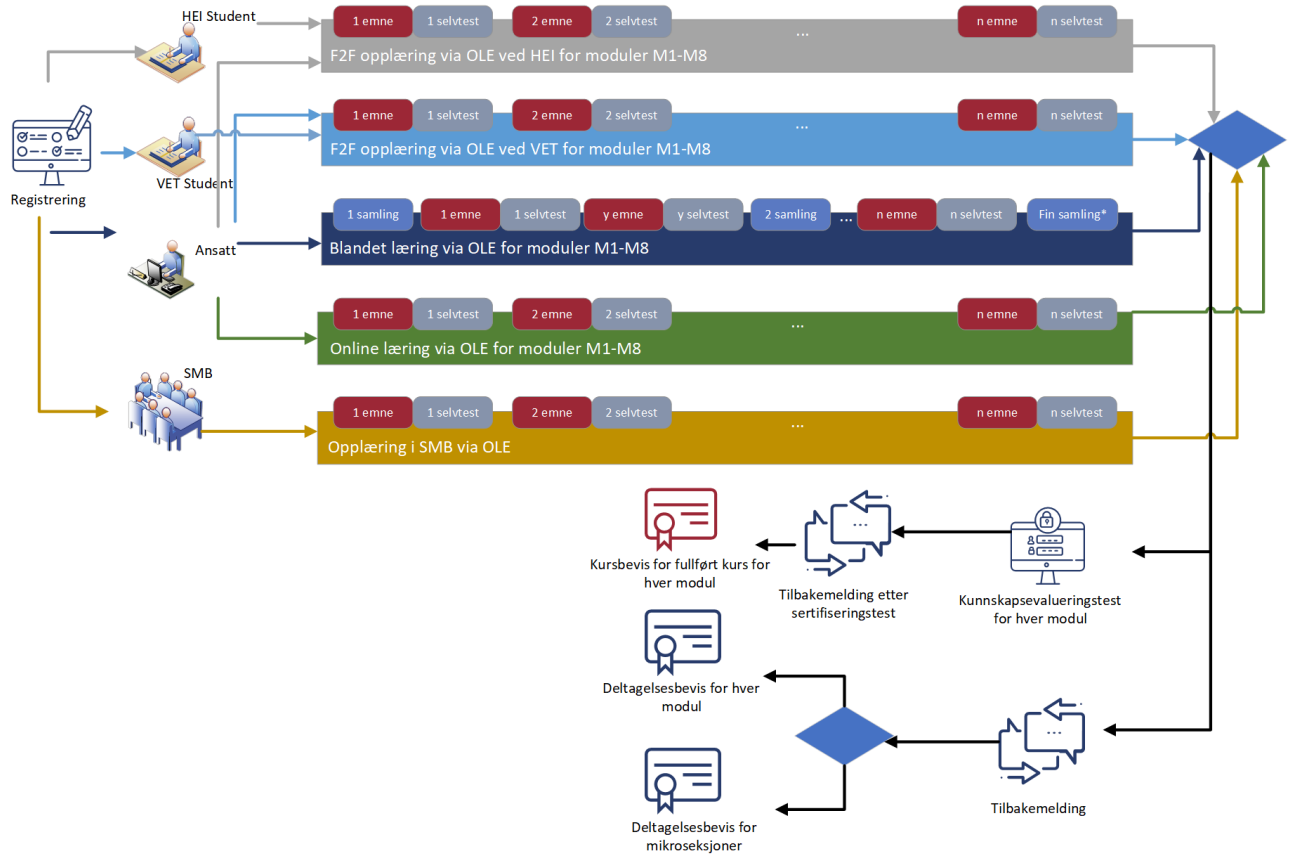
Denne delen oppsummerer informasjonen fra alle kapitlene i dette dokumentet og beskriver i detalj lærings- / undervisningsprosessen, som starter med innmelding i et CyberAgent-kurs på læringsplattformen og slutter med fullføring av kurset eller utstedelse av et sertifikat.

CyberAgent-kursene er designet for å imøtekomme et mangfoldig utvalg av elever, inkludert studenter fra høyere utdanningsinstitusjoner (HEI), yrkesutdanning og opplæring (VET) studenter, samt ansatte fra små og mellomstore bedrifter. Vi tar sikte på å gi hver deltaker muligheten til å velge den læringsmåten som passer dem best, med tanke på deres personlige forhold og opplæringsinstitusjonens organisasjonspolitikk.

Til tross for lærings-/treningsmetoden som er valgt, registrerer deltakerne seg på CyberAgent-plattformen og bruker plattformen under opplæringen.

Registrering

Potensielle deltakere som er interessert i å melde seg på CyberAgent-kurset, må fylle ut et registreringsskjema, velge ønskede moduler og foretrukket læringsmetode. Et konseptuelt diagram er gitt for å veilede deltakerne gjennom læringsveien fra den første til den åttende CyberAgent-modulen.



Figur 15. CyberAgent lærings- / undervisningsforløp

Konfidensialitet av deltakernes informasjon vil bli sikret under registreringsprosessen, spesielt med hensyn til GDPR-krav. Under registreringen vil deltakerne ha mulighet til å gjøre seg kjent med reglene for treningsplattformen, personvern og databeskyttelsesregler.

Deltakerregistreringsdata er bare tilgjengelige for utpekte personer i partnernes organisasjon, i samsvar med interne organisasjonsretningslinjer. Under pilotopplæringsøkter kan deltakerdata fra prosjektpartnere være tilgjengelige for CyberAgent-koordinatoren, og de andre partnerne har ikke lov til å se hverandres deltakerdata. Ved prosjektslutt kan koordinator kun få tilgang til anonymiserte data fra andre partnere for å overvåke prosjektresultater, som spesifisert i prosjektsøknaden, i opptil 5 år etter prosjektets avslutning.

Vi tilbyr skreddersydde opplæringsalternativer for å møte behovene til våre ulike målgrupper. HEI og VET-studenter kan engasjere seg i opplæringen gjennom universitetskontakt. SMB-ansatte kan velge læringsmetoden som passer best for deres behov: blandet læring, kun online, eller, mindre vanlig, bli med på HEI- eller VET-forelesninger.

Opplæring kan også tilbys til større bedrifter med flere ansatte. I slike tilfeller vil opplæringsmetoden bli tilpasset for å møte spesifikke behov, samtidig som CyberAgent-modulkursene inkorporeres.

Ved registrering på plattformen velger deltakerne sin læringsmetode og begynner studiene. Etter å ha fullført en modul eller en del av en modul, kan de kvalifisere seg for et deltakerbevis eller et kursbevis, hvorav sistnevnte utstedes dersom en deltaker består modultesten med en poengsum på minst 75%.

Til slutt må deltakerne fylle ut et tilbakemeldingsskjema før de mottar et sertifikat. Denne tilbakemeldingen er avgjørende for kontinuerlig forbedring av våre opplæringstilbud og for å sikre deltakernes tilfredshet.

Lærings-/opplæringsmåter

Ansatte har flere alternativer for å engasjere seg i emneinnholdet:

- Dersom høgskoler eller yrkesfaglige institusjoner tillater at ansatte deltar som gjestedeltaker, kan den ansatte delta i forelesninger sammen med påmeldte studenter. Slike eksterne deltakerøkter kan organiseres 1-2 ganger per år, basert på den publiserte forelesningsplanen.
- Ansatte kan velge en blandet opplæringsmetode, der opplæringsøkter gjennomføres på bestemte datoer med en anbefalt varighet på 2-4 måneder. Grupper på minst 10 deltakere anbefales, med maksimalt 30 deltakere per gruppe. Blandet opplæring inkluderer både ansikt til ansikt og online konsultasjoner i begynnelsen, under og på slutten av kurset for å lette direkte tilbakemelding og forberedelse til sluttvurderingen.
- Ansatte kan velge den elektroniske læringsmåten for læring i eget tempo, uten fast varighet for kursgjennomføring.
- Ytterligere detaljer om CyberAgent-moduler er gitt i avsnitt 1. Studieforløp.

Studentenes medvirkning

Studenter som er påmeldt cybersecurity-studiet, kan støte på forskjellige veier basert på deres akademiske institusjons forskrifter. De kan enten bli pålagt å fullføre noen eller alle CyberAgent-modulene, eller, avhengig av interne universitetspolitikker, kan studenter som oppfyller kriteriene velge å studere en eller flere CyberAgent-moduler. HEI- eller VET-studenter engasjerer seg vanligvis med fagene gjennom tradisjonell klasseromsinstruksjon som tilbys av institusjonen, eller kan velge selvstudiemetoder for å forberede seg til den endelige kunnskapsvurderingstesten.

Involvering av små og mellomstore bedrifter

I organisasjoner der opplæring i cybersikkerhet anses som nødvendig, kan en representant fra selskapet registrere organisasjonen for interne opplæringsøkter. I slike tilfeller, etter separat avtale med universitetet og / eller instruktører, kan metoden for opplæring, tidsplan og utstedelse av sertifikater skreddersys til organisasjonens spesifikke behov basert på eksisterende moduler.

Innsamling av tilbakemeldinger

Etter modulens ferdigstillelse må deltakerne fylle ut et anonymt tilbakemeldingsskjema som er tilgjengelig online. Tilbakemeldingsdata er bare tilgjengelige for autorisert personell i partnerens organisasjon, med lignende konfidensialitetstiltak brukt under pilotopplæringsøkter og databruk etter prosjekt.

Tilbakemeldinger vil i hovedsak bli innhentet fra kursdeltakerne, men tilbakemeldinger fra mentorer/kursholdere vil også bli samlet inn. Tilbakemeldingene som samles inn vil vurdere deltakernes organisatoriske tilfredshetsnivå, aspekter ved kursorganiseringen, læringsprosessen, bruken av de tilegnede kompetansene i praksis, innholdet i kurset, vurderingsstrategier, inkludering av gamification-elementer, forbedringsområder osv.

Resultatene av tilbakemeldingene vil regelmessig bli gjennomgått og presentert for prosjektledelsen for å reagere raskt og forbedre opplæringsstrategiene i henhold til reelle behov og markedsendringer.

Først etter å ha fylt ut dette skjemaet, er deltakerne kvalifisert til å få et deltakerbevis eller å få kursbevis eller deltakerbevis.

Sertifikat for fullføring av kurs

Vellykket gjennomføring av vurderingstesten resulterer i generering av et kursbevis for deltakeren. Det er en siste test per modul.

Sertifikat for deltakelse

Deltakere som velger å ikke ta kunnskapsvurderingstesten, kan motta et deltakerbevis. Denne bekreftelsen kan utstedes ved gjennomføring av en enkelt modul eller flere mikrodeler i kurset.

KONKLUSJONER OG SAMMENDRAG

Denne rapporten har utviklet strukturerte læringsbaner for endringsagenter for cybersikkerhet i små og mellomstore bedrifter, skreddersydd for å imøtekomme de spesifikke behovene på ulike utdannings- og yrkesnivåer, fra HEI til yrkesfag og direkte opplæring av SMB-ansatte. Læreplanen utvikles, bestående av åtte omfattende moduler, integrerer tekniske, analytiske, organisatoriske og risikostyringsevner som er avgjørende for effektiv styrking av fremtidige cybersecurity-fagfolk.

Den strukturerte tilnærmingen til læringsveier sikrer en omfattende utdanningsreise for SMB-ansatte. Gjennom stadier av Pre-læring, læring og Post-læring, støtter den kunnskapsoppbevaring og praktisk anvendelse. Mikromoduler gir fleksibilitet og tilpasningsevne til individuelle behov, og forbedrer læring med mikrocredits som gir anerkjente kvalifikasjoner. Denne tilpasningen til bransjestandarder bidrar betydelig til å styrke cybersikkerhetskapasiteten i små og mellomstore bedrifter, og forbereder ansatte på å møte dagens utfordringer og fremtidige fremskritt. Følgende karriereforløps-analyse har kartlagt utviklingen av cybersikkerhetsroller som definert av ESCO-rammeverket, og legger til rette for en målrettet pedagogisk tilnærming som forbereder enkeltpersoner på effektiv integrering i cybersikkerhetsarbeidsstyrken, og til slutt forbedrer karriereutsiktene og faglig utvikling.

Det utforskede mangfoldet av pedagogiske tilnærminger innenfor læreplanen for cybersikkerhet bør gi rom for et dynamisk og fleksibelt læringsmiljø som imøtekommer ulike læringsstiler og behov. Inkorporering av ulike undervisningsmetoder, inkludert teoretiske forelesninger, praktiske laboratorier, gamification og samarbeidsprosjekter, sikrer at studentene ikke bare er mottakere av kunnskap, men aktive deltakere i deres læringsreise. Denne omfattende strategien skal øke engasjementet, forståelsen og forberede studentene bedre på virkelige cybersikkerhetsutfordringer. Tilpasningsevnen til undervisningsmetoder til modulspesifikke krav bør ytterligere tilpasse læringsopplevelsen, slik at utdanningsresultatene maksimeres for hver student.

Ved systematisk å kartlegge CyberAgent-prosjektets underemner og moduler til internasjonalt anerkjente kunnskapsenheter, oppfyller læreplanen ikke bare, men forutser de dynamiske kravene til cybersecurity-feltet. Denne metodiske tilnærmingen sikrer at hvert læringsutbytte er strategisk knyttet til virkelige kompetanser som er avgjørende for effektiv styring av cybersikkerhetstrusler. Læreplanens tilpasningsevne gjør det mulig å betjene ulike faglige roller i bransjen, forberede elevene ikke bare for umiddelbare utfordringer, men for langsiktig karriereutvikling innen cybersikkerhet.

Kursvurderingsstrategien som er skissert, gir et rammeverk for å evaluere ferdigheter og fremgang for studenter i cybersecurity-programmer. Denne to-trinns tilnærmingen, som kombinerer selvvurderingstester og omfattende kunnskapsevalueringstester, lar elevene aktivt engasjere seg i materialet, kontinuerlig evaluere forståelsen og justere læringsstrategiene tilsvarende. Ved å utforme vurderingen for å imøtekomme både høgskoler og yrkesfagstudenter med skreddersydde spørsmål, sikrer strategien relevans og hensiktsmessighet for hvert utdanningsnivå, og forbedrer læringsopplevelsen. Denne metoden muliggjør et klart mål på

studentens mestring og beredskap til å anvende sin kunnskap praktisk. Videre motiverer innføringen av gamification-elementer som merker og poengsystemer ikke bare studenter, men fremmer også et konkurransedyktig, men samarbeidende læringsmiljø.

Til sist, gir CyberAgent lærings- og undervisningsprosessen et omfattende og tilpasningsdyktig pedagogisk rammeverk som passer for et mangfoldig utvalg av elever fra HEI, VET-institusjoner og små og mellomstore bedrifter. Dette systemet gir mulighet for ulike deltakende metoder, inkludert ansikt til ansikt, blandet og online læring, noe som sikrer fleksibilitet i hvordan opplæring i cybersikkerhet leveres og åpnes. Registrering på CyberAgent-plattformen starter en vei der deltakerne velger foretrukne moduler og læringsmetoder, som ender i utstedelse av sertifikater etter vellykket gjennomføring og vurdering. Denne strukturen støtter ikke bare personlige læringsbaner, men justerer også de strenge personvernstandardene som er avgjørende for å opprettholde deltakernes konfidensialitet gjennom hele opplæringsprosessen.

Anbefalingene og veiledningen gitt i dette dokumentet vil bli brukt i neste fase for å utvikle CyberAgents omfattende opplæringsplaner, opplæringsmateriell, kunnskapstester og vurderinger, øvelsesøvelser og annet opplæringsinnhold, som vil bli integrert i CyberAgent-opplæringsplattformen.

VEDLEGG 1. MODULBESKRIVELSE

MODULEBESKRIVELSE

Modultittel	Modulkode
...	

Foreleser(e)	Institusjon eller avdeling hvor modulen blir gjennomført
...	...

Leveringsmåte	Språk
Ansikt-til-ansikt online, blandet, konsultasjoner	*engelsk, ...*

Forkunnskaper
...

Antall studiepoeng tildelt	Studentens arbeidsmengde	Kontakt arbeidstid	Individuell arbeidstid
5	...	...	...

Formål og resultater av modulen		
...		
Læringsutbytte av modulen	**Undervisnings- og læringsmetoder**	**Vurderingsformer**
Tekniske ferdigheter		
Analytiske ferdigheter		
Risikostyring		
Organisatoriske ferdigheter		

Tilrettelegge for ressurser (utstyr, programvare, teknologi)
...

Modulinnhold: Emneinndeling	Kontakt arbeidstimer					Individuelle arbeidstimer og oppgaver	
	Forelesninger (HEI/VET)	Konsultasjoner	Øvelser (HEI/VET)	Prøver	**Alle arbeidstimer for kontakt**	**Individuell arbeid**	**Oppgaver**
1							
...							
n							
Totalt antall timer							

Vurderingsstrategi	Komparativ vektningsprosent	Vurderingskriterie
Selv-evaluering 1		...
...		...
Selv-evaluering n		...
Kunnskapsevaluering		...
HEI/VET Sertifisering -> Selv-evaluering I + ...+ Selv-evaluering n + Kunnskapsevaluering		
SMB/Selv-studiesertifisering -> Selv-evaluering I + ...+ Selv-evaluering n + Kunnskapsevaluering		
Mikromoduler, mikroseksjon -> Selv-evaluering I (ikke obligatorisk), Selv-evaluering n (ikke obligatorisk)		

Studiemateriell *(Etternavn, første initial. (År, Måned, Dag). Artikkeltittel. Magasin/tidsskrift/avistittel, volumnummer (utgavenummer), sidetall for hele artikkelen, utgiver, URL)*
Nødvendig lesing
...
Anbefalt lesing
...

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