CyberAgent

Co-funded by the European Union

PK-YRITYSTEN KYBERTURVALLISUUDEN MUUTOSAGENTTIEN OPPIMISPOLUN RAKENNE

CYBER AGENT 06.2024

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

Työpaketti 2: CyberAgent-lähestymistapa ja rakenteen suunnittelu

Toimitus 2.3: PK-yritysten kyberturvallisuuden muutosagenttien oppimispolun rakenne

Työpaketin 2 johtaja – Olemisen Balanssia ry
Toimituksen 2.3 johtaja – Vilnan yliopisto

SISÄLTÖ

LYHENTEET 2
LUETTELO LUVUISTA 3
TAULUKKOLUETTELO 3
JOHDANTO 4
1. OPINTOPOLKU 7
2. KULJETUSREITTI 11
3. OPETUSMENETELMÄT 15
4. MODUULIN RAKENNE 19
5. KYBERAGENTIN OPETUSSUUNNITELMA JA KOULUTUSOHJELMA 24
6. KURSSIN ARVIOINTISTRATEGIA 33
7. CYBERAGENT-OPPIMIS-/OPETUSPROSESSI 39
PÄÄTELMÄT JA YHTEENVETO 43
LIITE 1. Moduulin kuvaus 45

LYHENTEET

CBL - haasteisiin perustuva oppimismalli

CL - Yhteistoiminnallisen oppimisen malli

EC - Euroopan komissio

ECTS - Eurooppalainen opintosuoritusten siirto- ja kertymisjärjestelmä (European Credit Transfer and Accumulation System)

EQF - Eurooppalainen tutkintojen viitekehys

GICL - Guided Inquiry Collaborative Learning Model - Ohjattu tutkivan oppimisen yhteistoimintamalli

HEI - Korkeakoulut

PBL - projektipohjainen oppimismalli

POGIL - prosessikeskeinen ohjattu tutkivan oppimisen malli (Process Oriented Guided Inquiry Learning Model)

Pk-yritykset - pienet ja keskisuuret yritykset

VET - ammatilliset oppilaitokset

LUETTELO LUVUISTA

Kuva 1. EY:n suuntaviivojen mukainen havainnollistava kaavio kuvaa kahdeksan EQF-tasoa ja tarjoaa visuaalisen esityksen koulutuksen viitekehyksestä 5
Kuva 2. Oppimispolku ennen opintojen aloittamista 7
Kuva 3. Tutkimusten rakenne 8
Kuva 4. Korkeakoulun opintorakenne 9
Kuva 5. Ammatillisen koulutuksen opintojen rakenne 9
Kuva 6. Itsearvioinnin opintorakenne 9
Kuva 7. Mikromoduulin tutkimusrakenne 9
Kuva 8. Oppimispolkujen yhteydet 10
Kuva 9. Edellisessä raportissa määritellyt ESCO-ammatit 12
Kuva 10. Mahdolliset oppimisen jälkeiset polut 13
Kuva 11. Moduulin rakenne 19
Kuva 12. Itsearvioinnin ja osaamisen arvioinnin tietokannat 33
Kuva 13. Itsearviointitietokannan rakenne 34
Kuva 14. Tietämyksen arvioinnin tietokannan rakenne 35
Kuva 15. CyberAgent-oppimis-/opetuspolku 39

TAULUKKOLUETTELO

Taulukko 1. Suositellut opetusmenetelmät 15
Taulukko 2. Työmäärä tunneittain 21
Taulukko 3. Suositellut moduulit työmäärä 21
Taulukko 4. CyberAgent-moduulien tyypillinen rakenne 22
Taulukko 5. Opetussuunnitelman laatimisen etenemissuunnitelma 25
Taulukko 6. Kysymystyypit 36

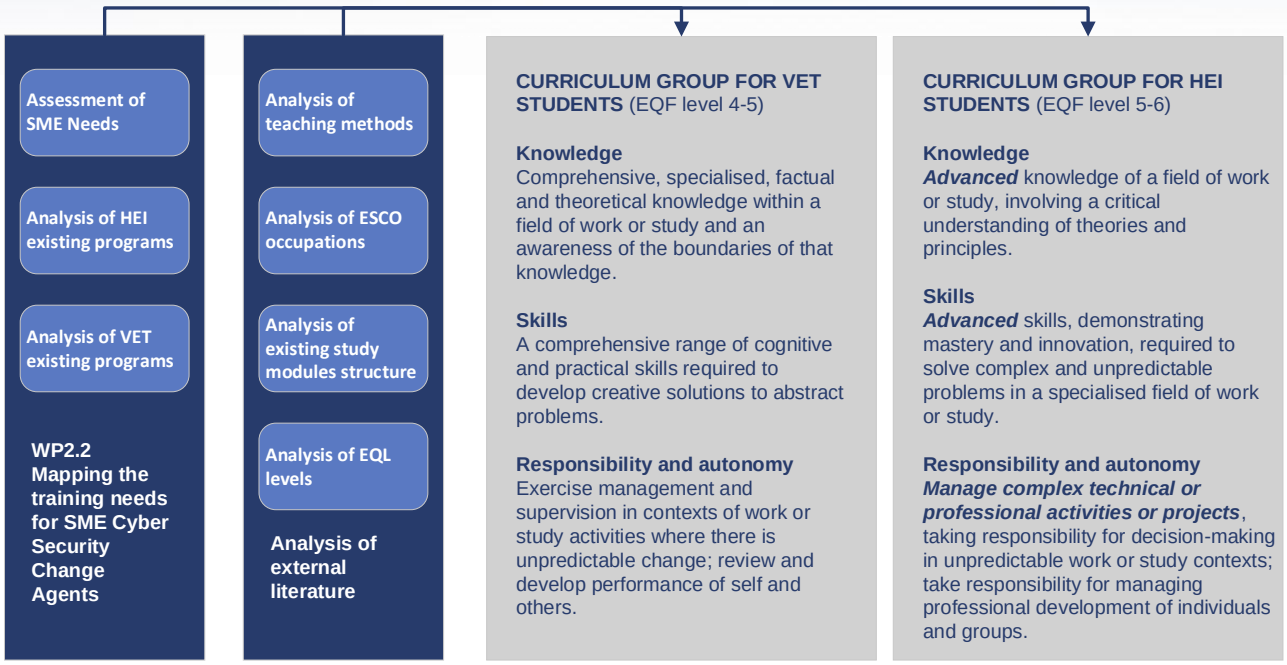
JOHDANTO

Tämän raportin yleistavoitteena on kehittää ja kuvata uusia ammatillisia oppimispolkuja eurooppalaisten pk-yritysten (pk-yritysten) työntekijöiden kyberturvallisuustaitojen kehittämiseksi.

Pk-yritysten kyberturvallisuuden muutosagenttien koulutustarpeiden kartoituksen tulosten perusteella määritettiin ulkoisten resurssien analyysi oppimistuloksista tietojen, taitojen ja pätevyyksien osalta. Tunnistettujen oppimistulosten analyysin perusteella tässä raportissa annetaan ohjeita kahdentyyppisistä, eurooppalaisen tutkintojen viitekehyksen (EQF) tasojen 4-6 mukaisista koulutusohjelmista, jotka kattavat hankkeen kohderyhmiltä, pk-yritysten työntekijöiltä ja opiskelijoilta, vaadittavien taitojen ja tietojen kirjon, ja mukautetaan koulutustulokset koulutettavien erilaisiin taustoihin ja profiileihin.

- EQF-tasoa 4-5 sovelletaan pk-yritysten työntekijöihin, joilla ei ole korkeakoulutaustaa, sekä ammatillisen koulutuksen (VET) opintoihin. Tämä taso tarjoaa tietoverkkoturvallisuuden perustaidot ja -tiedot sekä kevyen erikoistumisen joihinkin moduuleihin.
- Eurooppalaisen tutkintojen viitekehyksen taso 5-6, jota tarjotaan pk-yritysten työntekijöille, joilla on myös riittävä tausta sen seuraamiseen, ja korkeakouluopiskelijoille. Tällä tasolla suoritetaan edistyneempiä ja monimutkaisempia koulutustoimia.

EQF:n tasot päätettiin päivittää tasolle 4-6, jotta ne kattaisivat laajan valikoiman oppimistuloksia, kuten aiemmin mainittiin, mutta myös mahdollistaisivat väylän koulutuksen opetussuunnitelmien välille, jotta ammatillisen koulutuksen opiskelijat ja työntekijät, jotka ovat tasolla 4, pääsisivät tasolle 6. Taso 6 on myös osaamisen kehittämispolku.



Kuva 1. EY:n suuntaviivojen mukainen havainnollistava kaavio kuvaa kahdeksan EQF-tasoa ja tarjoaa visuaalisen esityksen koulutuksen viitekehyksestä.[1]

Opetussuunnitelmassa käsitellään oppimistuloksia ja tarvetta kouluttaa pk-yritysten työntekijöitä, jotta he voivat kouluttautua pk-yritysten kyberturvallisuuden muutosagenttien tehtäviin, sekä kouluttaa korkeakoulujen ja ammatillisen koulutuksen opiskelijoita, jotta he voivat täyttää tehtävänsä opintojen jälkeen. Kussakin opetussuunnitelmassa on kahdeksan moduulia, jotka kattavat neljä alateemaa:

- Tekniset taidot - Ajantasainen tietämys kyberturvauhkista ja niihin liittyvistä oikeudellisista kysymyksistä - Käytännön tietämys siitä, miten kyberturvauhkia käsitellään.
- Analyyttiset taidot - Kriittinen ajattelutapa - Kyky analysoida ja ymmärtää paikallisia uhkia, niiden toteutustapoja, riskiryhmiä jne.
- Riskienhallinta - Opi tarjoamaan ja kuvaamaan pk-yritysten työpaikoille kyberturvallisuusrutiineja - Luo oma työpaikan pk-yrityksille kyberturvallisuuden käsikirja ja miten sitä seurataan.
- Organisaatiotaidot - Miten uusia rutiineja ja toimintatapoja voidaan ottaa käyttöön kyberturvallisuuden alalla pk-yritysten työpaikoilla; johtajien tukeminen kyberturvallisuuden alalla.

Lisäksi keskeinen osa eurooppalaisten pk-yritysten kyberturvallisuustaitojen parantamiseen tähtäävien oppimispolkujen luomista on se, miten mikrotodistukset pannaan täytäntöön. Niiden on viitattava oppimistuloksiin (tiedot, taidot ja pätevyydet), kurssin sisältöön, koulutukseen (tiedot, taidot ja pätevyydet), pelillistämiselementteihin, kestoon ja ECTS-järjestelmän (European Credit Transfer and Accumulation System) määrään. Jotta ne soveltuisivat tarkoitukseen, ne on

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

toteutettava luomalla kumppanuuksia korkeakoulujen, ammatillisen koulutuksen tarjoajien ja kyberturvallisuusalan yksityisten yritysten välille.

Mikrojaksot antavat oppijoille enemmän vapautta valita moduuleja tai moduulien osia ja päättää, minkä tason todistuksen he tarvitsevat: osallistumistodistuksen tai todistuksen kurssin suorittamisesta, johon sisältyy sertifiointitesti eli todiste siitä, että kurssi on suoritettu tietyn osaamisen hankkimisen jälkeen. Kurssin suorittamisesta annetaan todistus, kun on läpäissyt loppukokeen vähintään 75 prosentin tuloksella, ja osallistumistodistus annetaan, kun on osallistunut tiettyjen aiheiden/moduulien lähiopetukseen, yhdistelmäopetukseen tai verkkokoulutukseen. Tämä käytäntö ei ainoastaan lisää koulutuksen sovellettavuutta ja tehokkuutta, vaan se myös lisää motivaatiota oppimiseen ja tarjoaa selkeän arvolähtökohdan osallistujien uran ja jatkokehityksen kannalta.

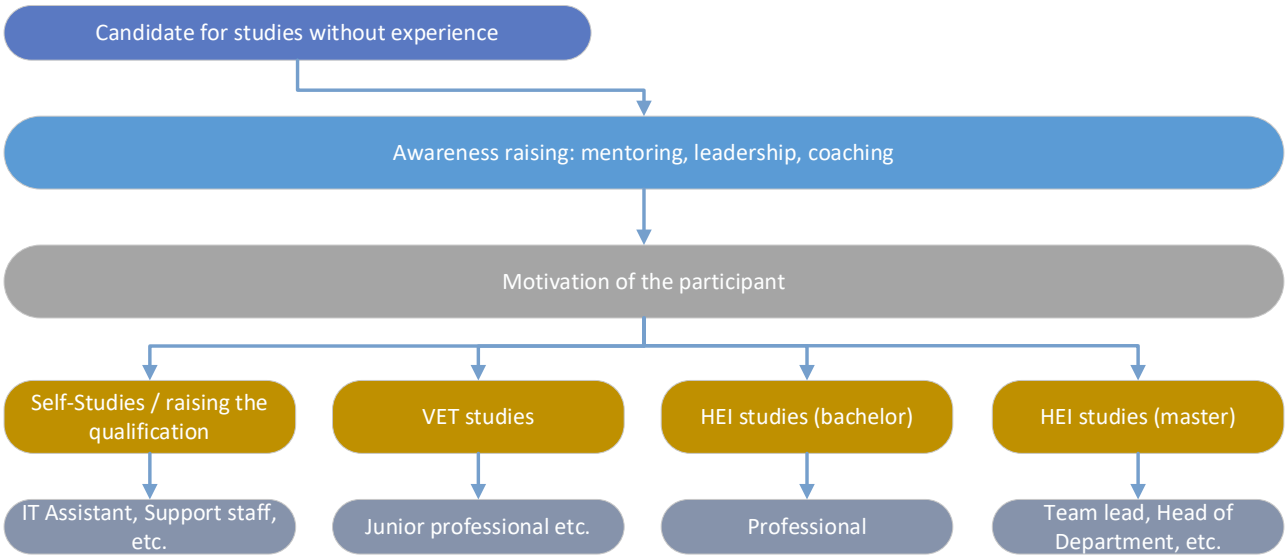
Yleisesti ottaen tässä raportissa esitetään yksityiskohtaiset ohjeet CyberAgent-moduulien kehittämistä varten, mukaan lukien opinto- ja urapolkujen sisällöllinen hahmotelma, koulutus- ja arviointimenetelmät sekä opetussuunnitelmien rakentamisen etenemissuunnitelma.

1. OPINTOPOLKU

Oppimispolku on koko matka, jonka osallistuja kulkee siitä hetkestä, kun hän ymmärtää, että hänen on parannettava taitojaan, aloitettava ja saatettava koulutus päätökseen, siihen hetkeen, kun hän saa oppimisen päätökseen ja alkaa soveltaa saamaansa tietoa. Oppimispolussa on kolme vaihetta:

- Esiopetus,
- Oppiminen,
- Oppimisen jälkeen.

Esiopetusvaihetta havainnollistetaan alla olevassa kuvassa.



Kuva 2. Oppimispolku ennen opintojen aloittamista

Pk-yrityksissä tätä oppimis-/opiskelupolkua voidaan jatkaa. Kuvassa osallistuja joko päättää kouluttautua itse tai häneen vaikuttaa tiedotuskampanja ja hän saa käsityksen koulutuksen hyödyistä, mahdollisuuksista ja urasta, jonka hän voi saada koulutuksen jälkeen.

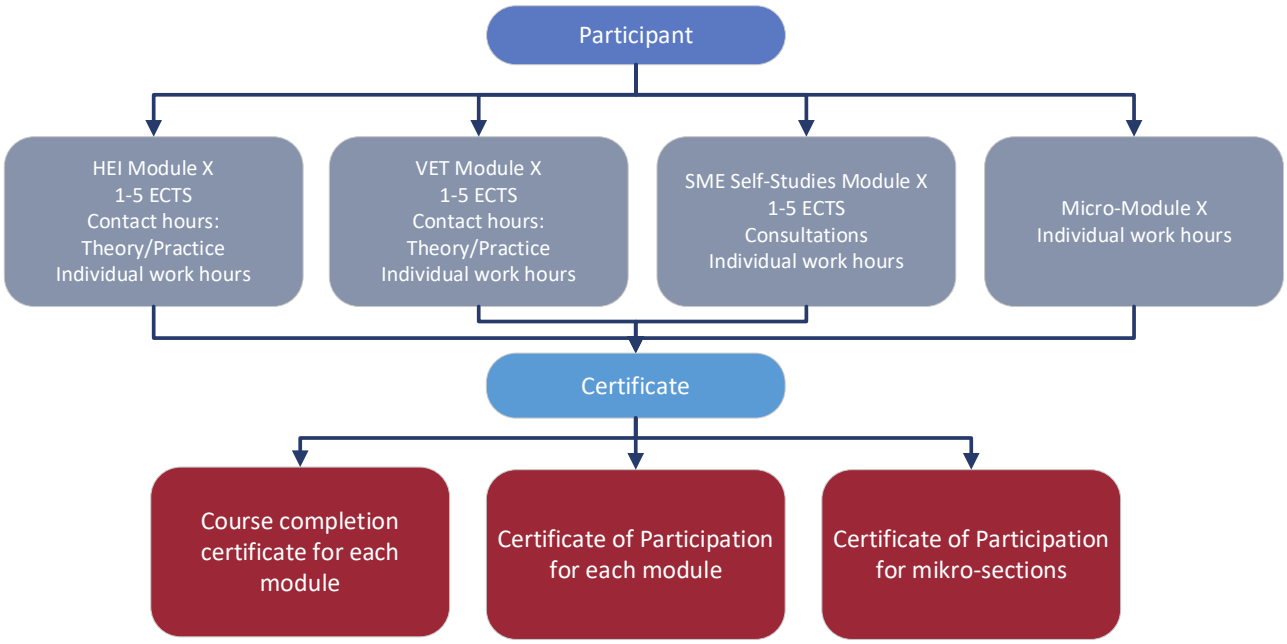
On myös ehdotettu, että oppimispolku on tyypillinen moduuli OLE-rakenteen (Online Learning Environment) avulla. Kirjallisuusanalyysin ja useiden mikroopintosuoritusten periaatetta soveltavien hankkeiden jälkeen , ,[2][3][4] ehdotetaan, että kukin CyberAgent-moduuli olisi 1-5 opintopisteen laajuinen (kukin opintopiste vastaa 25-30 tunnin työmäärää), ja se alkaa johdannolla, jonka jälkeen se jaetaan teemoihin, jotka sisältävät alateemoja.

[2] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Moving Forward and Beyond in Education: FLEXIBLE LEARNING PATHWAYS. In KTU leidykla "Technologija" eBooks. 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/

Aihealueiden lopussa annetaan useista kysymyksistä koostuva itsearviointitesti. Moduulin koulutusmateriaalin tulisi tukea 6-8 aiheen opiskelua, joista jokaisessa on 4-6 alateemaa. Kurssin voi päättää tietämystestiin, joka ei ole pakollinen. Tämä antaa pk-yritysten työntekijöille ja oppilaitosten opiskelijoille mahdollisuuden hankkia ja osoittaa tietyssä moduulissa tai koulutuksen osassa opitut taidot.



Kuva 3. Tutkimusten rakenne

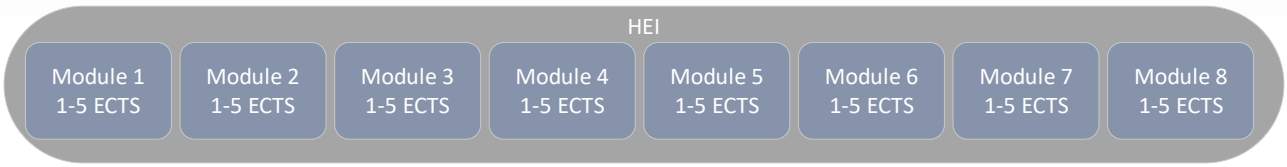
Mikrotodistukset integroidaan oppimisprosessiin seuraavien keskeisten toimien avulla:

- Koulutusmoduulien kehittäminen: Kukin moduuli on laadittava huolellisesti ottaen huomioon pk-yrityssektorilla vaadittavat erityistiedot ja -taidot, ja siinä on määriteltävä selkeät tavoitteet, oppimistulokset, opetus- ja oppimismenetelmät sekä kurssin kesto.
- Käytännön tehtävät ja projektit: oppijat suorittavat käytännön tehtäviä ja kehittävät projekteja, jotka arvioidaan ja jotka antavat selkeää näyttöä hankituista taidoista.
- Selkeästi kuvattu osaamisen arviointistrategia ja arviointikriteerit: Kunkin moduulin lopussa järjestetään osaamisen arviointi, jossa määritetään, onko osallistuja saavuttanut vaaditut oppimistulokset ja voiko hän saada todistuksen siitä.

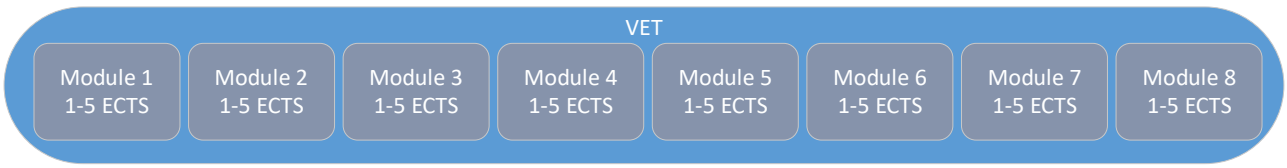
Koska hankkeen kohderyhmänä ovat pk-yritysten työntekijät, korkeakouluopiskelijat ja ammatillisen koulutuksen opiskelijat, tarjolla on neljää erilaista opiskelumuotoa oppijoiden mahdollisuuksien ja tarpeiden mukaan:

- Korkeakoulujen tutkimukset: Kahdeksan moduulia, kukin 1-5 opintopistettä, joissa on kontaktitunteja (teoriaa ja käytäntöä) ja yksilöllisiä työtunteja;
- Ammatillisen koulutuksen opinnot: Kahdeksan moduulia, kukin 1-5 ECTS, joissa on kontaktitunteja (teoriaa ja käytäntöä) ja yksilöllisiä työtunteja;
- Itseopiskelu (pk-yrityksille): 8 moduulia, kukin 1-5 opintopistettä, joissa on konsultaatioita (tarvittaessa) ja yksilöllisiä työtunteja;

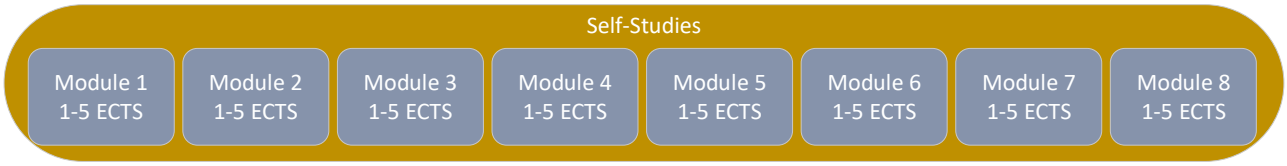
- Mikromoduulit: yksilöllinen työtunti riippuen valittujen aiheiden määrästä.



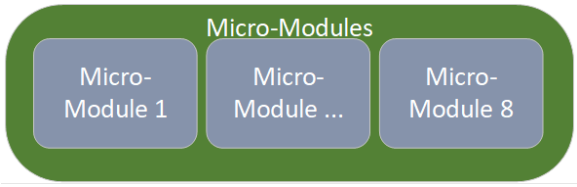
Kuva 4. Korkeakoulun opintorakenne



Kuva 5. Ammatillisen koulutuksen opintojen rakenne

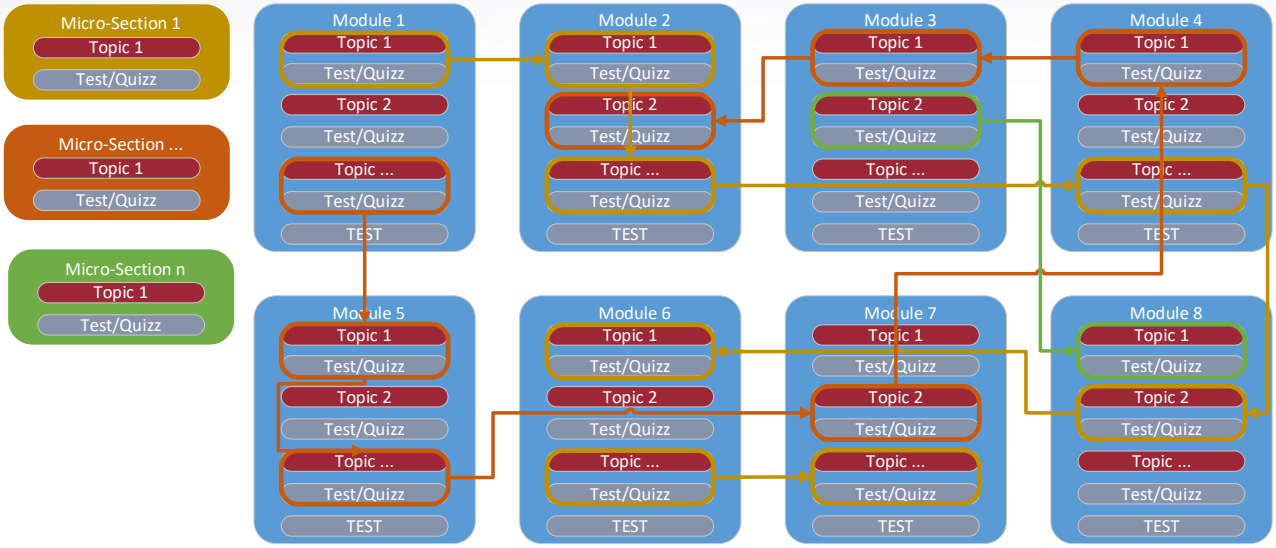


Kuva 6. Opintojen rakenne itseopiskelua varten



Kuva 7. Mikromoduulin tutkimusrakenne

Korkeakoulu- ja ammatillisen koulutuksen opiskelijat voivat opiskella yhden 1-5 opintopisteen moduulin. Pk-yritykset voivat opiskella yhden moduulin kerrallaan, tai voimme tarjota mikrojaksoja osana kurssia.



Kuva 8. Oppimispolkujen yhteydet

Kaikissa kolmessa oppimistyypissä (korkeakoulu, ammatillinen koulutus, pk-yritykset) opiskelija opiskelee 8 moduulia. Mikromoduuleissa opiskelija valitsee moduulit itse.

Mikromoduulit ovat lyhyitä tai pitkiä avoimesti arvioituja oppimiskokemuksia. Osallistuja voi suorittaa ne yhdessä haasteen kanssa tai erikseen. Kukin mikromoduuli arvostetaan erilaisella oppimistyömäärällä (kuten ECTS), ja se päättyy arviointiin. Mikromoduulien arvioinnin onnistunut suorittaminen palkitsee oppijat mikrotodistuksilla.

Ehdotuksen mukaan kukin HEI-ohjelman moduuli voidaan modulaarisoida yhdeksi mikromoduuliksi, joka sisältää erikoistehtäviä ja yksityiskohtaisen toteutussuunnitelman. Testien tuloksia voidaan arvioida merkkien avulla, jotka ovat kuvapohjaisia ja yleisesti tietokoneiden luettavissa. Näihin kuviin on upotettu metatietoja, joissa esitetään yksityiskohtaisesti kuhunkin merkkiin liittyvät pätevyydet ja tiedot merkin haltijasta.

Mikro-todistus tarkoittaa kirjaa oppimistuloksista, jotka osallistuja on saavuttanut pienen oppimäärän jälkeen. Nämä oppimistulokset on arvioitu läpinäkyvien ja selkeästi määriteltyjen kriteerien perusteella. Mikrotodistuksiin johtavat oppimiskokemukset on suunniteltu siten, että osallistuja saa erityisiä tietoja, taitoja ja pätevyyksiä, jotka vastaavat yhteiskunnallisiin, henkilökohtaisiin, kulttuurisiin tai työmarkkinoiden tarpeisiin[5,6] .

[5] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Moving Forward and Beyond in Education: FLEXIBLE LEARNING PATHWAYS. In KTU leidykla "Technologija" eBooks. https://doi.org/10.5755/e01.9786090218204.

[6] Neuvoston suositus, annettu 16 päivänä kesäkuuta 2022, eurooppalaisesta lähestymistavasta elinikäisen oppimisen ja työllistyvyyden mikrotodistuksiin." Euroopan unionin virallinen lehti, vol. 2022/C, 16. kesäkuuta 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022H0627(02)&from=EN.

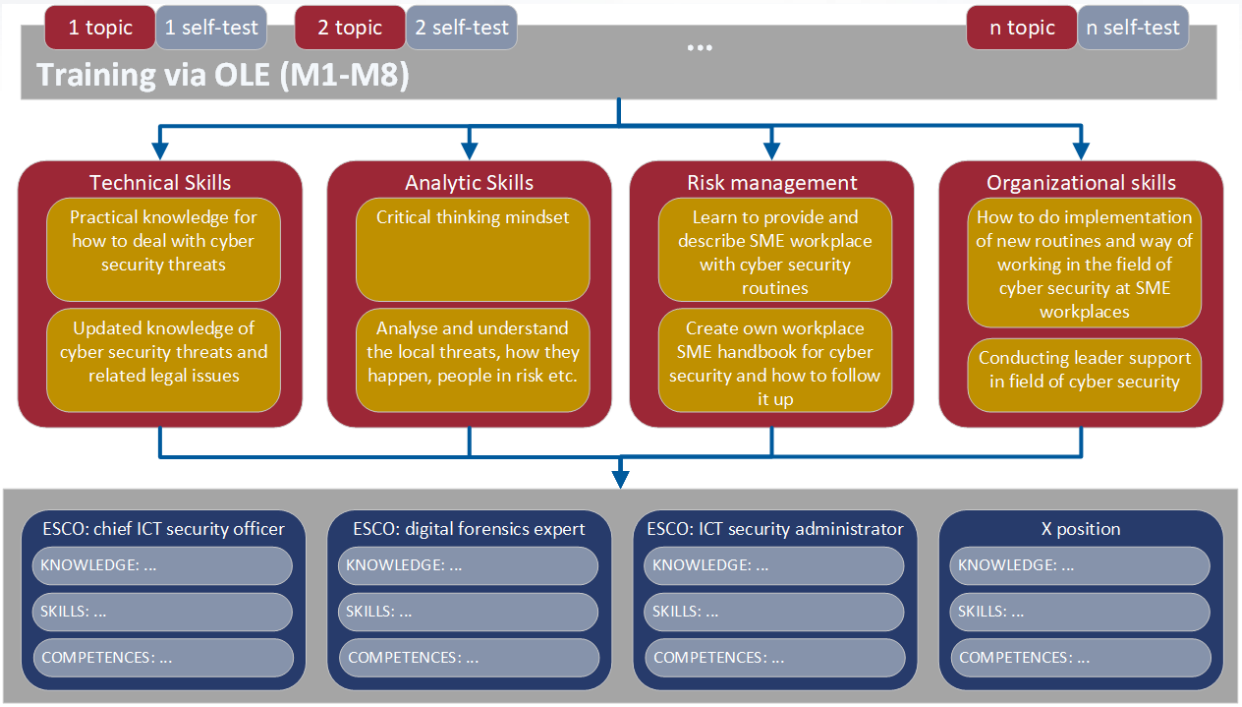
2. URAPOLKU

Oppimisen jälkeistä polkua voitaisiin kutsua urapoluksi. Hankkeen alussa tehtiin tutkimusanalyysi ESCO-ammateista (Kuvattu raportissa: D2.2 - Pk-yritysten kyberturvallisuuden muutosagenttien koulutustarpeiden kartoitusraportti). Kolmessa vaiheessa toteutetun analyysin tavoitteena oli tutkia erilaisia ESCO-kehyksessä lueteltuja kyberturvallisuusammatteja. Ensimmäisessä vaiheessa kyberturvallisuuteen liittyvät ammatit tunnistettiin ja dokumentoitiin **ESCO-portaalista** ja tuotiin esiin niiden taidot, pätevyydet ja tiedot. Näihin ammatteihin kuuluivat esimerkiksi tieto- ja viestintätekniikan turvallisuuspäällikkö, digitaalisen rikostekniikan asiantuntija, sulautettujen järjestelmien tietoturva-insinööri, eettinen hakkeri, tieto- ja viestintätekniikan resilienssipäällikkö, tieto- ja viestintätekniikan tietoturvan ylläpitäjä, tieto- ja viestintätekniikan tietoturva-insinööri, tietoturvapäällikkö ja tietämyssinööri. Kukin ammatti määriteltiin sen erityisvastuiden ja painopistealueiden mukaan kyberturvallisuuden alalla, jotka vaihtelivat yritysten turvallisuustoiminnoista digitaaliseen rikostutkintaan, eettiseen hakkerointiin ja häiriönsietokyvyn suunnitteluun.

Toisessa vaiheessa jokaisesta tarkastellusta ESCO-ammatista täytettiin taulukko, jossa ilmoitettiin yksityiskohtaisesti sen nimike ja keskeiset tehtävät. Näihin kuuluivat muun muassa turvatoimien suunnittelu ja toteuttaminen, haavoittuvuusarviointien tekeminen, häiriönsietokyvyn ja katastrofista toipumisen mallien kehittäminen sekä tiedon integroiminen tietokonejärjestelmiin.

Lisäksi kolmannessa vaiheessa kartoitettiin ESCO-ammatit ja niihin liittyvät oppimistulokset ja luokiteltiin ne tietoihin, taitoihin ja pätevyyksiin. Tämä prosessi helpotti kokonaisvaltaisen ymmärryksen saamista kunkin kyberturvallisuustehtävän koulutusvaatimuksista ja odotettavissa olevista taidoista ja varmisti yhdenmukaisuuden alan standardien ja parhaiden käytäntöjen kanssa. Näiden vaiheiden kautta analyysi tuotti arvokasta tietoa jatkotutkimusta varten.

Kuva 9. Edellisessä raportissa määritellyt ESCO-ammatit



Kuva 10. Mahdolliset oppimisen jälkeiset polut

Kuviossa 10 kuvataan mahdollisia urapolkuja, joita voi kulkea opintojen suorittamisen jälkeen verkko-oppimisympäristön kautta (korkeakoulu, ammatillinen koulutus, pk-yritykset) ja taitojen hankkimisen jälkeen ESCO-ammattien mukaisesti.

Kun tietoverkkoturvallisuutta opiskelevat korkeakouluopiskelijat ja ammatillisen koulutuksen opiskelijat saavat selkeämmän käsityksen uravaihtoehdoista ja voivat valita jatko-opiskelualan tai työskennellä yrityksissä erityisissä tehtävissä, kun taas tietotekniikan ja muiden alojen opiskelijat voivat valita CyberAgent-moduuleja yksilöllisiksi opintokokonaisuuksiksi ja parantaa näin opiskelualansa osaamista, kuten organisaatio- ja riskinhallintataitoja jne.

Pk-yritysten henkilöstöllä on mahdollisuus päivittää ja kehittää työelämävalmiuksiaan. Kehitetyn urapolun ja selkeiden uramahdollisuuksien perusteella pk-yritysten muu henkilöstö voi kouluttautua uudelleen kyberturvallisuuden alalla.

Sekä opiskelijoiden että pk-yritysten henkilöstön osallistumista on tarkoitus lisätä ottamalla mukaan mentorointijärjestelmiä, järjestämällä tiedotustapahtumia, työpajoja (hankkeeseen kuuluu kuusi kaikkien kumppaneiden järjestämää yhteistä työpajaa sekä kunkin kumppanin järjestämiä tiedotuskampanjoita), kutsumalla yritysten ja kyberturvallisuuden edustajia, tekemällä yhteistyötä työmarkkinaosapuolten ja CyberAgent-verkoston kanssa, tarjoamalla harjoittelupaikkoja opiskelijoille jne. Lisäksi monimuotoisuutta koskevilla aloitteillamme, kuten kohdennetuilla tiedotus- ja tukiohjelmilla, pyritään lisäämään naisten osallistumista ja edistämään osallistavaa kyberturvallisuustyövoimaa.

Kun ESCO-ammatteja kartoitetaan kattavasti CyberAgent-koulutusmoduuleihimme, osallistujat voivat siirtyä saumattomasti oppimisympäristöistä vaikuttaviin tehtäviin kyberturvallisuuden alalla. CyberAgent-koulutettavien urakehityksen seuraamiseksi on tarkoitus järjestää ennen

koulutusta, koulutuksen jälkeen ja kolmen kuukauden kuluttua koulutuksen päättymisestä kyselytutkimuksia, joilla selvitetään, miten heidän taitonsa edistävät heidän työpaikkojensa kyberturvallisuutta. Kyselyt integroidaan koulutusalustaan, ja ne tarjotaan automaattisesti koulutettaville ennen kurssin alkua ja kurssin lopussa, jotta voidaan mitata edistymistä ja arvioida kurssia ja koulutuksen laatua. Kolmannen kyselyn avulla selvitetään, onko osallistujien urakehityksessä tapahtunut muutoksia.

3. OPETUSMENETELMÄT

Vilnan yliopiston (VU) tietojärjestelmien ja kyberturvallisuuden koulutusohjelman, Timtalin ja Moisil Buzaun koulutusohjelmien pedagogisten menetelmien ja ulkopuolisen kirjallisuuden analyysin perusteella voimme suositella useita innovatiivisia opetusmenetelmien yhdistelmiä. Nämä yhdistelmät voitaisiin sisällyttää opintokokonaisuuksiin ottaen huomioon kunkin moduulin rakenne.[7]

Taulukko 1. Suositellut opetusmenetelmät

Luokka	Yksityiskohtaiset tiedot
Luento ja suora opetus	- **Teoreettiset luennot:** peruskäsitteet ja teoriat. - **Vierailevat puhujat** ((sertifioidut asiantuntijat: 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 (GIAC Certified Incident Handler (GCIH), Offensive Security Certified Professional (OSCP)).

Käytännönläheinen ja käytännönläheinen oppiminen	- **Käytännön tehtävät/laboratoriot:** käytännön kokeet ja käytännön harjoitukset.
	- **Käytännön toimet**: reaalimaailman sovellukset ja vuorovaikutteiset tehtävät.
	- **Tekninen videoanalyysi:** videosisällön analysointi teknisten taitojen oppimista varten.
	- **Simuloidut ympäristöt**:
	  o Pilviympäristön isännöidyt koneet.
	  o Käynnistää hyökkäyksiä kohdekoneeseen.
	  o Kone hyökkäysten suunnittelua ja toteuttamista varten - hyökkäyslaatikko.

Arviointi ja evaluointi	- **Tietokilpailut, pelit, säännöt ja kiellot**: Osallistavat ja vuorovaikutteiset arvioinnit.

[7] Kyberturvallisuuden opettaminen: A Project-Based Learning and Guided Inquiry Collaborative Learning Approach https://scholar.utc.edu/cgi/viewcontent.cgi?article=1945&context=theses https://scholar.utc.edu/cgi/viewcontent.cgi?article=1945&context=theses

Luokka	Yksityiskohtaiset tiedot
	- **Itsearviointitestit**: Oppijan itsearviointia varten aiheiden lopussa.
Itseopiskelu	- **Itseohjautuva oppiminen:** Tämä menetelmä tukee yksilöllisiä oppimispolkuja, ja sitä voidaan täydentää digitaalisilla resursseilla ja modulaarisella sisällöllä, jota oppilaat voivat käyttää tarpeen mukaan.
Yhteisöllinen ja vertaisoppiminen	- **Yhteistoiminnallinen oppiminen, ryhmätyöskentely**: ryhmäprojektit ja yhteistehtävät. - **Vertaisopetus ja -oppiminen**: oppijat opettavat toisiaan ja oppivat toisiltaan. - **Ryhmämentorointi ja/tai yksilömentorointi**: kokeneempien henkilöiden antama ohjaus.
Teknologiaa hyödyntävä oppiminen	- **Pelillistetyn kyberturvallisuuden oppimisalustan käyttö**: oppijoiden sitouttaminen pelillisten elementtien avulla oppimisalustoissa. - **Capture the flag -kilpailut**: kilpailutapahtumat kyberturvallisuustaitojen parantamiseksi. - **Kilpailut**: Kilpailuissa testataan opiskelijoiden taitoja ja tietoja käytännönläheisessä, soveltavassa ympäristössä ja mitataan heidän osaamistaan kilpailumuodossa.
Yhteisön ja yleisön osallistuminen	- **Koulutustapahtumat:** erityistapahtumat esimerkiksi kyberturvallisuuskuukauden aikana. - **Julkiset esitykset**: seminaarit, konferenssit ja webinaarit. - **Sosiaalinen verkostoituminen**: sosiaalisen median ja verkostojen käyttö oppimisessa ja sitoutumisessa. - **Päiväkampus**: tyypillisesti kampuksella järjestettävät tapahtumat, joihin voi sisältyä työpajoja, luentoja ja verkostoitumismahdollisuuksia.

Luokka	Yksityiskohtaiset tiedot
Innovatiiviset oppimismallit	- **BSCS:n 5E-opetusmalli (5E)** - 5E-mallissa keskitytään seuraaviin vaiheisiin, jotka koostuvat seuraavista: Engagement, Exploration, Explanation, Elaboration, Evaluation. - **Challenge-Based Learning Model (CBL)** - CBL:n varhainen toteutus tarjoaa kuudesta vaiheesta koostuvan kehyksen: Haasteen kuvaaminen, ideoiden tuottaminen ja ideoiden ideointi, useiden eri näkökulmien tarkastelu, jotka kyseenalaistavat ja tukevat, parhaiden ratkaisujen tutkiminen ja tarkistaminen, hypoteesin testaaminen, havaintojen ja johtopäätösten jakaminen. - **Yhteistoiminnallisen oppimisen malli (CL)** - 5E- ja CBL-mallien tavoin yhteistoiminnallisessa oppimisessa edistetään aktiivista oppimista pienryhmissä, ja oppilaat saavat suoritukseensa perustuvan palkkion, joka voi olla arvosana, konkreettinen palkinto, kuten todistus tai stipendi, tai opettajan hyväksyntä. - **Projektipohjainen oppimismalli (PBL)** - projektipohjaisessa oppimisessa ja ongelmalähtöisessä oppimisessa käytetään samaa lyhennettä PBL, ja molemmissa keskitytään ongelmanratkaisun, kriittisen ajattelun, tiimityön, viestinnän ja luovien taitojen parantamiseen; ne koostuvat kuitenkin eri vaiheista., Itsenäinen ja ryhmätutkimus, Kehittäminen ja esittäminen, Analysoi ja arvioi prosessi. - **Prosessisuuntautunut ohjattu tutkivan oppimisen malli (POGIL)** - tämä lähestymistapa ohjaa oppilaita käsitteen tutkimisen kautta, jonka jälkeen oppilaat keksivät käsitteen, jossa he syntetisoivat ja selittävät käsitteen, ja oppimissykli päättyy teoreettisen käsitteen soveltamiseen. - **Guided Inquiry Collaborative Learning Model (GICL)** - tämä on uusi lähestymistapa, joka perustuu pitkälti POGIL-malliin.

Jotta varmistetaan, että tarjotuilla eri koulutusstrategioilla on paras mahdollinen vaikutus, kukin lähestymistapa valitaan ja sovitetaan yhteen kyberturvallisuusmoduulien erityisten oppimistavoitteiden kanssa, kun kehitetään kattava moduulin opetussuunnitelma ja koulutusmateriaali. CyberAgent-koulutusta antavat luennoitsijat/mentorit voivat myös valita muita menetelmiä. Koulutusmateriaalien kehittämisvaiheessa pilottikoulutusten kouluttajille annetaan koulutusta, jossa heille kerrotaan koulutuksen tavoitteista, prosessista ja vastuista sekä valmistellaan heitä opettamaan tehokkaasti CyberAgent-opetussuunnitelmaa. Pilottikoulutusprosessiin kuuluu myös palautteen kerääminen oppijoilta ja kouluttajilta, jotta voidaan seurata käytettyjen koulutusmenetelmien tehokkuutta ja tehdä tarvittaessa muutoksia.

Moduulit järjestetään eri opetusmuodoissa:

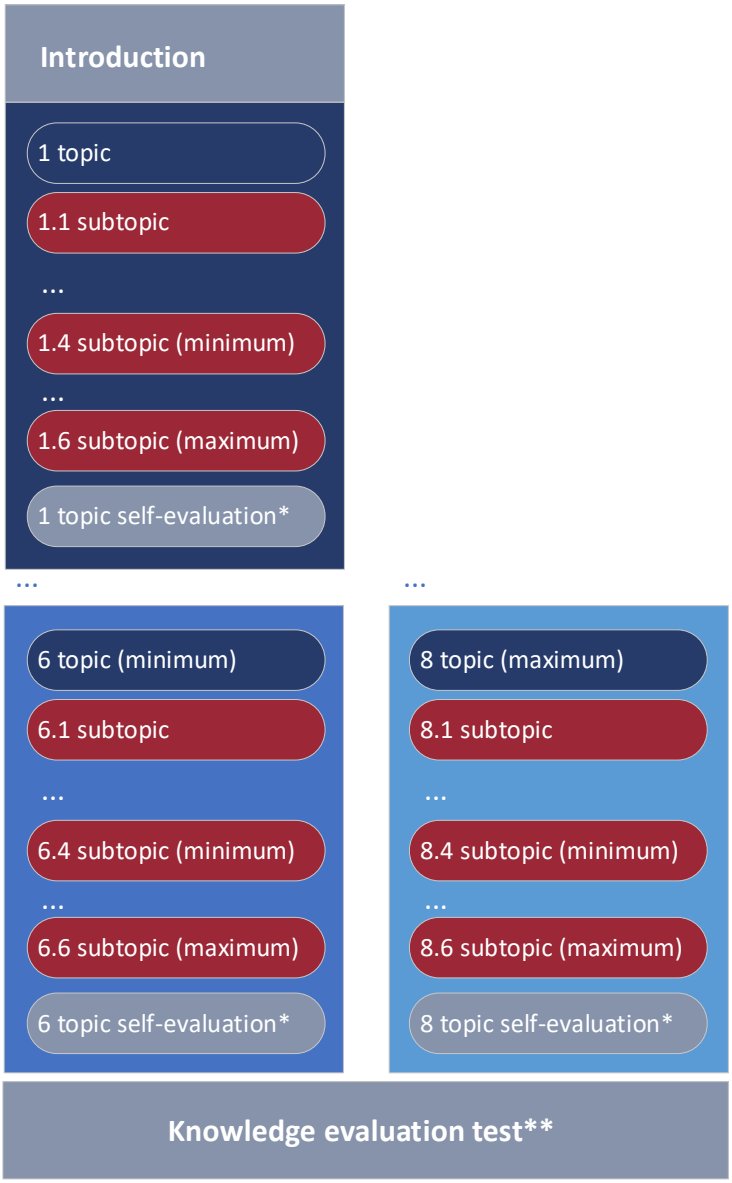
- **etämuodossa**,
- **synkronisessa oppimisessa** (opettajan täysi tuki),
- sekä **asynkronisessa oppimisessa** (opettajan tuki tarvittaessa), sekamuotoisessa oppimisessa ja itseopiskelussa.

Koska koulutuksen toteuttamiseen on suunniteltu erilaisia tapoja, koulutusmenetelmät esitetään tässä vaiheessa ohjeellisina.

4. MODUULIN RAKENNE

VU:n kyberturvallisuuden koulutusohjelman moduulirakenteen analyysin, kansainvälisten hankkeiden (**CyberPhish**, **FuseIT**, **dComFra**) moduulirakenteen analyysin ja kaupallisten alustojen, kuten **Udemyn** ja **Courseran**, moduulirakenteen analyysin perusteella on luotu tyypillinen moduulirakenne, jota voidaan soveltaa sekä korkeakoulujen että ammatillisen koulutuksen moduuleihin.

Päätavoitteena on kehittää 8 moduulia, joista 8 moduulia olisi tarkoitettu korkeakouluopiskelijoille (EQF-taso 5 - 5 -- 6), ammatillisen koulutuksen opiskelijoille ja pk-yrityksille (EQF-taso 4-5) sekä mikromoduuleja kaikenlaisille opiskelijoille.



Kuva 11. Moduulin rakenne

* On suositeltavaa, että jokaisen alateeman jälkeen on kysymyksiä itsetestaukseen (itsereflektioon). Moduulin kehittämisvaiheessa voidaan kuitenkin valita erilainen arviointimenetelmä tai -vaihtoehto valitun opiskelutyypin mukaan, esim. opiskelijoille voidaan antaa käytännön harjoituksia, simulaatioita jne., kun taas itsenäisille oppijoille tarjotaan itsetestiä koskevia kysymyksiä.

** Tietojen arviointitesti on vapaaehtoinen. Jos oppija haluaa saada todistuksen kurssin suorittamisesta hankkimiensa tietojen todentamiseksi, tämä testi on pakollinen. Oppija voi kuitenkin halutessaan hankkia kurssin päättötodistuksen todistaakseen, että hän on osallistunut koulutukseen, jolloin tämä testi on vapaaehtoinen.

Jotta varmistetaan, että kukin koulutusmoduuli liittyy suoraan käytännön sovellettavuuteen, kunkin moduulin kuvauksessa annetaan selkeitä esimerkkejä siitä, miten teoriaa sovelletaan käytännössä. Tämä sisältää paitsi yksityiskohtaisia skenaarioita moduulien sovellettavuudesta, myös erityisiä tehtäviä, joita opiskelijat suorittavat teoreettisen tietämyksen vakiinnuttamiseksi todellisissa kyberturvallisuustilanteissa.

Kunkin moduulin olisi tarjottava teknisiä taitoja, analyyttisiä taitoja, riskinhallintataitoja ja organisatorisia taitoja eri osuuksin. Itsearviointitesti testaa oppijoiden tietämystä minkä tahansa moduulin (aiheen) osan lopussa. Tämä mahdollistaa paitsi hankitun osaamisen arvioinnin myös sen, että oppijan edistyminen kirjataan ja osallistuja kerää pisteitä ja merkkejä, jolloin hän voi osallistua enemmän oppimisprosessiin.

ECTS-muodollisuuksien noudattaminen, jossa kukin ECTS on 25-30 tunnin työmäärä. Tämän mukaan kukin moduuli voi vastata 5 ECTS:ää. Työmäärä voitaisiin jakaa näin:

Taulukko 2. Työmäärän tunnit

	Moduulien lukumäärä	**ECTS yhteensä**	**Etätunnit teoreettisia taitoja varten**	**Etätunnit käytännön taitoja varten**	**Yksilöllinen työaika**	**Työmäärän kokonaistunnit**
Moduulit korkeakouluopiskelijoille (EQF-taso 5-6)	8	8-40	20%	20%	60%	200-1200
Moduulit ammatillisen koulutuksen opiskelijoille (EQF-taso 4-5)	8	8-40	15%	25%	60%	200-1200
Itseopiskelu (yhdistelmäopiskelu)	8	8-40	10%		90%	200-1080
Itsetutkimukset (verkossa)	8	8-40				200-1200
Mikromoduulit	1-8	1-40				25-1200

Taulukko 3. Suositellut moduulit työmäärä

Moduuli	**ECTS**	**Yhteensä tuntia**	**Yhteystunnit**	**Kontaktitunnit (teoria)**	**Kontaktitunnit (harjoittelu)**	**Yksilöllinen työaika**
HEI Moduulin nimi	1-5	25-150	40%	20%	20%	60%
VET Moduulin nimi	1-5	25-150	40%	15%	25%	60%
Itseopiskelu (yhdistelmäopiskelu)	1-5	25-150	10%			90%
Itsetutkimukset (verkossa)	1-5	25-150				100%
Mikroleikkaukset						10%-100%

Jokaisella moduulilla on oltava oma kuvauksensa. VU:n, Timtalin ja muiden mikrotodistuksia käyttävien ohjelmien analyysin perusteella ehdotetaan kullekin CyberAgent-moduulille tyypillistä moduulirakennetta (esimerkki tyypillisestä moduulirakenteesta on esitetty liitteessä 1).

Taulukko 4. CyberAgent-moduulien tyypillinen rakenne

Luokka	Yksityiskohtaiset tiedot
Moduulin tunniste (perustiedot moduulista)	- Moduulin nimi - Moduulin koodi - Lehtori - Oppilaitos tai laitos, jossa moduuli suoritetaan - Toimitusmalli - Kieli - Edellytykset
Moduulin kesto ja työmäärä (selkeästi ajallinen sitoutuminen ja rakenne)	- Kokonaiskesto (ECTS) - Opiskelijoiden työmäärä tunteina - Yhteystiedot työaika - Yksilöllinen työaika

Koulutustavoitteet ja oppimistulokset (yksityiskohtaiset tiedot siitä, mitä moduulilla pyritään saavuttamaan ja mitä opiskelijat oppivat).	- Moduulin tarkoitus ja tulokset
	- Oppimistulokset
	  o Tekniset taidot
	  o Analyyttiset taidot
	  o Riskitaidot
	  o Organisaatiotaidot

Opetus- ja oppimismenetelmät	- Opetus- ja oppimismenetelmät
Arviointi ja arviointi (selvitys siitä, miten oppilaita arvioidaan).	- Arviointimenetelmät - Tehtävät (laboratoriot, projektit, esitykset, raportit jne.). - Arviointistrategia, arviointiperusteet
Helpottaa resursseja	- Laitteet, ohjelmistot ja teknologia
Kurssin sisältö	- Moduulin aiheet ja alateemat
Resurssit	- Lähdeluettelo - Lisälähteet

Jokainen opintopiste lasketaan 25-30 tunniksi (kontakti- tai verkkotunteja + yksilöllinen opiskelu).

Moduulissa on oltava vähintään kaksitasoinen hierarkia:

- **Hierarkian ensimmäinen taso** - aiheet. Tällä tasolla moduulin pääelementit voivat olla johdanto, pääsykoe, loppukoe ja peruselementti - aihe.
- **Hierarkian toinen taso** - alateemat, moduulin tärkeimmät opetuselementit.

Jokaisen hierarkian ensimmäisen tason moduulin tulisi sisältää:

- **JOHDANTO** moduuliin (tekstimuotoinen kuvaus, videoesittely): moduulin merkitys ja hyödyt, moduulin perustavoitteet ja tulokset, tarvittavat ohjelmistot ja laitteistot, osallistujille asetettavat vaatimukset.
- **TEEMAT** - kurssin pääaiheet, teoreettinen materiaali ja teoreettiset opetusmenetelmät.
- **SUBTOPIC** - kunkin aiheen alateema, käytännön, analyyttinen analyysi ja tehtävät, käytännön ja analyyttiset opetusmenetelmät. Aiheet ja alateemat voivat sisältää tekstimuotoista tietoa, videoita, äänileikkeitä, esityksiä, linkkejä lisälukemistoon.
- **MODUULIN johdantotesti** (tarvittaessa). Keskitason ja edistyneen tason johdantokokeessa on vahvistettava, että hakija on omaksunut riittävästi tietoja ja taitoja edellisillä tasoilla.
- **MODUULIN kuittaustestit**. Kuittauskokeella on varmistettava objektiivisesti opiskelijan taidot ja osoitettava hänen pätevyytensä moduulin vaatimuksiin.
- **OHJEET ohjaajille/opettajille**. Tämän asiakirjan olisi sisällettävä mentoreille/opettajille suunnattuja metodologisia suosituksia moduulien opetuselementtien käytöstä.

Jokaisen hierarkian toisen tason TOPICin tulisi sisältää:

- **JOHDANTO** aiheen tavoitteisiin ja tuloksiin, lyhyt sisältö.
- **ALAKOHTA**: kaikki tarvittavat opetukselliset elementit, joilla tuetaan oppilasta hallitsemaan asiaankuuluvat taidot.
- **TEEMATESTI**: lyhyet suositukset ohjaajille/opettajille moduulin toteuttamisesta ja soveltamisesta. Jokaisen SUBTOPICin tulisi koostua opetuksellisista elementeistä, joiden sisältö vastaa moduulin kuvauksen tehtäviä. Jokaiseen alateemaan voi (pitäisi) sisältyä ALATEEMATESTI, jolla vahvistetaan, että opiskelija on omaksunut asiaankuuluvat taidot riittävän korkealla tasolla.

Moduulin koulutusmateriaalin tulisi tukea 6-8 aiheen opiskelua, joista kussakin on 4-6 alateemaa ja vähintään yksi aiheen testi. Moduulin tulisi siis sisältää (noin) 30-40 opetuselementtiä (opetusmenetelmät kuvataan kohdassa opetusmenetelmät) ja 6-8 testiä sekä yksi moduulin loppuarviointitesti.

5. KYBERAGENTIN OPETUSSUUNNITELMA JA KOULUTUSOHJELMA

Opetussuunnitelman rakentamisen etenemissuunnitelma

CyberAgent-opetussuunnitelma ja koulutusohjelma noudattavat ACM:n, IEEE:n, AIS SIGSEC:n ja IFIP:n yhteisen työryhmän (2017)[8] kehittämiä opetussuunnitelmaohjeita (Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity)[9] (jäljempänä '**ohjeet**'). Koska CyberAgent-hankkeessa keskitytään erityisesti eurooppalaisten pk-yritysten sisäisen kyberturvallisuusosaamisen lisäämiseen, opetussuunnitelmassa noudatetaan näiden suuntaviivojen suositusten mukaista Organizational Security -osaamisalueen kehystä.

Ensimmäinen vaihe opetussuunnitelman laatimisessa on kuitenkin kartoittaa CyberAgent-hankkeen ennalta määritellyt alateemat ja moduulit ohjeissa (s. 59-70) suositeltujen ja kuvattujen tietoyksiköiden ja keskeisten aiheiden kanssa. Kartoitus perustuu näiden kahden pilarin väliseen loogiseen korrelaatioon, josta hankekumppanit ovat keskustelleet ja sopineet.

Toisessa vaiheessa edellä kartoitetut tietämysyksiköt ja keskeiset aiheet yhdistetään erityisiin oppimistuloksiin, jotka on yksilöity ja kuvattu kohdassa T2.2 "Pk-yritysten kyberturvallisuuden muutosagenttien koulutustarpeiden kartoittaminen". Tässä yhteydessä on huomattava, että kyberturvallisuuteen liittyvillä eri ammateilla voi olla erilaisia tietoja, taitoja ja osaamista, kuten edellä mainitussa T2.2-toimituksessa on selkokielisesti kartoitettu. Jäljempänä esitetty ehdotus kuvastaa kuitenkin CyberAgentilta odotettuja tietoja, taitoja ja pätevyyksiä, joita voidaan mukauttaa tiettyjen ammattien tai harjoittelijaryhmien erityistarpeisiin.

Opetussuunnitelmien laatimisen tulokset esitetään taulukossa 5 jäljempänä.

[8] Kyberturvallisuuskoulutusta käsittelevä yhteinen työryhmä . (2017). Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity: A Report in the Computing Curricula Series. Association for Computing Machinery, 31. joulukuuta 2017. Saatavissa: **https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf** [Viitattu 3.3.2024].

Taulukko 5. Opetussuunnitelman laatimisen etenemissuunnitelma

Alateemat ja moduulit	Tietoyksikkö ja keskeiset aiheet	Oppimistulokset HEI	Oppimistulokset Ammatillinen koulutus
Tekniset taidot			
- ajantasainen tietämys kyberturvallisuusuhkista ja niihin liittyvistä oikeudellisista kysymyksistä.	**Turvallisuusohjelman hallinta** - Projektinhallinta - Resurssien hallinta - Turvallisuusmittarit - Laadunvarmistus ja laadunvalvonta	**Tieto**: Oppilaat saavat syventävää tietoa kehittyneistä kyberturvallisuusperiaatteista, kuten kehittyneistä kyberuhkista ja hyökkäysvektoreista, kansallisesta ja kansainvälisestä kyberturvallisuuslainsäädännöstä, -standardeista ja vaatimustenmukaisuusvaatimuksista, jotka liittyvät heidän toimialaansa. **Taidot**: Oppilaat osaavat suunnitella ja toteuttaa kehittyneitä riskinarviointi- ja -hallintastrategioita tunnistettujen riskien vähentämiseksi käyttäen kehittyneitä menetelmiä ja työkaluja. **Osaaminen**: Opiskelijoilla on valmiudet johtaa ja hallinnoida kyberturvallisuusprojekteja ja -tiimejä, jotka toteuttavat strategisia kyberturvallisuuskäytäntöjä ja -puitteita, jotka ovat linjassa organisaation tavoitteiden ja	**Tieto**: Oppijat saavat käytännön tietoa uusimmista kyberturvallisuusuhista, kuten tietojenkalastelusta, lunnasohjelmista ja DDoS-hyökkäyksistä, ja siitä, miten niitä hallitaan tehokkaalla projekti- ja resurssienhallinnalla sekä laadunvarmistus- ja valvontatoimenpiteiden toteuttamisella. **Taidot**: Oppilaat osaavat käyttää työkaluja ja ohjelmistoja suojautuakseen kehittyviltä verkkouhilta ja soveltaa vankkoja turvallisuuskäytäntöjä projekti- ja resurssienhallinnassa parantaakseen yleistä turvallisuusmittaristoa ja laadunvalvontaa organisaatiossaan. **Osaaminen**: Oppilaat osaavat arvioida ja lieventää mahdollisia tietoturvauhkia, viestiä tehokkaasti kyberturvallisuuskysymyksistä ja raportoida uhkat ja

		vaatimustenmukaisuusvelvoitteiden kanssa.	tietoturvaloukkaukset tarkasti organisaationsa asianmukaisia kanavia käyttäen.
- Käytännön tietämys siitä, miten kyberturvallisuusuhkiin voi vastata.	**Järjestelmien hallinta** - Käyttöjärjestelmän ylläpito - Tietokantajärjestelmän ylläpito - Verkonhallinta - Pilvipalvelun hallinta - Kyberfyysisten järjestelmien hallinnointi - Järjestelmän kovettuminen - Saatavuus	**Tieto**: Oppilaat saavat kehittynyttä tietämystä käyttö-, tietokanta-, verkko-, pilvi- ja kyberfyysisten järjestelmien hallinnasta sekä muista aloista, minkä ansiosta he voivat tehokkaasti koventaa järjestelmiä ja varmistaa niiden käytettävyyden sekä soveltaa uusimpia kyberturvallisuuden puolustusmekanismeja. **Taidot**: Oppilaat osaavat käyttää kehittyneitä menetelmiä ja työkaluja turvallisten järjestelmäarkkitehtuurien suunnitteluun ja toteuttamiseen, mukaan lukien käyttöjärjestelmät, tietokannat, verkot ja pilvi-infrastruktuurit. **Osaaminen**: Oppilaat osaavat kehittää ja toteuttaa strategisia kyberturvallisuuspuitteita järjestelmänhallintaa varten, johtaa hankkeita ja ryhmiä, joilla parannetaan järjestelmien kovettumista ja käytettävyyttä, ja tehdä eettisiä päätöksiä vankkojen kyberturvallisuuskäytäntöjen ylläpitämiseksi eri hallintoalueilla.	**Tieto**: Opiskelijat saavat käytännön tietoa siitä, miten käyttöjärjestelmiä, tietokantoja, verkkoja, pilvipalveluja ja kyberfyysisiä järjestelmiä voidaan hallinnoida ja suojata yleisiltä kyberuhilta, kuten tietojenkalastelulta, lunnasohjelmilta ja DDoS-hyökkäyksiltä, ja samalla toteuttaa tehokkaita riskinhallintakäytäntöjä. **Taidot**: Oppilaat osaavat tunnistaa mahdolliset kyberturvallisuusriskit ja -haavoittuvuudet eri järjestelmäalustoilla, käyttää erikoistyökaluja ja -ohjelmistoja järjestelmien suojauksen ja käytettävyyden parantamiseksi sekä ottaa käyttöön kyberturvallisuuden peruskäytännöt, kuten turvallisen salasanan luominen, turvallinen selailu ja arkaluonteisten tietojen turvallinen käsittely. **Osaaminen**: Oppilaat osaavat arvioida ja lieventää tietoturvauhkia järjestelmänhallinnassa, tiedottaa tehokkaasti kyberturvallisuuteen liittyvistä asioista ja ilmoittaa viipymättä

			kaikista uhkista ja tietoturvaloukkauksista asianmukaisille organisaatiokanaville.
Analyyttiset taidot			
- Kriittinen ajattelutapa	**Analyyttiset työkalut** - Suorituskyvyn mittaaminen (metriikka) - Data-analytiikka - Turvallisuustiedustelu	**Tieto**: Oppilaat saavat lisätietoa kansallisesta ja kansainvälisestä kyberturvallisuuslainsäädännöstä, standardeista ja vaatimustenmukaisuusvaatimuksista sekä muista oman toimialansa kannalta merkityksellisistä vaatimuksista. **Taidot**: Osaamistavoitteet: Oppilaat osaavat käyttää suorituskyvyn mittauksia, data-analytiikkaa ja tietoturvatietoja tehokkaiden riskinhallintastrategioiden suunnitteluun ja toteuttamiseen. **Osaaminen**: Oppilaat osaavat käyttää analyyttisiä työkaluja strategisten kyberturvallisuuspolitiikkojen kehittämiseksi kriittisesti ajatellen ja tehdä päätöksiä kyberturvallisuuskäytännöistä organisaation tavoitteiden ja	**Tieto**: Opiskelijat saavat käytännön tietoa siitä, miten suorituskykymittauksia, data-analytiikkaa ja tietoturvatietoja voidaan soveltaa organisaation omaisuuden suojaamiseksi. **Taidot**: Oppilaat osaavat käyttää analyyttisiä työkaluja mahdollisten kyberturvallisuusriskien ja haavoittuvuuksien tunnistamiseen, soveltaa tietoon perustuvia oivalluksia kyberturvallisuuskäytäntöjen vahvistamiseen ja hyödyntää suorituskykymittareita salasanojen, selaamisen, sähköpostin ja tietojenkäsittelyn turvallisuuden arvioimiseksi ja parantamiseksi. **Osaaminen**: Oppilaat osaavat arvioida ja lieventää mahdollisia tietoturvauhkia analyyttisten työkalujen avulla ja

		vaatimustenmukaisuusvelvoitteiden mukaisesti.	raportoida uhkat ja tietoturvaloukkaukset täsmällisesti organisaationsa asianmukaisille kanaville.
- Analysoidaan ja ymmärretään paikallisia uhkia, niiden syntytapoja, vaarassa olevia ihmisiä jne.	**Turvallisuusoperaatiot** - Turvallisuuden lähentyminen - Maailmanlaajuiset turvallisuusoperaatiokeskukset (GSOC)	**Tieto**: Opiskelijat saavat lisätietoa paikallisista kyberuhkista käyttämällä maailmanlaajuisten turvallisuusoperaatiokeskusten näkemyksiä ja kyberturvallisuuspuolustusstrategioiden nykytrendejä. **Taidot**: Oppilaat osaavat käyttää kehittyneitä menetelmiä ja työkaluja globaaleissa turvallisuusoperaatiokeskuksissa tehokkaiden riskinhallintastrategioiden suunnittelemiseksi ja suunnitelmien kehittämiseksi paikallisten kyberturvallisuusuhkien tehokkaaksi lieventämiseksi. **Osaaminen**: Oppilaat osaavat kehittää ja panna täytäntöön strategisia kyberturvallisuuspolitiikkoja, joilla vastataan paikallisiin uhkiin käyttämällä maailmanlaajuisia turvallisuusoperaatiokeskuksia.	**Tieto**: Oppilaat saavat käytännön tietoa paikallisista kyberuhkista ja niiden alkuperästä sekä arvioivat, miten nämä uhat vaikuttavat organisaation omaisuuteen. **Taidot**: Oppilaat osaavat tunnistaa paikalliset kyberturvallisuusriskit ja -haavoittuvuudet ja käyttää omiin ympäristöihinsä räätälöityjä työkaluja ja ohjelmistoja, kuten turvallisen salasanan luomista, turvallista selaamista ja turvallista tietojenkäsittelyä. **Osaaminen**: Oppilaat osaavat arvioida ja lieventää paikallisia tietoturvauhkia käyttämällä maailmanlaajuisten tietoturvaoperaatiokeskusten tietoja, tiedottaa tehokkaasti kyberturvallisuusongelmista ja raportoida tarkasti uhkista ja tietoturvaloukkauksista organisaationsa asianmukaisille kanaville.
Riskienhallinta			

- Opi tarjoamaan ja kuvaamaan pk-yritysten työpaikoilla kyberturvallisuusrutiinit.	**Riskienhallinta** - Riskien tunnistaminen - Riskien arviointi ja analysointi - Sisäpiirin uhat - Riskien mittaus- ja arviointimallit ja -menetelmät - Riskien valvonta	**Tieto**: Oppilaat saavat syventävää tietoa riskinhallintaprosesseista, mukaan lukien riskien tunnistaminen, arviointi ja valvonta, jotta he voivat luoda ja kuvata tehokkaita kyberturvallisuusrutiineja, jotka on räätälöity pk-yritysten työpaikkojen erityistarpeisiin kansallisten ja kansainvälisten standardien mukaisesti. **Taidot**: Oppilaat osaavat soveltaa kehittyneitä menetelmiä ja työkaluja kattavien riskinarviointien tekemiseen, tehokkaiden riskinhallintastrategioiden suunnitteluun ja toteuttamiseen sekä erityisesti pk-yritysten työpaikoille räätälöityjen vankkojen kyberturvallisuusrutiinien kehittämiseen. **Osaaminen**: Oppilaat osaavat kehittää ja toteuttaa strategisia kyberturvallisuuspolitiikkoja pk-yritysten työpaikoilla.	**Tieto**: Oppilaat saavat käytännön tietoa riskien tunnistamisen, arvioinnin ja hallinnan prosesseista sekä riskinhallintastrategioista, joiden avulla pk-yritysten työpaikat voidaan suojata tehokkaasti. **Taidot**: Oppilaat osaavat tunnistaa ja analysoida mahdollisia kyberturvallisuusriskejä pk-yritysten ympäristöissä, käyttää asianmukaisia työkaluja ja ohjelmistoja uhkien vähentämiseksi sekä edistää ja toteuttaa keskeisiä kyberturvallisuuskäytäntöjä, kuten turvallisten salasanojen luomista, turvallista selaamista ja arkaluonteisten tietojen turvallista käsittelyä. **Osaaminen**: Oppilaat osaavat arvioida ja lieventää tietoturvauhkia pk-yritysten työpaikoilla, viestiä tehokkaasti kyberturvallisuuteen liittyvistä asioista ja menettelyistä sekä raportoida tarkasti asiaankuuluvista uhkista ja tietoturvaloukkauksista asianmukaisille organisaatiokanaville.
- Luo oma työpaikan pk-yritysten käsikirja	**Liiketoiminnan jatkuvuus, katastrofista toipuminen ja**	**Tieto**: Oppilaat saavat lisätietoa siitä, miten luodaan ja pannaan täytäntöön kattava pk-yrityksen työpaikan kyberturvallisuuskäsikirja, joka sisältää	**Tieto**: Opiskelijat saavat käytännön tietoa siitä, miten luoda kattava pk-yritysten työpaikan kyberturvallisuuskäsikirja, joka sisältää

kyberturvallisuudesta ja sen seurannasta.	**häiriötilanteiden hallinta ja henkilöstöturvallisuus** - Tapahtumiin reagoiminen - Katastrofien jälkeinen toipuminen - Liiketoiminnan jatkuvuus - Tietoturvatietoisuus, koulutus ja koulutus - Turvallisuusalan palkkauskäytännöt - Turvallisuuden päättämiskäytännöt - Kolmannen osapuolen turvallisuus - Arviointiprosessien turvallisuus - Työntekijöiden henkilötietojen yksityisyyden suojaa koskeva erityiskysymys	kehittyneet kyberturvallisuusperiaatteet, uusimmat puolustusmekanismit sekä kansallisen ja kansainvälisen lainsäädännön ja standardien noudattamisen vaaratilanteiden hallinnan, liiketoiminnan jatkuvuuden ja henkilöstöturvallisuuden alalla. **Taidot**: Oppilaat osaavat luoda ja ylläpitää pk-yrityksen työpaikan kyberturvallisuuskäsikirjaa käyttäen kehittyneitä menetelmiä riskien arvioimiseksi, tehokkaan riskinhallinnan ja häiriötilanteisiin reagoimisen strategioiden suunnittelemiseksi sekä kattavien, organisaation tarpeisiin räätälöityjen liiketoiminnan jatkuvuussuunnitelmien laatimiseksi. **Osaaminen**: Oppilaat osaavat kehittää ja toteuttaa pk-yrityksille tarkoitetun kyberturvallisuuden käsikirjan, johtaa tehokkaasti tietoturvaprojekteja ja -tiimejä ja varmistaa, että ne ovat linjassa organisaation tavoitteiden ja vaatimustenmukaisuusvelvoitteiden kanssa.	strategioita häiriötilanteisiin reagoimiseksi, katastrofista toipumiseksi, liiketoiminnan jatkuvuuden varmistamiseksi ja henkilöstön turvallisuuden varmistamiseksi sekä organisaation omaisuuden ja arkaluonteisten tietojen suojaamiseksi. **Taidot**: Oppilaat osaavat tunnistaa mahdolliset kyberturvallisuusriskit, käyttää työkaluja ja ohjelmistoja uhkilta suojautumiseen ja soveltaa parhaita kyberturvallisuuskäytäntöjä kehittääkseen ja ylläpitääkseen pk-yrityksen käsikirjaa, jossa käsitellään turvallista salasanan luomista, selaamista, sähköpostin turvallisuutta ja tietosuojaa. **Osaaminen**: Oppilaat osaavat arvioida ja lieventää tietoturvauhkia, tiedottaa tehokkaasti kyberturvallisuuspolitiikoista ja -käytännöistä sekä raportoida järjestelmällisesti tietoturvatapahtumista pk-yrityksessään, kuten heidän räätälöidyssä kyberturvallisuuden käsikirjassaan esitetään.
Organisointitaidot			

- Miten pk-yritysten työpaikoilla voidaan ottaa käyttöön uusia rutiineja ja työskentelytapoja kyberturvallisuuden alalla?	**Turvallisuushallinto ja -politiikka** - Organisaatiokonteksti - Yksityisyys - Lait, etiikka ja sääntöjen noudattaminen - Turvallisuushallinto - Johto- ja hallitustason viestintä - Johdon politiikka	**Tieto**: Oppilaat saavat lisätietoa siitä, miten pk-yritysten työpaikoilla voidaan ottaa käyttöön uusia kyberturvallisuusrutiineja ja -työnkulkuja, joissa otetaan huomioon nykyiset kyberturvallisuusperiaatteet ja -suuntaukset sekä oman toimialan kannalta merkityksellisen kansallisen ja kansainvälisen lainsäädännön noudattaminen. **Taidot**: Oppilaat osaavat käyttää kehittyneitä menetelmiä riskinarviointien tekemiseen, uusien tietoverkkoturvarutiinien suunnitteluun ja toteuttamiseen sekä vastestrategioiden laatimiseen varmistaakseen tehokkaan hallinnon ja vaatimustenmukaisuuden pk-yritysten työpaikoilla. **Osaaminen**: Oppijat osaavat kehittää ja toteuttaa strategisia kyberturvallisuuspolitiikkoja, johtaa aloitteita uusien rutiinien ja työnkulkujen luomiseksi pk-yritysten työpaikoilla ja tehdä eettisiä päätöksiä, jotka ovat linjassa organisaation tavoitteiden ja vaatimustenmukaisuusvaatimusten kanssa.	**Tieto**: Oppilaat saavat käytännön tietoa siitä, miten uusia kyberturvallisuusrutiineja ja -käytäntöjä voidaan integroida pk-yritysten työpaikoille tietoturvalainsäädännön, standardien, strategioiden ja toimintatapojen mukaisesti tietoturvan, riskienhallinnan ja tietosuojan osalta. **Taidot**: Oppilaat osaavat soveltaa kyberturvallisuustyökaluja ja -ohjelmistoja uusien tietoturvarutiinien toteuttamiseksi, riskien tunnistamiseksi ja lieventämiseksi sekä keskeisten kyberturvallisuuskäytäntöjen, kuten turvallisten salasanojen luomisen, selaamisen ja tietojenkäsittelyn, edistämiseksi pk-yritysten työpaikkojen hallintorakenteissa. **Osaaminen**: Oppilaat osaavat arvioida ja lieventää mahdollisia tietoturvauhkia, viestiä tehokkaasti kyberturvallisuuteen liittyvistä muutoksista ja käytännöistä sekä raportoida tietoturvatapahtumista pk-yrityksissä hallinto- ja vaatimustenmukaisuusvaatimusten mukaisesti.

- Johtajien tukeminen kyberturvallisuuden alalla.	**Kyberturvallisuuden suunnittelu** - Strateginen suunnittelu - Operatiivinen ja taktinen hallinnointi	**Tieto**: Opiskelijat saavat lisätietoa siitä, miten edistyneet kyberturvallisuusperiaatteet ja nykyiset suuntaukset sisällytetään strategiseen suunnitteluun ja operatiiviseen johtamiseen. **Taidot**: Näin he voivat tehokkaasti suunnitella ja toteuttaa kyberturvallisuusstrategioita, joilla vastataan uusiin riskeihin ja varmistetaan vankat taktiset vastatoimet. **Osaaminen**: Oppilaat osaavat kehittää ja panna täytäntöön strategisia kyberturvallisuuspuitteita sekä johtaa ja hallinnoida kyberturvallisuusaloitteita.	**Tieto**: Opiskelijat saavat käytännön tietoa siitä, miten kyberturvallisuuden strateginen suunnittelu ja operatiivinen johtaminen integroidaan organisaation omaisuuden suojaamiseksi, asiaankuuluvan lainsäädännön ja standardien noudattamiseksi sekä tehokkaiden tietoturvastrategioiden ja riskienhallintapolitiikkojen toteuttamiseksi. **Taidot**: Osaamistavoitteet: Oppilaat osaavat tunnistaa kyberturvallisuusriskit, käyttää strategisen suunnittelun ja operatiivisen johtamisen välineitä uhkien torjumiseksi ja edistää perustavanlaatuisten kyberturvallisuuskäytäntöjen käyttöönottoa johtamista tukevissa tehtävissään. **Osaaminen**: Oppilaat osaavat arvioida ja lieventää tietoturvauhkia, viestiä tehokkaasti kyberturvallisuusstrategioista ja -ongelmista sekä raportoida luotettavasti vaaratilanteista ja haavoittuvuuksista organisaationsa asianmukaisille kanaville.

6. KURSSIN ARVIOINTISTRATEGIA

Tiedon arviointi on olennainen osa oppimisprosessia ja edistää syvempää oppimista. Tässä luvussa kuvataan kurssin arviointiin sovellettava lähestymistapa, jota tarvitaan sen varmistamiseksi, että kaikki CyberAgent-kurssien osallistujat saavuttavat vaaditut oppimistulokset ja pätevyydet. Kurssin arviointiprosessi jakautuu kahteen pääosaan: itsearviointiin ja osaamisen arviointikokeisiin, jotka on räätälöity sekä korkeakoulu- että ammatillisen koulutuksen opiskelijoille ottaen huomioon heidän erilaiset tarpeensa ja oppimistavoitteensa.

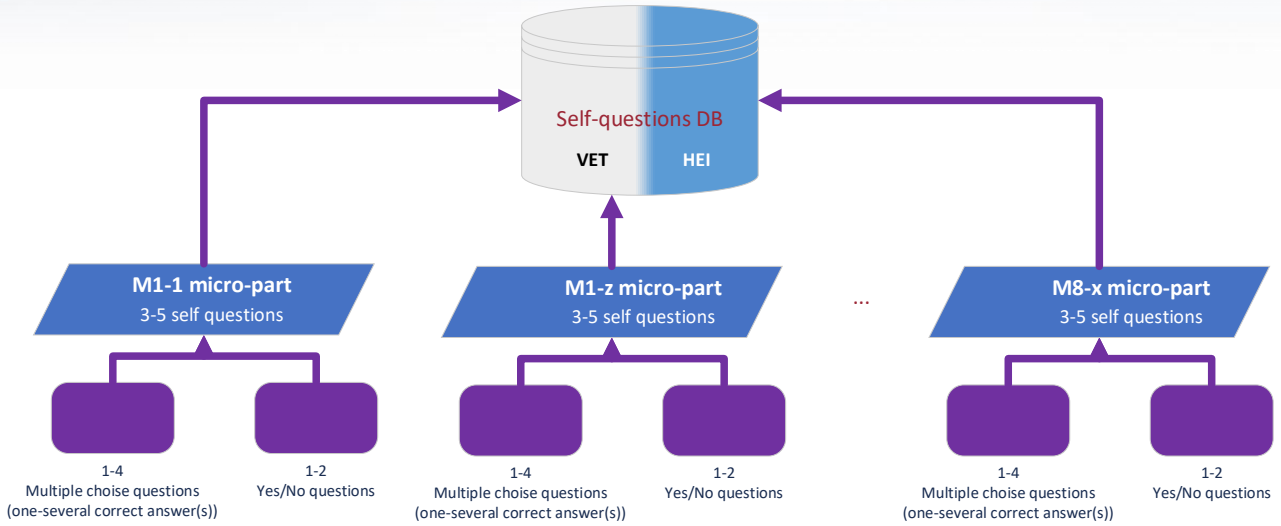
Koska moduulien aiheet voivat olla samat sekä korkeakouluissa että ammatillisessa koulutuksessa, osa kysymyksistä voi soveltua sekä korkeakoulu- että ammatillisen koulutuksen kursseille. Näin ollen kysymyksiä suunniteltaessa on mahdollista täsmentää, onko kysymys tarkoitettu vain ammatilliselle koulutukselle vai vain korkea-asteen oppilaitoksille vai molemmille. Tätä merkintätapaa käytetään vain kysymyksiä suunniteltaessa, koska se helpottaa kysymysten suunnittelua. Kun kysymykset on tuotu alustaan, tietokannat ovat erilaiset ammatillisen koulutuksen ja korkeakoulujen osalta.

Kuva 12. Itsearvioinnin ja osaamisen arvioinnin tietokannat

1. Itsearviointitestit: Kurssin jokaisen aiheen päätyttyä opiskelijat tekevät itsearviointitestejä. Nämä arvioinnit on suunniteltu antamaan välitöntä palautetta, jonka avulla opiskelijat voivat arvioida äskettäin käsitellyn materiaalin ymmärtämistä. Tämä vaihe rohkaisee itsearviointiin ja auttaa vahvistamaan kunkin aiheen oppimistavoitteita. Lisäksi se antaa oppijoille mahdollisuuden tunnistaa alueet, joilla he saattavat tarvita lisäopiskelua tai selvennystä, mikä edistää ennakoivaa lähestymistapaa oppimiseen.

Itsearviointitestien avulla kurssin osallistujat pystyivät määrittämään tietämyksensä lähtötason ja tarkistamaan edistymisen kunkin koulutusaiheen jälkeen.

Suositellaan 3-5 kysymystä sisältävää itsearviointitehtävää, jossa on tosia/väärää, täsmääviä ja/tai monivalintakysymyksiä. Toinen aihe tulisi avata vasta, kun kaikkiin kysymyksiin on vastattu oikein. Aikarajoja tai rajoituksia yrittämiselle ei pitäisi olla. Kysymykset tulisi valita satunnaisesti tietokannan mukaisista kysymyksistä.



Kuva 13. Itsearviointitietokannan rakenne

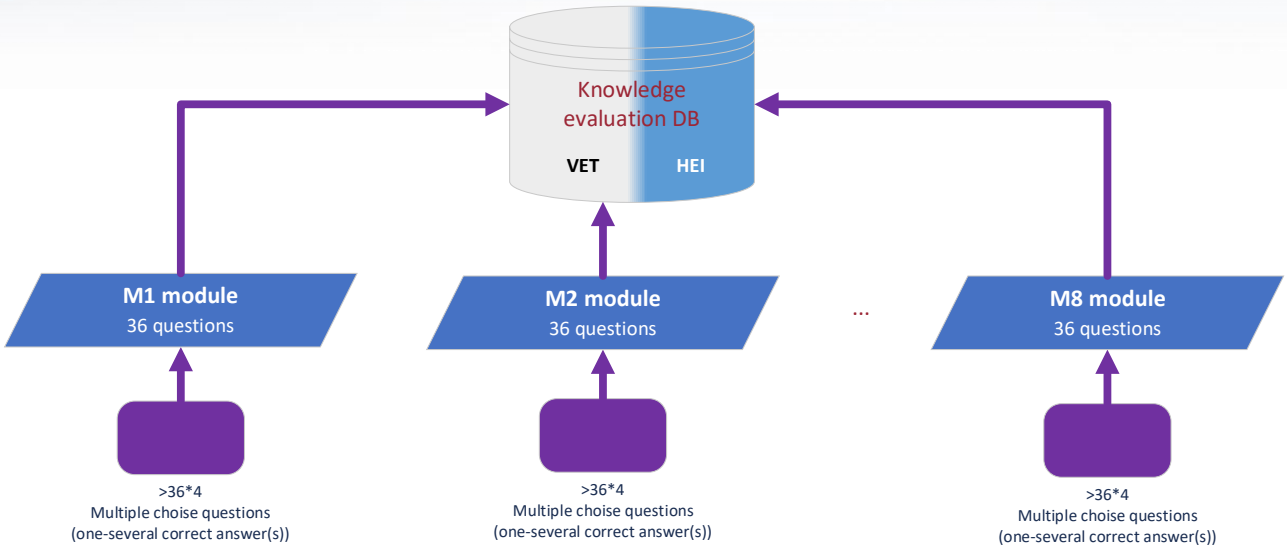
2. Tietojen arviointitesti*: Kurssin kaikki aiheet suoritettuaan opiskelijoiden on suoritettava loppukoe saadakseen todistuksen kurssin suorittamisesta. Tässä kattavassa arvioinnissa arvioidaan heidän yleistä ymmärrystään ja kurssin sisällön hallintaa. Loppukokeessa arvioidaan, miten hyvin opiskelijat ovat omaksuneet materiaalin ja miten hyvin he pystyvät soveltamaan tietojaan laajemmassa kontekstissa.

* Opetussuunnitelmaa ja materiaalia kehitettäessä harkitaan muita menetelmiä kurssin suorittamisen ja osaamisen arvioimiseksi, kuten tapaustutkimuksia, käytännön harjoituksia ja reflektiivisiä raportteja, joiden avulla voidaan arvioida kattavammin osallistujien analyyttisiä ja kriittisiä ajattelutaitoja. Tämä lähestymistapa on myös korkeakoulujen ja ammatillisen koulutuksen opiskelijoiden luennoitsijoiden käytettävissä kurssin toteutuksessa.

Tietämyksen arviointitestin avulla kurssin osallistujat pystyivät määrittelemään lopullisen tietämystasonsa, ja jos he olivat läpäisseet testin, he saivat kurssin suorittamisesta kertovan merkin (todistuksen).

Suositellaan 36 kysymystä sisältävää tietämyksen arviointitestiä, jossa on sekaisin tosi/väärää, täsmääviä ja monivalintakysymyksiä. Aikarajan tulisi olla 45 minuuttia, ja vain yksi yritys olisi sallittu. Testi olisi suoritettava valitsemalla kysymyksiä satunnaisesti tietokannasta.

Lisäksi arvioinnissa olisi otettava huomioon myös huijaamisen ehkäiseminen, ja siksi olisi laadittava noin neljä kysymyssarjaa. Osa sekä ammatillisen koulutuksen että korkea-asteen oppilaitosten tietämystestin kysymyksistä voi olla päällekkäisiä, joten kehittämishetkellä meillä on kolme ominaisuutta: VET, HEI tai VET ja HEI.



Kuva 14. Tietämyksen arviointitietokannan rakenne

Tämä kaksivaiheinen arviointistrategia ei ainoastaan tue tehokasta oppimista tarjoamalla useita palautesilmukoita, vaan se myös antaa oppijoille mahdollisuuden ottaa aktiivinen rooli koulutuksessaan.

Itsearviointitestit ja tietämyksen arviointitestit kehitetään kurssien opetussuunnitelman mukaisesti ja tässä hankkeessa kehitettyjen tulosten ja suositusten perusteella.

KYSYMYSTIETOKANNAN KOOSTUMUS

Riittävän laajan ja tasapainoisen kysymyspohjan varmistamiseksi kutakin ammatillisen koulutuksen tai korkea-asteen koulutuksen kurssin aihetta varten laaditaan vähintään viisi tosi/väärin-kysymystä tai täsmäkysymystä ja viisi monivalintakysymystä.

Jos oletetaan, että kullakin kurssilla on vähintään 10 aihealuetta, kunkin ammatillisen koulutuksen tai korkea-asteen koulutuksen kurssin kokonaispohjan olisi sisällettävä vähintään 10-20 prosenttia tosi/väärin-kysymyksiä tai vastauksia ja 90-80 prosenttia monivalintakysymyksiä. Tämä on yleinen ohje, mutta opettajalla on mahdollisuus valita kysymysten rakenne kurssin aiheen mukaan.

Kun otetaan huomioon ammatillisen koulutuksen ja korkea-asteen koulutuksen oppimistavoitteiden ja tulosten erot, yksittäisen kurssin kysymystietokannan kokonaiskoostumuksen tulisi olla seuraavassa taulukossa esitetyn mukainen.

Taulukko 6. Kysymystyypit

	Totta/väärää tai vastaavia kysymyksiä	**Monivalintakysymykset**
Kurssin yleinen osa	20%	80%
Kurssin ammatillista koulutusta koskeva osa	20%	80%
Korkeakoulukohtainen kurssin osa	20%	80%
Ammatillisen koulutuksen ja korkea-asteen koulutuksen kurssien kokonaismäärä:	20%	80%

KYSYMYSTEN LAATIMISTA KOSKEVAT OHJEET

Itsearviointikokeiden ja tietämyksen arviointikokeiden kysymykset on laadittava englanniksi, ja ne on sitten lokalisoitava kumppanikielille.

Kun kurssilla laaditaan testikysymyksiä sekä itsearviointia että osaamisen arviointia varten, on tärkeää varmistaa, että kysymykset ovat selkeitä, ytimekkäitä ja kaikkien kokelaiden ymmärrettävissä heidän taustastaan riippumatta. Tällä lähestymistavalla varmistetaan, että arvioinnit heijastavat tarkasti oppijoiden ymmärrystä kurssin sisällöstä ja heidän kykyään saavuttaa kurssin opetussuunnitelmassa esitetyt taidot ja tavoitteet.

Kysymysten laatimista koskevat yleiset ohjeet:

Koekysymyksiä laadittaessa noudatetaan selkeitä ohjeita: kysymysten on oltava ymmärrettäviä ja suoraan kurssin oppimistavoitteisiin liittyviä, eikä niissä saa käyttää monimutkaista terminologiaa tai sekavia sanamuotoja. Myös kulttuurisidonnaisia tai hämmentäviä kysymyksiä vältetään, jotta varmistetaan oikeudenmukaisuus ja saavutettavuus kaikille kurssilaisille. Seuraavassa annetaan lisäohjeita kysymysten suunnittelusta.

Selkeys ja yksinkertaisuus: Kysymysten on oltava selkeitä, ja niissä on vältettävä monimutkaista kieltä tai ammattisanastoa, joka voisi hämmentää tai johtaa hakijoita harhaan. Tavoitteena on arvioida hakijoiden tietämystä ja ymmärrystä aiheesta, ei heidän kykyään tulkita monimutkaisia kysymyksiä.

Suoraviivaisuus ja relevanssi: jokaisen kysymyksen on liityttävä suoraan kurssin opetussuunnitelman avaintaitoihin ja tavoitteisiin. Epäolennaista tai epäolennaista sisältöä olisi vältettävä, jotta keskitytään edelleen arvioimaan aiottuja oppimistuloksia.

Kulttuuri- ja taustaherkkyys: varmista, että kysymykset eivät edellytä erityistä kulttuuritietämystä tai -kokemusta, jotta ne ovat avoimia ja oikeudenmukaisia erilaisista taustoista tuleville hakijoille.

Ei hankalia kysymyksiä: jokaisen kysymyksen tarkoituksen on oltava selvä, eikä ehdokkaita saa yrittää johtaa harhaan tai huijata. Kysymyksillä, joiden tarkoituksena on saada hakijat ansaan tai testata heidän kykyään havaita huijaus, ei arvioida tehokkaasti hakijoiden ymmärrystä aiheesta.

Yksiselitteinen ja tiivis esitystapa: kysymykset on muotoiltava siten, että ne eivät jätä tulkinnanvaraa ja että kaikki kokelaat ymmärtävät kysymyksen samalla tavalla. Pidä kysymykset lyhyinä ja vältä tarpeettoman pitkiä kysymyksiä, jotka voisivat hämärtää pääkohdan.

Positiivinen muotoilu: vältä negatiivista muotoilua kysymyksissä (esim. "Mikä seuraavista ei ole..."). Kielteinen muotoilu voi johtaa sekaannukseen ja väärintulkintoihin erityisesti koeolosuhteissa. Sen sijaan muotoile kaikki kysymykset myönteisesti selkeyden edistämiseksi.

Erityiset ohjeet kysymysten laatimista varten:

Monivalintakysymykset: Varmista, että kaikki vaihtoehdot ovat uskottavia ja liittyvät kysymykseen. Oikean vastauksen pitäisi olla kiistatta oikea, kun taas harhauttavien vaihtoehtojen pitäisi olla selvästi virheellisiä aineistoa ymmärtävälle henkilölle.

Totta/väärin -kysymykset: Esitä selkeitä, tosiseikkoja sisältäviä väittämiä, jotka liittyvät suoraan kurssin sisältöön, jotta niiden totuusarvosta ei jää epäselvyyttä.

Vastaavat kysymykset: Varmista, että molemmat luettelot (esim. termit toisella puolella ja määritelmät toisella puolella) liittyvät selkeästi toisiinsa ja että kunkin vastaavuuden tekeminen on perusteltua. Vältä epätasaisia luetteloita, joissa kohtien määrä ei ole yhdenmukainen, ellei nimenomaisesti ilmoiteta, että joitakin kohteita ei käytetä tai että niitä voidaan käyttää useaan kertaan.

Pilottikoulutuksessa analysoidaan tietoa osaamisen arviointimenetelmistä ja arviointiprosessista keräämällä palautetta sekä oppijoilta että kouluttajilta. Näin voidaan arvioida osaamisen arviointimenetelmien soveltuvuutta ja tarvittaessa täydentää tai parantaa arviointimenetelmää.

Pelillistäminen

Tässä jaksossa kuvataan CyberAgent-kursseilla toteutetut pelillistämisen elementit. Pelillistäminen on prosessi, jossa pelillistämisen periaatteita sisällytetään perinteisiin oppimistoimintoihin osallistujien motivaation ja sitoutumisen lisäämiseksi. Nämä elementit on valittu viimeisimmän koulutusteknologiaa koskevan tutkimuksen perusteella, joka osoittaa, että pelillistäminen voi merkittävästi parantaa oppimistuloksia, lisätä opiskelijoiden motivaatiota oppimiseen ja lisätä heidän sitoutumistaan oppimisprosessiin.

Kursseihin integroituja pelillistämiselementtejä ovat muun muassa merkit, pisteet, sijoitukset ja värikoodatut lempinimet, jotka kuvastavat osallistujan kokemusta ja saavutuksia.

- Merkkejä jaetaan seuraavista:

- **Moduulin suorittaminen**.
- **Kokeen läpäisystä hyväksytyn prosenttiosuuden perusteella**. Osallistuja saa esimerkiksi pronssimerkin, jos hän on läpäissyt testin, hopeamerkin, jos hän on läpäissyt testin vähintään 75 %, kultamerkin, jos hän on läpäissyt testin vähintään 76 %-90 % ja platinamerkin, jos hän on läpäissyt testin vähintään 90 %-100 %. Tällöin yhdellä osallistujalla voi olla 8 tällaista merkkiä.
- **Aiheen loppuunsaattaminen**.
- **Kirjautuminen järjestelmään joka päivä kymmenen päivän ajan**.
- Kurssin ohjaaja/opettaja myöntää myös jokaisesta aiheesta **erityisen toimintamerkin.**

- Pisteet ja pistemäärät lasketaan itsearviointitestin pisteiden + lopullisen testin pisteiden ja kertoimen perusteella.

CyberAgent-kurssin osallistujat eivät voi nähdä edistymistään yksilöllisesti, mutta he voivat kilpailla muiden osallistujien kanssa ryhmissä tai joukkueissa (eniten pisteitä ja myös eniten merkkejä saavuttaneiden perusteella). Tämä kannustaa paitsi yksilölliseen myös ryhmäkilpailuun ja yhteistyöhön, mikä on tärkeää yhteistyötaitojen kehittämisessä.

Jokainen osallistuja näkee kurssille kirjautuessaan lempinimensä, joka on värikoodattu kurssin etenemisen ja kerätyn kokemuksen (suoritetut/kirjatut kurssit) mukaan.

Tämä auttaa kurssilaisia osallistumaan paremmin koulutusprosessiin. Kurssilaiset voivat toistaa saman testin useita kertoja parantaakseen pistemääräänsä (pisteitä saa eniten oikein suoritetuista itsearviointitesteistä).

Erityinen algoritmi laskee kunkin osallistujan pistemäärän ottaen huomioon vastaamiseen kuluneen ajan, testin toistokertojen määrän ja muut parametrit, mikä minimoi huijaamisen mahdollisuuden.

Kaikki pelisäännöt kuvataan ja kerrotaan osallistujille selkeästi, jotta jokainen voi helposti ymmärtää, miten eri pelitasot voidaan saavuttaa ja miten ne lasketaan.

7. CYBERAGENT-OPPIMIS-/OPETUSPROSESSI

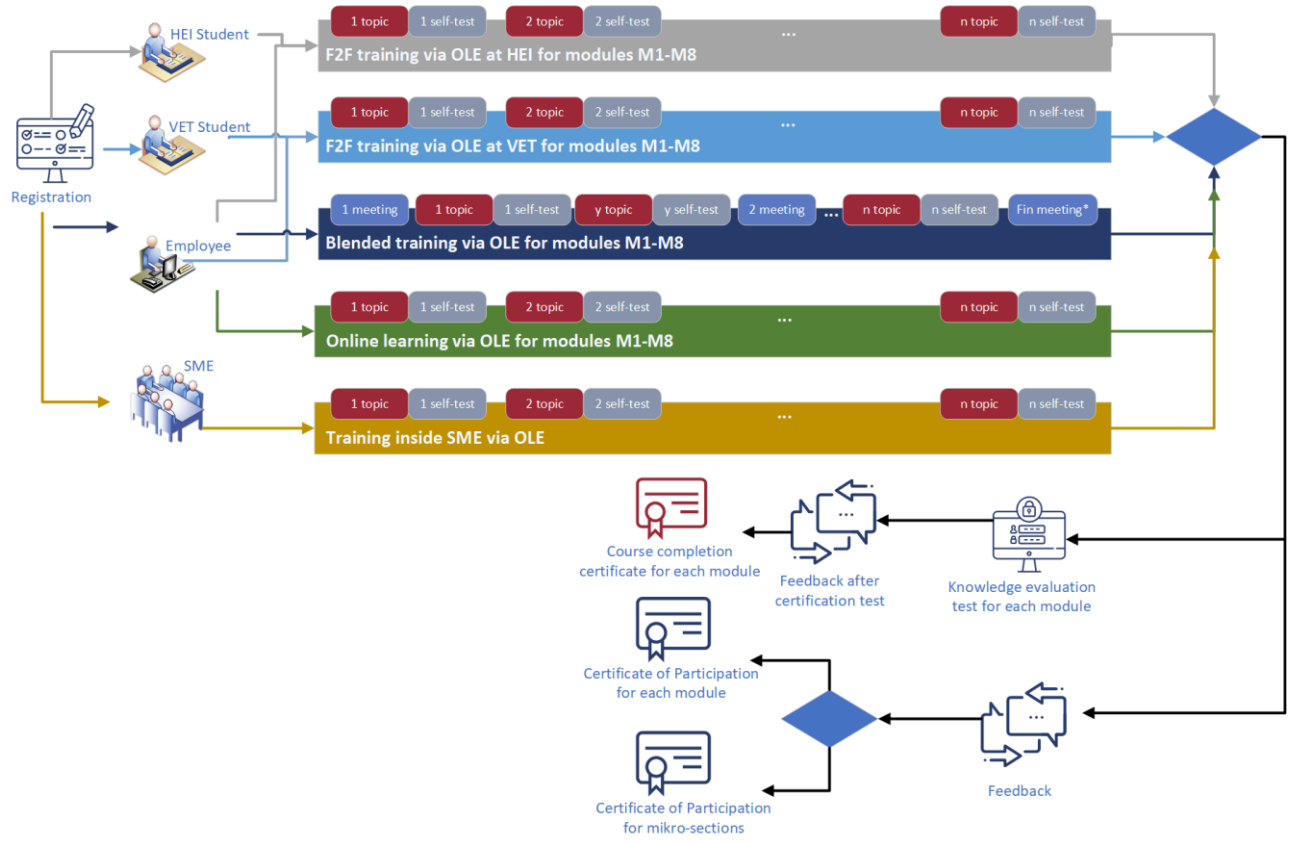
Tässä jaksossa esitetään yhteenveto tämän asiakirjan kaikkien lukujen tiedoista ja kuvataan yksityiskohtaisesti oppimis-/opetusprosessi, joka alkaa ilmoittautumisesta CyberAgent-kurssille oppimisalustalla ja päättyy kurssin suorittamiseen tai todistuksen myöntämiseen.

CyberAgent-kurssit on suunniteltu erilaisille oppijoille, kuten korkeakouluopiskelijoille, ammatillisen koulutuksen opiskelijoille sekä pk-yritysten työntekijöille. Pyrimme antamaan jokaiselle osallistujalle mahdollisuuden valita itselleen parhaiten sopivan oppimistavan ottaen huomioon henkilökohtaiset olosuhteet ja oppilaitoksen organisaatiokäytännöt.

Valitusta oppimis-/koulutusmenetelmästä huolimatta osallistujat rekisteröityvät CyberAgent-alustalle ja käyttävät sitä koulutuksen aikana.

Rekisteröinti

CyberAgent-kurssille ilmoittautumisesta kiinnostuneiden tulevien osallistujien on täytettävä ilmoittautumislomake ja valittava haluamansa moduulit ja haluamansa oppimismenetelmä. Osallistujia ohjataan käsitteellisellä kaaviolla oppimispolun läpi ensimmäisestä kahdeksanteen CyberAgent-moduuliin.



Kuva 15. CyberAgent-oppimis-/opetuspolku

Osallistujien tietojen luottamuksellisuus varmistetaan rekisteröintiprosessin aikana erityisesti yleisen tietosuoja-asetuksen vaatimusten mukaisesti. Rekisteröitymisen aikana osallistujilla on mahdollisuus tutustua koulutusalustan sääntöihin sekä yksityisyyden suojaa ja tietosuojaa koskeviin sääntöihin.

Osallistujien rekisteröintitietoihin pääsevät käsiksi vain kumppanien organisaatiossa nimetyt henkilöt organisaation sisäisten käytäntöjen mukaisesti. Pilottikoulutustilaisuuksien aikana hankekumppaneiden osallistujatietoihin voi päästä käsiksi CyberAgent-koordinaattori, eivätkä muut kumppanit saa nähdä toistensa osallistujatietoja. Hankkeen päätyttyä koordinaattori voi käyttää muiden kumppaneiden anonymisoituja tietoja ainoastaan hankkeen tulosten seurantaa varten, kuten hankehakemuksessa on määritelty, enintään viiden vuoden ajan hankkeen päättymisen jälkeen.

Tarjoamme räätälöityjä koulutusvaihtoehtoja erilaisten kohderyhmien tarpeisiin. Korkeakouluopiskelijat ja ammatillisen koulutuksen opiskelijat voivat osallistua koulutukseen yliopistojen yhteistilaisuuksien kautta. Pk-yritysten työntekijät voivat valita tarpeisiinsa parhaiten sopivan oppimismenetelmän: sekamuotoinen oppiminen, pelkkä verkko-opiskelu tai harvemmin osallistuminen korkeakoulun tai ammatillisen koulutuksen luennoille.

Koulutusta voidaan tarjota myös suuremmille yrityksille, joilla on useita työntekijöitä. Tällaisissa tapauksissa koulutusmenetelmä räätälöidään vastaamaan erityistarpeita, mutta siihen sisällytetään silti CyberAgent-moduulin kurssit.

Rekisteröitymisen jälkeen osallistujat valitsevat oppimismenetelmän ja aloittavat opinnot. Kun he ovat suorittaneet moduulin tai sen osan, he voivat saada osallistumistodistuksen tai kurssin päättämistodistuksen, joista jälkimmäinen myönnetään, jos osallistuja läpäisee moduulin kokeen vähintään 75 prosentin tuloksella.

Lopuksi osallistujien on täytettävä palautelomake ennen todistuksen saamista. Tämä palaute on ratkaisevan tärkeää koulutustarjontamme jatkuvan parantamisen ja osallistujien tyytyväisyyden varmistamisen kannalta.

Oppimis-/koulutustavat

Työntekijöillä on useita vaihtoehtoja osallistua kurssin sisältöön:

- Jos korkeakoulut tai ammatilliset oppilaitokset sallivat työntekijöiden osallistumisen vierailevana osallistujana, työntekijä voi osallistua luennoille ilmoittautuneiden opiskelijoiden rinnalla. Tällaisia ulkopuolisen osallistujan istuntoja voidaan järjestää 1-2 kertaa vuodessa julkaistun luentoaikataulun perusteella.
- Työntekijät voivat valita yhdistelmäkoulutuksen, jossa koulutustilaisuudet järjestetään tiettyinä päivinä, ja niiden suositeltu kesto on 2-4 kuukautta. Vähintään 10 osallistujan ryhmät ovat suositeltavia, ja ryhmässä voi olla enintään 30 osallistujaa. Sekakoulutukseen sisältyy sekä henkilökohtaisia että verkkokonsultaatioita kurssin alussa, sen aikana ja lopussa, mikä helpottaa suoran palautteen antamista ja valmistautumista loppuarviointiin.

- Työntekijät voivat valita verkko-opiskelutavan itseopiskelua varten, eikä kurssin suorittamiselle ole asetettu kestoaikaa.
- Lisätietoja CyberAgent-moduuleista on kohdassa 1. Opintopolku.

Opiskelijoiden osallistuminen

Kyberturvallisuuden opinto-ohjelmaan ilmoittautuneet opiskelijat voivat kohdata erilaisia reittejä oppilaitoksensa sääntöjen mukaan. Heiltä voidaan joko vaatia joidenkin tai kaikkien CyberAgent-moduulien suorittamista, tai korkeakoulun sisäisistä käytännöistä riippuen kriteerit täyttävät opiskelijat voivat valita yhden tai useamman CyberAgent-moduulin opiskelun. Korkeakoulu- tai ammatillisen koulutuksen opiskelijat osallistuvat aiheisiin yleensä oppilaitoksensa tarjoaman perinteisen luokkahuoneopetuksen avulla tai voivat valita itseopiskelumenetelmän valmistautuakseen lopulliseen tietämyksen arviointikokeeseen.

Pk-yritysten osallistuminen

Organisaatioissa, joissa kyberturvallisuuskoulutusta pidetään tarpeellisena, yrityksen edustaja voi ilmoittaa organisaation sisäisiin koulutustilaisuuksiin. Tällöin koulutusmenetelmä, aikataulu ja todistusten antaminen voidaan räätälöidä organisaation erityistarpeiden mukaan olemassa olevien moduulien pohjalta, kun asiasta on sovittu erikseen yliopiston ja/tai kouluttajien kanssa.

Palautteen kerääminen

Moduulin päätyttyä osallistujien on täytettävä verkossa oleva anonyymi palautelomake. Palautetietoihin on pääsy vain yhteistyökumppanin organisaation valtuutetuilla henkilöillä, ja samanlaisia luottamuksellisuustoimenpiteitä sovelletaan pilottikoulutustilaisuuksissa ja hankkeen jälkeisessä tietojen käytössä.

Palautetta kerätään pääasiassa kurssilaisilta, mutta palautetta kerätään myös ohjaajilta/kouluttajilta. Kerätyssä palautteessa arvioidaan osallistujien tyytyväisyyttä organisaatioon, kurssin järjestämiseen liittyviä näkökohtia, oppimisprosessia, hankitun osaamisen käyttöä käytännössä, kurssin sisältöä, arviointistrategioita, pelillistämisen elementtien sisällyttämistä kurssille, parannettavaa jne.

Palautteen tuloksia tarkastellaan säännöllisesti ja ne esitellään hankkeen johtoryhmälle, jotta voidaan reagoida nopeasti ja parantaa koulutusstrategioita todellisten tarpeiden ja markkinoiden muutosten mukaan.

Vain tämän lomakkeen täyttämisen jälkeen osallistujat ovat oikeutettuja saamaan osallistumistodistuksen tai todistuksen kurssin suorittamisesta tai osallistumistodistuksen.

Kurssin suorittamista koskeva todistus

Arviointitestin hyväksytyn suorittamisen jälkeen osallistujalle annetaan todistus kurssin suorittamisesta. Kussakin moduulissa on yksi loppukoe.

Osallistumistodistus

Osallistujat, jotka päättävät olla osallistumatta tietämyksen arviointikokeeseen, voivat saada osallistumistodistuksen. Osallistumistodistus voidaan antaa yksittäisen moduulin tai useamman kurssin pienosion suorittamisesta.

PÄÄTELMÄT JA YHTEENVETO

Tässä raportissa on onnistuneesti kehitetty pk-yritysten kyberturvallisuuden muutosagenttien jäsenneltyjä oppimispolkuja, jotka on räätälöity vastaamaan erityistarpeisiin eri koulutus- ja ammattitasoilla korkeakouluista ammatilliseen koulutukseen ja pk-yritysten työntekijöiden suoraan koulutukseen. Kahdeksasta kattavasta moduulista koostuvassa opetussuunnitelmassa yhdistyvät tekniset, analyyttiset, organisatoriset ja riskinhallintataidot, jotka ovat ratkaisevan tärkeitä tulevien kyberturvallisuuden ammattilaisten tehokkaan voimaannuttamisen kannalta.

Oppimispolkuja koskeva jäsennelty lähestymistapa takaa pk-yritysten työntekijöille kattavan oppimismatkan. Se tukee tietojen säilyttämistä ja käytännön soveltamista esiopetuksen, oppimisen ja jälkiopetuksen vaiheiden avulla. Mikromoduulit tarjoavat joustavuutta ja mukautuvuutta yksilöllisiin tarpeisiin ja tehostavat oppimista mikrotodistuksilla, jotka antavat tunnustettuja pätevyyksiä. Tämä mukautuminen alan standardeihin auttaa merkittävästi vahvistamaan pk-yritysten kyberturvallisuusvalmiuksia ja valmistaa työntekijöitä vastaamaan nykyisiin haasteisiin ja tuleviin edistysaskeliin. Seuraavassa Career Pathway -analyysissä on kartoitettu ESCO-kehyksen määrittelemien kyberturvallisuustehtävien eteneminen, mikä helpottaa kohdennettua koulutuslähestymistapaa, joka valmistaa yksilöitä tehokkaaseen integroitumiseen kyberturvallisuustyövoimaan, mikä viime kädessä parantaa heidän uranäkymiään ja ammatillista kehittymistään.

Tutkittujen pedagogisten lähestymistapojen moninaisuuden kyberturvallisuuden opetussuunnitelmassa pitäisi mahdollistaa dynaaminen ja joustava oppimisympäristö, jossa otetaan huomioon erilaiset oppimistyylit ja -tarpeet. Erilaisten opetusmenetelmien, kuten teoreettisten luentojen, käytännön laboratorioiden, pelillistämisen ja yhteistoiminnallisten projektien sisällyttäminen opetukseen varmistaa, että opiskelijat eivät ole vain tiedon vastaanottajia vaan aktiivisia osallistujia oppimismatkallaan. Tämän kokonaisvaltaisen strategian pitäisi lisätä sitoutumista ja ymmärrystä ja valmistaa opiskelijat paremmin reaalimaailman kyberturvallisuushaasteisiin. Opetusmenetelmien mukauttaminen moduulikohtaisiin vaatimuksiin yksilöllistää oppimiskokemusta entisestään ja varmistaa, että oppimistulokset maksimoidaan jokaisen opiskelijan osalta.

Kun CyberAgent-hankkeen alateemat ja moduulit kartoitetaan järjestelmällisesti kansainvälisesti tunnustettuihin tietoyksiköihin, opetussuunnitelma ei ainoastaan vastaa kyberturvallisuusalan dynaamisiin vaatimuksiin vaan myös ennakoi niitä. Tällä metodisella lähestymistavalla varmistetaan, että jokainen oppimistulos on strategisesti kytketty reaalimaailman osaamiseen, joka on ratkaisevan tärkeää kyberturvallisuusuhkien tehokkaan hallinnan kannalta. Opetussuunnitelman mukautuvuuden ansiosta se soveltuu alan eri ammatillisiin tehtäviin ja valmistaa oppijat paitsi välittömiin haasteisiin myös pitkän aikavälin urakehitykseen kyberturvallisuuden alalla.

Hahmoteltu kurssin arviointistrategia tarjoaa puitteet kyberturvallisuusohjelmien opiskelijoiden taitojen ja edistymisen arvioimiseksi. Kaksivaiheinen lähestymistapa, jossa yhdistyvät itsearviointitestit ja kattavat osaamisen arviointitestit, antaa opiskelijoille mahdollisuuden

paneutua aktiivisesti materiaaliin, arvioida jatkuvasti ymmärrystään ja mukauttaa oppimisstrategiansa sen mukaisesti. Suunnittelemalla arviointi räätälöityjen kysymysten avulla niin, että se sopii sekä korkeakoulujen että ammatillisen koulutuksen opiskelijoille, strategia varmistaa relevanssin ja soveltuvuuden kullekin koulutustasolle ja parantaa oppimiskokemusta. Menetelmän avulla voidaan mitata selkeästi opiskelijoiden hallintaa ja valmiutta soveltaa tietojaan käytäntöön. Lisäksi pelillistämisen elementit, kuten merkit ja pisteytysjärjestelmät, motivoivat opiskelijoita ja edistävät kilpailukykyistä mutta samalla yhteistoiminnallista oppimisympäristöä.

Lopuksi voidaan todeta, että CyberAgent-oppimis- ja opetusprosessi tarjoaa kattavan ja mukautettavan opetuskehyksen, joka soveltuu monenlaisille korkeakoulujen, ammatillisten oppilaitosten ja pk-yritysten oppijoille. Järjestelmä mahdollistaa erilaiset osallistumismenetelmät, kuten kasvokkain tapahtuvan, yhdistetyn ja verkko-oppimisen, mikä takaa joustavuuden siinä, miten kyberturvallisuuskoulutusta annetaan ja miten siihen pääsee osallistumaan. Rekisteröityminen CyberAgent-alustalle käynnistää polun, jossa osallistujat valitsevat haluamansa moduulit ja oppimismenetelmät, ja joka huipentuu todistusten antamiseen, kun koulutus on suoritettu ja arvioitu onnistuneesti. Tämä rakenne ei ainoastaan tue yksilöllisiä oppimispolkuja, vaan se vastaa myös tiukkoja yksityisyysvaatimuksia, jotka ovat välttämättömiä osallistujien luottamuksellisuuden säilyttämiseksi koko koulutusprosessin ajan.

Tässä asiakirjassa annettuja suosituksia ja ohjeita käytetään seuraavassa vaiheessa kehitettäessä CyberAgent-koulutusjärjestelmän kattavia koulutusohjelmia, koulutusmateriaaleja, tietämystestejä ja -arviointeja, harjoitusharjoituksia ja muuta koulutussisältöä, jotka integroidaan CyberAgent-koulutusalustaan.

LIITE 1. MODUULIN KUVAUS

MODUULIN KUVAUS

Moduulin nimi	Moduulin koodi
...	

Luennoitsija (s)	Oppilaitos tai laitos, jossa moduuli suoritetaan
...	...

Toimitustapa	Kieli
Kasvokkain, verkossa, yhdistelmäkonsultaatiot, kuulemiset.	*Englanti, ...*

Edellytykset
...

Myönnettyjen ECTS-opintopisteiden määrä	Opiskelijan" työmäärä	Yhteystiedot työaika	Yksilöllinen työaika
5	...	...	...

Moduulin tarkoitus ja tulokset		
...		
Moduulin oppimistulokset	**Opetus- ja oppimismenetelmät**	**Arviointimenetelmät**
Tekniset taidot		
Analyyttiset taidot		
Riskitaidot		
Organisaatiotaidot		

Resurssien (laitteet, ohjelmistot, teknologia) helpottaminen.
...

Moduulin sisältö: aiheiden jakautuminen	**Yhteystiedot työaika**					**Yksilölliset työajat ja tehtävät**	
	Luennot (HEI/VET)	Kuulemiset (pk-yritykset)	Käytäntö (HEI/VET)	Testit	**Kaikki kontaktityöt**	**Yksilöllinen työ**	**Tehtävät**
1							
…							
n							
Yhteensä							

Arviointistrategia	**Vertailukelpoinen painoprosentti**	**Arviointiperusteet**
Itsetesti I		…
…		…
Itsetesti n		…
Tietojen arviointitesti		…
HEI/VET-todistus -> Itsetesti I + …+ Itsetesti n + Tietojen arviointitesti.		
Pk-yritykset / itseopiskelijoiden sertifiointi -> Itsetesti I + …+ Itsetesti n + Osaamisen arviointitesti.		
Mikromoduulit, mikro-osat -> Itsetesti I (valinnainen), Itsetesti n (valinnainen).		

Tutkimusaineisto *(Sukunimi, etunimi. (Vuosi, kuukausi, päivä). Artikkelin otsikko. Aikakauslehden/lehden/uutislehden otsikko, niteen numero (numeron numero), koko artikkelin sivunumerot, kustantaja, URL-osoite).*
Pakollinen lukeminen
…
Suositeltu lukeminen
…

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