UNIVERSITY OF TURKU
Faculty of Technology

Tietoturva ohjelmoinnin ja ohjelmistotuotannon kursseilla Suomen yliopistoissa – nykytila ja opettajien näkemykset

Anne-Maarit Majanoja, Antti Hakkala, Ville Leppänen, Seppo Virtanen

Reports from the Faculty of Technology No. 3

University of Turku, Finland, 2024

UNIVERSITY
OF TURKU
Faculty of Technology

Reports from the Faculty of Technology No. 3
University of Turku, Finland, 2024

Teknillisen tiedekunnan raportteja nro 3
Turun yliopisto, 2024

Copyright © the Authors

ISBN 978-952-02-0004-6 (PDF)
ISSN 2984-360X (Online)

TIIVISTELMÄ

Tekijät: Anne-Maarit Majanoja[1,*], Antti Hakkala[1], Ville Leppänen[1], Seppo Virtanen[1]

Otsikko: Tietoturva ohjelmoinnin ja ohjelmistotuotannon kursseilla Suomen yliopistoissa – nykytila ja opettajien näkemykset

Julkaisun tiedot: Reports from the Faculty of Technology No. 3, University of Turku, Finland, 2024, 47 pages

Tässä raportissa kuvataan yliopistojen ohjelmoinnin ja ohjelmistotuotannon opettajille suunnatun kyselyn tuloksia. Kysely toteutettiin Kansallisen kyberturvallisuuskoulutuksen yhteistyöverkoston rakentaminen -hankkeen aikana. Hankkeeseen osallistuu yhdeksän suomalaista yliopistoa, jotka tarjoavat kyberturvallisuusalan koulutusta. Kyselyn tarkoituksena oli tunnistaa nykytilanne: miten hyvin tietoturva-aiheita on ollut mahdollista integroida osaksi ohjelmoinnin ja ohjelmistotuotannon kursseja; opettajien kokemia ja tunnistamia puutteita, tarpeita ja ideoita, sekä aiheita kyberturvallisuuskoulutuksen kehittämiseksi Kartoitus toteutettiin 26.8.-13.9.2024., ja kyselyyn vastasi 54 ohjelmoinnin ja/tai ohjelmistotuotannon kurssien opettajaa.

Opettajat pitävät tietoturvaopetusta tärkeänä osana ohjelmistokehityksen ja ohjelmoinnin koulutusta, mutta kohtaavat monia haasteita sen integroimisessa kurssien sisältöihin. Yleisesti havaittiin, että tietoturvan opetuksen laajuus ja syvyys vaihtelevat huomattavasti eri kurssien ja opintojen tasojen välillä. Monien mielestä peruskurssien resurssit eivät riitä kattavaan tietoturvaan perehdyttämiseen, ja monet perustason opiskelijat kokevat aiheen liian haastavaksi, sillä heillä ei ole vielä riittävästi pohjatietoja ymmärtää tietoturvaan liittyviä aiheita syvällisesti.

Perusopintojen tasolla tietoturva-aiheiden käsittely on hyvin rajallista, sillä kurssit keskittyvät pääasiassa ohjelmoinnin ydintaitoihin. Opettajat kokevat, että tietoturva-aiheiden lisääminen peruskursseille voisi olla haastavaa ja mahdollisesti liian vaativaa opiskelijoille, joilta puuttuu perusosaaminen laajemman tietoturvakuvan ymmärtämiseen. Tietoturvaan liittyviä aiheita ei juurikaan käsitellä ohjelmoinnin perusteissa tai ohjelmistotuotannon kursseilla. Aineopinnoissa tietoturvaa käsitellään jonkin verran enemmän, mutta se ei ole systemaattisesti integroitu kurssien sisältöihin. Useat opettajat toivoisivat lisää käytännön harjoituksia ja tietoturvan soveltamista projektitöihin, jotta opiskelijat voisivat soveltaa tietoturvaoppiaan käytännössä.

---

[1] Yksikkö: Turun yliopisto, tietotekniikan laitos
* Yhteyskirjoittaja: Anne-Maarit Majanoja, amtmaj@utu.fi

Syventävissä opinnoissa opiskelijoilla on paremmat valmiudet käsitellä tietoturvan monimutkaisia käytäntöjä ja konsepteja. Ehdotuksena onkin, että tietoturvanäkökulmille tulisi järjestää erillisiä kursseja (Secure Programming ja Secure Software Development -kurssit), joissa keskityttäisiin esimerkiksi tietoturvan huomioimiseen vaatimusmäärittelyssä, uhkamallinnukseen, penetraatiotestaukseen ja arkkitehtuuritason tietoturvaan, sekä tietoturvaan ohjelmoinnin näkökulmasta. Tämä mahdollistaisi tietoturvan syvällisemmän ja kattavamman käsittelyn ilman, että se rikkoo muiden kurssien ydinsisältöjä ja oppimistavoitteita. Haasteena koetaan, että usein yliopistojen budjetit ja resurssit eivät kuitenkaan riitä tarjoamaan erityisiä tietoturvaharjoituksia tai -ympäristöjä esimerkiksi penetraatiotestauksen tai verkkoliikenteen analyysin toteuttamiseen.

Opettajat kohtaavat merkittäviä haasteita ajan ja resurssien puutteessa, mikä estää tietoturva-aiheiden syvällisen käsittelyn kurssien aikana. Monet opettajat kokevat, että heidän tietoturvaosaamisensa on rajallista, koska he joutuvat seuraamaan monia aiheita ja näkökulmia, jotka liittyvät ohjelmointiin ja/tai ohjelmistotuotantoon, kun taas tietoturva on oma erityisalansa, joka vaatii jatkuvaa oppimista ja perehtyneisyyttä.

Kehitystoimenpiteinä nousi esille tietoturvaopetuksen strategian kautta tapahtuva integrointi eri kurssien sisältöihin, erillisten tietoturvakurssien luominen sekä käytännön harjoitusten lisääminen osaksi opetusta. Tietoturva tulisi käsitellä jokaisen kurssin omassa kontekstissa, jotta opiskelijat ymmärtäisivät sen merkityksen eri teknisissä aiheissa. Teknisten näkökulmien lisäksi olisi hyödyllistä käsitellä kyberturvallisuutta laajemmassa kontekstissa, joka sisältäisi myös eettiset näkökulmat ja kyberpsykologian.

Tietoturva on tärkeä, mutta haasteellinen osa ohjelmistokehityksen opetusta. Erillisten tietoturvakurssien tarjoaminen ja käytännönläheisten oppimismenetelmien lisääminen auttaisivat vastaamaan työelämän odotuksiin tietoturvataitojen osalta. Tietoturvaopetuksen kehittäminen edellyttää kuitenkin lisäresursseja, strategista suunnittelua ja tarvittavien opetusmateriaalien saatavuutta, jotta aiheeseen voidaan paneutua nykyistä paremmin eri opintojen tasoilla.

AVAINSANAT: Kyberturvallisuuskoulutus, Ohjelmoinnin kurssit, Ohjelmistotuotannon kurssit, Opettajakysely, Opettajien näkemykset ja kokemukset, Opetuksen kehittäminen, Kyberturvallisuuskoulutuksen kehittäminen

Sisällys

1 Johdanto

Ohjelmointi- ja ohjelmistotekniikan kurssit luovat perustan kaikille tietotekniikkataidoille, myös kyberturvallisuudelle. Siksi on tärkeää ottaa huomioon ohjelmointi- ja ohjelmistotekniikan tärkeä rooli kyberturvallisuustaitojen kehittämisen perustana. Traficom toteutti vuonna 2023 Ohjelmistoturvallisuuden tila -selvityksen, jonka tuloksissa tuotiin esille, että ohjelmistokehityksen turvallisuusaiheiden opetuksessa on puutteita. Kuitenkin Traficomin toteuttamaan selvitykseen osallistuneiden korkeakoulujen määrä on hyvin alhainen (4 korkeakoulua). Tästä syystä on tarpeen tehdä lisäselvitystä yliopistojen ohjelmoinnin ja ohjelmistotuotannon opetuksen osalta. Tämän Turun yliopiston ohjelmistotekniikan ja kyberturvallisuusteknologioiden tutkimusyksiköiden toteuttaman kyselyn kautta pyritään täydentämään kuvaa nykytilanteesta ja kartoittamaan mahdollisia syitä sille, miksi kyberturvallisuuden aiheiden käsittely osana kursseja on jäänyt vähäiseksi sekä tunnistamaan ideoita ja keinoja kyberturvallisuusopetuksen kehittämiseksi.

Kansallisen kyberturvallisuuskoulutuksen yhteistyöverkoston rakentamisen hankkeen (jatkossa kyberturvallisuushanke) ohjausryhmässä on myös noussut esille turvallisen ohjelmoinnin ja turvallisen ohjelmistotuotannon aiheiden käsittely osana ICT-alan tutkintoja. Hankkeeseen osallistuu 9 suomalaista yliopistoa (Jyväskylän yliopisto, Turun yliopisto, Tampereen yliopisto, Vaasan yliopisto, Lappeenrannan-Lahden teknillinen yliopisto, Helsingin yliopisto, Aalto-yliopisto, Oulun yliopisto, Åbo Akademi), joissa järjestetään kyberturvallisuusalan koulutusta sekä ohjelmoinnin ja ohjelmistotuotannon koulutusta. Hankkeen tehtävänä on vahvistaa korkeakoulujen kyberturvallisuusalan opetusyhteistyötä sekä vuorovaikutusta teollisuuden ja julkisen sektorin kanssa, jotta alan tutkinto-opetuksen ja jo työelämässä olevien kyberturvallisuusosaamisen kehittäminen mahdollistuu. Hankkeen rahoittajana toimii Suomen opetus- ja kulttuuriministeriö. Hankeaika on 1.1.2023-31.12.2025.

Tämä raportti perustuu kyselyyn, jossa kartoitettiin suomalaisten yliopistojen opettajien näkemyksiä ja kokemuksia tietoturva-aiheiden sisällyttämisestä ohjelmoinnin ja ohjelmistotuotannon kursseille. Kartoitus toteutettiin 26.8.-13.9.2024., ja kyselyyn vastasi 54 ohjelmoinnin ja/tai ohjelmistotuotannon kurssien opettajaa. Kyselyn tarkoituksena oli selvittää, miten tietoturva tällä hetkellä näkyy eri kurssien sisällöissä ja mitä haasteita ja

kehitysmahdollisuuksia opettajat kokevat sen opetuksessa. Tämän ohjelmoinnin ja ohjelmistotuotannon opettajille suunnatun kyselyn tulosten avulla tunnistetaan puutteita, tarpeita ja ideoita sekä tunnistetaan aiheita kyberturvallisuuskoulutuksen kehittämiseksi.

Tietoturvan merkitys on kasvanut digitalisaation ja teknologisten uhkien lisääntyessä nopeasti. Ohjelmistokehitys on yksi aloista, joissa tietoturvallisuus on keskeisessä roolissa, koska ohjelmistot ovat keskeisessä roolisissa resurssien toteutuksen osalta ja tietoturvauhat kohdistuvat juuri näihin resursseihin. Lisäksi ohjelmistojen heikot tietoturvakäytännöt voivat altistaa kriittiset järjestelmät ja henkilökohtaiset tiedot hyökkäyksille. Tämä on herättänyt tarpeen selvittää opettajien mahdollisuuksia integroida tietoturva-aiheita osaksi ohjelmoinnin ja ohjelmistotuotannon koulutusta. Suomen yliopistoissa tietoturvaopetuksen käytännöt ja resurssit kuitenkin vaihtelevat, mikä luo haasteita sen järjestelmälliselle ja kattavalle opetukselle.

Opettajien vastauksista nousee esille näkemyksiä ja kokemuksia, jotka heijastavat tietoturvan integroimiseen liittyviä käytännön kysymyksiä. Tällaisia ovat ajan, resurssien ja materiaalien puute, opiskelijoiden vaihtelevat taidot sekä tarve koordinoida tietoturvan opetus strategisella tasolla osaksi muuta koulutusta.

Yliopistojen kyberturvallisuushankkeen osalta tämä raportti tukee työvaihe 2:n tuloksia. Raportissa esitettyjen tulosten sekä aiempien kartoitusten avulla muodostuu kokonaiskuva nykyisistä kyberturvallisuusalan koulutussisällöistä. Ensimmäisessä kartoituksessa (Majanoja et al., 2024a) selvitettiin yliopistojen kybertuvallisuuskoulutuksen sisältöjä, ja toisessa (Majanoja et al. 2024b) kartoitettiin yritysten kyberturvallisuuskoulutukseen liittyviä tarpeita yrityskyselyn kautta. Tämä raportti laajentaa aiempien tulosten kokonaisuutta ja tuo lisänäkemystä nykyisiin ja tuleviin koulutustarpeisiin sekä korkeakoulujen koulutussisältöjen kehittämissuuntiin työelämän osaamistarpeet huomioiden.

2 Opettajakyselyn toteutus, tavoitteet ja vastaajat

Opettajille suunnattu kysely toteutettiin Turun yliopiston hallinnoimalla Webropol-kyselyllä. Kyselyn rakenne määriteltiin kesäkuussa 2024 ja kysely työstettiin valmiiksi Webropoliin lopulliseen muotoon elokuussa 2024. Kysely oli avoinna 26.8.-13.9.2024. Kyselyn vastaajia olivat ohjelmoinnin ja erilaisten ohjelmistotuotannon aiheiden opettajat, jotka on mainittu vastuuopettajina yliopistojen kurssikuvauksissa. Yhteystiedot opettajille koottiin kahdella tavalla: 1) kyberturvallisuushankkeeseen kuuluvat yliopistot toimittivat opettajalistan, joille kyselyn voi lähettää, 2) yliopistojen julkisista kurssikuvauksista tunnistettiin ohjelmoinnin ja ohjelmistotuotannon opettajia, joille kysely lähetettiin vastattavaksi.

Kyselyn tavoitteena oli tarkastella turvallisen ohjelmoinnin ja turvallisen ohjelmistotuotannon aiheiden käsittelyä osana ohjelmoinnin ja ohjelmistotuotannon kurssien aiheiden käsittelyä. Tutkimuksessa keskityttiin kahteen pääaiheeseen:

1. Miten paljon tietoturva-aiheita ehditään ja pystytään käsittelemään ohjelmoinnin ja ohjelmistotuotannon kurssien aikana
2. Mitä haasteita kohdataan ja koetaan tietoturva-aiheiden käsittelyssä ohjelmoinnin ja ohjelmistotuotannon kursseilla.

Kyselyllä pyrittiin selvittämään, mikä on nykytilanne, onko nykytilanteessa mahdollista käsitellä turvallisen ohjelmoinnin ja ohjelmistokehityksen näkökohtia kursseilla, ja jos käsittely on mahdollista, kuinka paljon sitä voidaan tehdä. Tavoitteena oli myös tunnistaa ja saada opettajilta ideoita siitä, millaisia tietoturvaan liittyviä aiheita olisi hyvä opettaa opiskelijoille ohjelmoinnin ja ohjelmistotuotannon kursseilla. Tämä suoraan ohjelmoinnin ja ohjelmistotuotannon opettajilta saatu tieto tarjoaa lisäksi kyberturvallisuushankkeelle kehitysideoita ja näkökulmia kyberturvallisuuskurssien ja -opetuksen kehittämiseksi. Kyselyn avulla laajennetaan jo aiemmin toteutettujen selvitysten ja kyselyiden kautta saatua kuvaa kyberturvallisuustaitojen nykytilanteesta ja tulevaisuuden tarpeista yrityksissä ja organisaatioissa. Tuloksia käytetään yliopistojen kyberturvallisuuskoulutuksen kehittämiseen ja parantamiseen.

Kysymyksiä oli yhteensä 18–20, riippuen vastaajan opettamista kursseista. Kaikki tiedot käsiteltiin nimettöminä, eikä mitään tietoja luovuteta sellaisenaan kolmansille osapuolille. Osittaisia tiivistelmiä ja anonymisoituja lainauksia saatetaan julkaista osana akateemisia julkaisuja tai muita raportteja, mutta kaikki viittaukset tunnistetietoihin poistetaan. Julkaistut tulokset sisältävät koottuja tilastollisia havaintoja, joista on mahdotonta tunnistaa yksittäisiä vastauksia.

Kyselyyn vastasi 54 ohjelmoinnin ja ohjelmistotuotannon kurssien opettajaa. Vastausprosentti oli 56 %. Näin ollen yli puolet opettajista, joille kysely lähetettiin, vastasi kyselyyn.

2.1 Kyselyn tausta ja kysymysten määrittäminen

Kyselyn taustalla on useita tekijöitä, joiden kautta tarve aiheen tarkemmalle tarkastelulle nousi ajankohtaiseksi. Traficom toteutti 2023 Ohjelmistoturvallisuuden tila -selvityksen, jossa myös tarkasteltiin ohjelmistoturvallisuuden koulutusta oppilaitoksissa. Raportti nostaa esille, että *”Ohjelmistoturvallisuus edellyttää kahdenlaista osaamista. On ymmärrettävä tarve turvallisuudelle, esimerkiksi liiketoimintaan kohdistuvien riskien vuoksi. Sen lisäksi on pystyttävä toteuttamaan ohjelmisto turvallisesti suunnittelusta ylläpitoon. Jälkimmäinen osa voidaan jakaa turvallisuustarpeiden määrittelyyn vaatimuksiksi ja niiden ohjelmointiteknistä osaamista edellyttävään toteuttamiseen”* (Kiravuo et al., 2023). Kyseisessä selvityksessä käsiteltiin neljän korkea-asteen oppilaitoksen haastatteluja (yliopistoja tai ammattikorkeakouluja), ja näiden haastatteluiden pohjalta tunnistettiin, että kyberturvallisuus on nykyään osa kaikkia tietotekniikan opintoja, mutta ohjelmistokehityksen turvallisuudessa alalla on aukko. Koska kyseiseen selvitykseen vastanneiden määrä on alhainen, pyritään tässä raportissa toteutetun kyselytutkimuksen kautta täydentämään nykytilannetta yliopistojen osalta ja tunnistamaan mahdollisia syitä sille, miksi tietoturva-aiheiden käsittely osana kursseja on jäänyt vähäiseksi.

Yrityksille suunnatussa kyberturvallisuuskoulutuksen kehittämisen osaamistarvekartoituksessa (Majanoja et al., 2024b) nousi esille erilaisia kyberturvallisuustaitojen kehittämistarpeita. Yritykset odottavat työntekijöiltä vahvaa kyberturvallisuusalan osaamis- ja tietoperustaa sekä kykyä jatkuvaan oppimiseen ja opittujen taitojen soveltamiseen käytännössä. Pehmeät taidot, kuten ymmärrys laajasta kybertoimintaympäristöstä, resilienssiajattelu ja lainsäädännön perusteet, ovat tärkeitä. Keskeisiin odotettuihin teknisiin taitoihin kuuluvat kiristyshaittaohjelmien tuntemus, digitaalinen forensiikka, ohjelmointi- ja skriptaustaidot sekä verkko-osaaminen. Tästä syystä useat toimintamallit opitaan kyberturvallisuuskurssien lisäksi ohjelmoinnin ja ohjelmistotuotannon kurssien

kautta. Yrityskyselyssä nousi esille myös jatkuvan oppimisen tarve ja yhtenä kouluttautumismuotona yritykset arvostivat ammattisertifikaattien suorittamista. Tästä syystä opettajille suunnatussa kyselyssä kartoitetaan myös opettajien omaa ammattisertifikaattien määrää, niiden tarvetta ja näkemyksiä ammattisertifikaattien tarpeellisuudesta.

Yliopistojen tarjoamia kyberturvallisuusalan kurssien sisältöjä tarkasteltiin Turun yliopiston kehittämän arviointityökalun kautta. Arviointityökalussa linkitettiin eurooppalainen kyberturvallisuusroolien avainosaaminen (ENISA, 2022) ja eurooppalainen kyberturvallisuustaksonomia (Nai Fovino et al., 2019) kursseilla käsiteltäviin aiheisiin. Arviointityökalun avulla tehdyssä tutkimuksessa havaittiin taksonomian aiheita, joita käsitellään hyvin vähän Suomen yliopistojen alan koulutuksessa (Majanoja et al., 2024a). Edellä mainitun tutkimuksen tulosten perusteella on nähtävissä, että useat ohjelmoinnin ja ohjelmistotuotannon sisällöt jäävät nykyisin vähäiselle huomiolle kurssien aiheiden ja harjoitusten osalta suomalaisten yliopistojen kyberturvallisuuskoulutustarjonnassa. Näitä ovat mm. tietoturvatestaus- ja validointi, laitteisto- ja ohjelmistomuutosten vaikutusten tunnistaminen tietoturvan hallinnassa, riskien havaitseminen, tietoturva- ja yksityisyydensuojakäytäntöjen noudattaminen, kyvykkyyskypsyysmallit, laitteiden elinkaaren lopun tietoturva- ja yksityisyydensuojaprosessit, tietoturvamittausten validointi- ja vertailukehykset, ohjelmointiympäristöjen tietoturvatuki, hyökkäystekniikat, luottamuksen hallinta digitaalisissa ja fyysisissä omaisuuksissa, reaaliaikainen tietoturvan vahvistaminen sekä rajat ylittävien ja organisaatioiden välisten tapausten koordinointi ja tiedonjakaminen. Koulutuksen kehitysehdotuksena em. tutkimuksessa suositeltiin, että yliopistot lisäävät jatkossa kurssi- ja harjoitustarjontaa, joissa käsitellään turvallisen ohjelmistokehityksen (secure software development) ja turvallisen ohjelmoinnin (secure programming) näkökulmia. Myös erilaiset laadun ja tietoturvan varmennuskäytännöt (assurance practices), jotka kattavat mm. tietoturvatestauksen, voisivat tuoda tarpeellisia näkökulmia ja taitoja.

Tätä raporttia varten toteutetun kyselyn (Liite 1) ensimmäisessä kysymyksessä kartoitetaan vastaajan pääasiallinen työnantajayliopisto. Kysymys 2 (monivalinta) kartoittaa, minkä tasoisia kursseja opettaja opettaa (perus, aine, syventävä). Kysymykset 3 ja 4 (molemmat Kyllä/Ei –tyyppisiä sisältäen mahdollisuuden kirjoittaa myös tarkempi vastaus) kartoittavat opettajien ammattisertifikaatteja sekä heidän näkemyksiänsä ammattisertifikaattien tarpeellisuudesta.

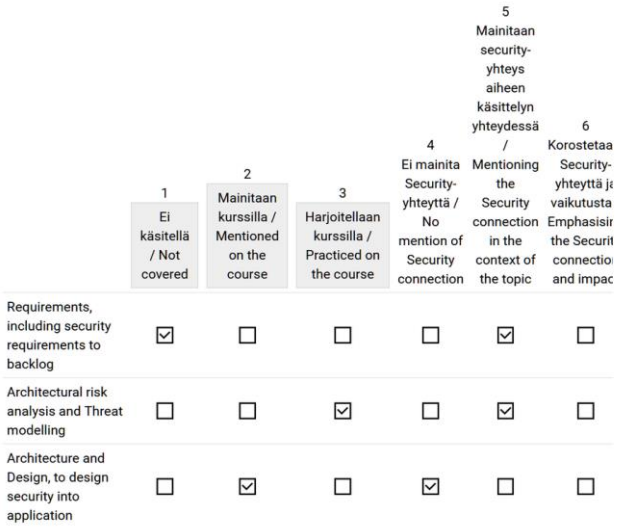
Kysymys 5 kartoittaa, miten hyvin opettaja pystyy tällä hetkellä huomioimaan turvallisen ohjelmoinnin ja/tai turvallisen ohjelmistokehityksen aiheita kurssien suunnittelussa ja toteutuksessa. Kysymys 6 kartoittaa, miten paljon aikaa nykyisissä kursseissa käytetään turvalliseen ohjelmointiin/ohjelmistokehitykseen liittyvien aiheiden käsittelyyn, ja millä tasolla (perus-, aine-, syventävät opinnot).

Kaksi kysymystä kysyy aihetta, jota opettaja opettaa (Kyllä/Ei -vastauksina): kysymys 7: opetatko ohjelmoinnin kursseja, ja kysymys 9: opetatko ohjelmistotuotannon kursseja. Vastaamalla ”Kyllä” avautuvat kysymykset 8 ja 10, jotka tarkentavat ohjelmoinnin ja ohjelmistotuotannon aiheiden käsittelyä tarkemmalla tasolla. Kysymys 8 pohjautuu OWASP:in Secure Programming Practices (OWASP, 2024) -listaukseen, jonka kautta tarkastellaan, miten paljon kurssin aikana ehditään käsitellä turvallisen ohjelmoinnin periaatteita. Kysymyksessä kartoitetaan, millä tasolla kurssilla käsitellään turvallisen ohjelmoinnin periaatteita, ja opettajaa pyydettiin määrittämään kaksi käsittelyn tasoa samasta kysymyksestä (Kuva 1): 1) aiheen käsittely ja 2) tietoturvan yhteys ja vaikutus. Kysymyksessä tarkastellut kategoriat perustuvat OWASP Secure Programming Practices -listaukseen (yhteenä 14 kategoriaa).

	1 Ei käsitellä / Not covered	2 Mainitaan kurssilla / Mentioned on the course	3 Harjoitellaan kurssilla / Practiced on the course	4 Ei mainita Security-yhteyttä / No mention of Security connection	5 Mainitaan security-yhteys aiheen käsittelyn yhteydessä / Mentioning the Security connection in the context of the topic	6 Korostetaan Security-yhteyttä ja vaikutusta / Emphasising the Security connection and impact
Input validation	☑	☐	☐	☑	☐	☐
Output encoding	☐	☑	☐	☐	☑	☐
Authentication and password management	☐	☐	☑	☐	☑	☐

Kuva 1: Kysymyksen 8 käsittelyn taso ja yhteys ohjelmoinnin kursseilla

Kysymys 10 pohjautuu OWASP:in project developer guide – Secure development and integration (OWASP, 2024a) -ohjeistukseen sekä Digi- ja väestötietoviraston Turvallisen ohjelmistokehityksen käsikirjaan (DVV, 2024). Kysymyksessä kartoitetaan, millä tasolla kursseilla käsitellään turvallisen ohjelmistokehityksen periaatteita, ja opettajaa pyydettiin määrittämään kaksi käsittelyn tasoa samasta kysymyksestä (Kuva 2): 1) aiheen käsittely ja 2) tietoturvan yhteys ja vaikutus. Kysymyksessä tarkastellut kategoriat perustuvat OWASP Project developer guide -oppaaseen sekä Digi- ja väestötietoviraston Turvallisen ohjelmistokehityksen käsikirjaan (yhteensä 18 kategoriaa).



	1 Ei käsitellä / Not covered	2 Mainitaan kurssilla / Mentioned on the course	3 Harjoitellaan kurssilla / Practiced on the course	4 Ei mainita Security-yhteyttä / No mention of Security connection	5 Mainitaan security-yhteys aiheen käsittelyn yhteydessä / Mentioning the Security connection in the context of the topic	6 Korostetaa Security-yhteyttä ja vaikutusta Emphasisir the Securit connectio and impac
Requirements, including security requirements to backlog	☑	☐	☐	☐	☑	☐
Architectural risk analysis and Threat modelling	☐	☐	☑	☐	☑	☐
Architecture and Design, to design security into application	☐	☑	☐	☑	☐	☐

Kuva 2: Kysymyksen 10 käsittelyn taso ja yhteys ohjelmistotuotannon kursseilla

Kysymyksien 6–10 täydentävänä kysymyksenä, joka mahdollistaa näkökulmien kirjoittamisen opintoihin (perus, aine, syventävät), on kysymys 11: Kysymyksien 6–10 pohjalta: mitä jää ohjelmoinnin ja ohjelmistokehityksen kursseilta puuttumaan, joka rakentaisi tietoturvaymmärryksen yhteyttä ohjelmistokehittäjille.

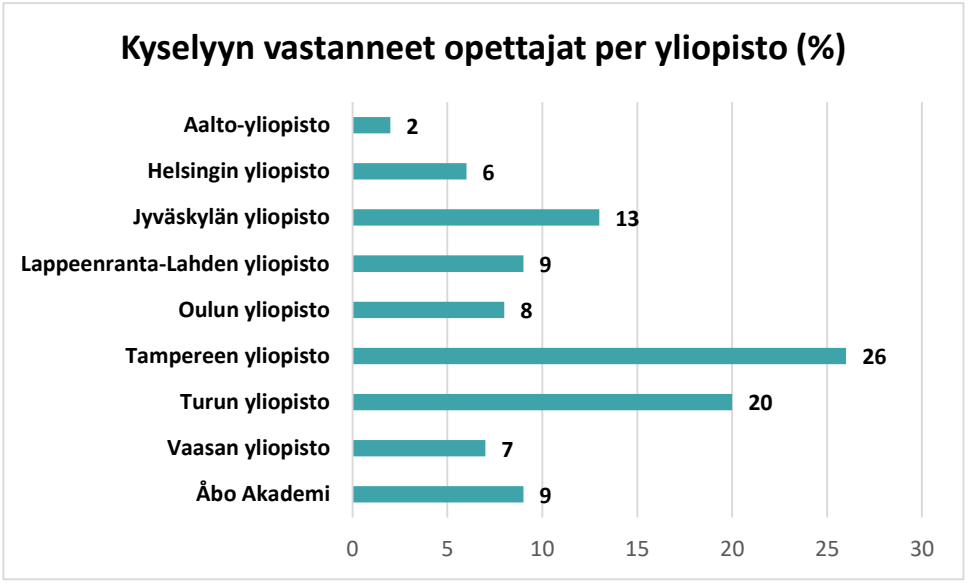
Kysymys 12 kartoittaa haasteita, joita opettajat kokevat tietoturvaan/turvalliseen ohjelmointiin/turvalliseen ohjelmistokehitykseen liittyvien aiheiden opettamisessa. Kysymys on monivalintakysymys, johon opettaja on voinut valita kaikki sopivat vaihtoehdot. Kysymys 13 täydentää aiempaa kysymystä (avoin tekstikenttä) kartoittaen haasteita tai ongelmia, joita opettajat kokevat turvallisen ohjelmoinnin/turvallisen ohjelmistotuotannon opettamisessa kursseilla.

Kysymyksillä 14–16 (valintakysymyksiä valitsemalla yksi vastaus vaihtoehdoista) kartoitetaan, kuinka paljon opettajat ehtivät ylläpitämään tietoturvaan liittyvää tietämystä, seuraamaan uusimpia tietoturvaan liittyviä aiheita sekä sitä, onko uutta tietoa mahdollista sisällyttää kursseihin. Kysymys 14 kartoittaa, miten paljon opettajat ehtivät seuraamaan tietoturva-aiheiden kehitystä ja ylläpitämään aiheeseen liittyvää osaamista. Kysymys 15 kartoittaa, miten tietoturvaopetus näkyy osana nykyistä opetusta. Kysymys 16 antaa opettajille mahdollisuuden kuvata tarkemmin, kysymyksiin 14–15 pohjautuen, vastauksiaan sekä tunnistamiaan haasteita ja tarpeita.

Kysymyksillä 17–20 pyritään tunnistamaan kyberturvallisuuskoulutukseen sekä turvalliseen ohjelmointiin/turvalliseen ohjelmistokehitykseen liittyviä aiheita ja harjoituksia, joita olisi hyvä käsitellä kursseilla kehittämään ohjelmistokehittäjien osaamista. Näitä ajatuksia ja ideoita hyödynnetään myös kansallisen kyberturvallisuuskoulutuksen yhteistyöverkoston rakentamisen kyberturvallisuushankkeessa koulutuksien ja kurssien sisältöjen kehittämisen yhteydessä. Kysymys 17 (avoin kysymys): Ideointia ja tarpeita: Ideaalitilanteessa, mitä turvallisen ohjelmoinnin/turvallisen ohjelmistokehityksen aiheita ohjelmoinnin ja/tai ohjelmistotuotannon kursseilla olisi hyvä opettaa (kurssin taso perus, aine, syventävä). Kysymys 18 (avoin kysymys): Ideointia ja tarpeita: Ideaalitilanteessa, minkälaisia turvallisen ohjelmoinnin/turvallisen ohjelmistokehityksen harjoituksia voisi tuoda osaksi ohjelmoinnin ja ohjelmistokehityksen kursseja. Kysymys 19: Jos olisi tietoturva-aiheisiin liittyvää kurssimateriaalia valmiina tarjolla (luentovideoita, lukumateriaaleja, harjoituksia, tms.), tarjoaisiko niitä opiskelijoille osana kurssia. Lisäksi viimeisenä kysymyksenä Kysymys 20 (avoin kysymys): Muita kommentteja tai asioita, joita opettajat haluavat tuoda esille ja kyberkoulutushankkeen pohdittavaksi.

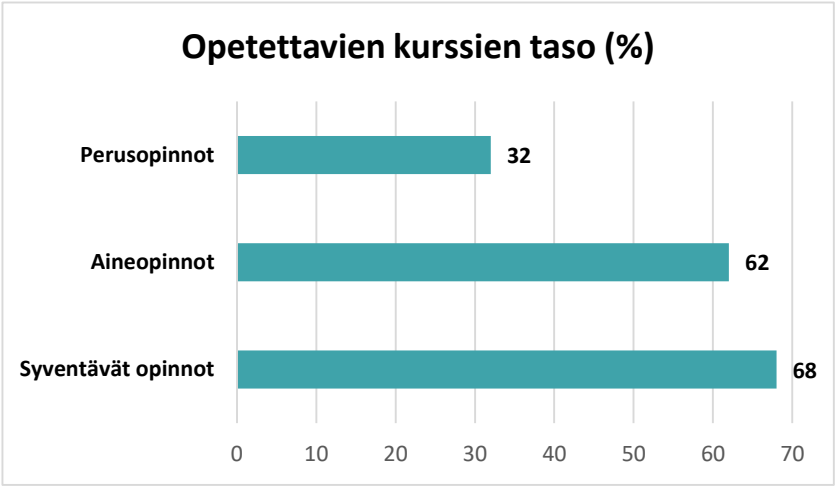
2.2 Kyselyyn vastanneet opettajat ja yliopistot

Kysely lähetettiin kyberturvallisuushankkeeseen osallistuneille yliopistoille ja kysely suunnattiin ohjelmoinnin ja ohjelmistotuotannon opettajille (Kuva 3).



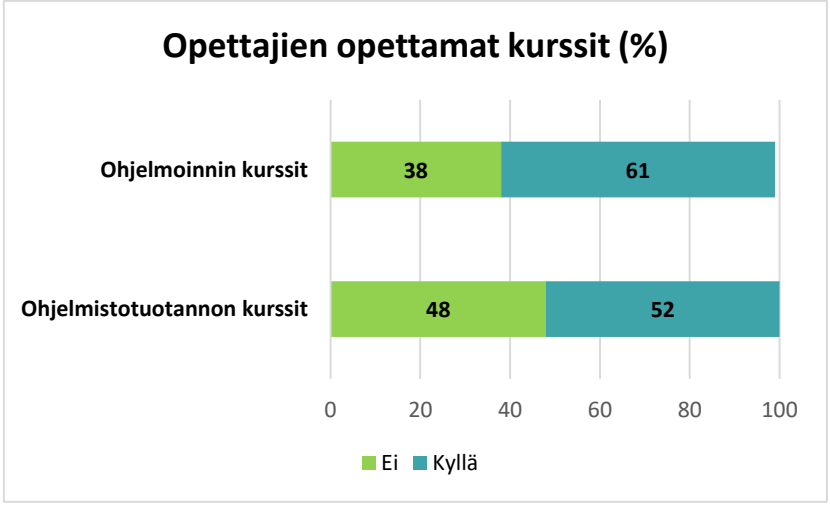
Kuva 3: Kyselyyn vastanneet opettajat per yliopisto (%)

Kyselyyn vastanneet opettajat opettivat pääasiassa aineopintotasoisia (62 %) ja syventävän tasoisia opintoja (68 %) (Kuva 4). Lisäksi perusopintotasoisia kursseja opetti 32 % vastaajista. Kysymys oli monivalintakysymys, jolloin opettajan oli mahdollista vastata opettavansa useampia kursseja eri tasoilla (perusopintoja, aineopintoja ja syventäviä opintoja).



Kuva 4: Kyselyyn vastanneiden opettajien opettamien kurssien taso (%)

Kyselyyn vastanneista opettajista n. 60 % opettaa ohjelmoinnin kursseja ja 52 % ohjelmistotuotannon kursseja (opettajan oli mahdollista vastata opettavansa sekä ohjelmoinnin että ohjelmistotuotannon kursseja) (Kuva 5).



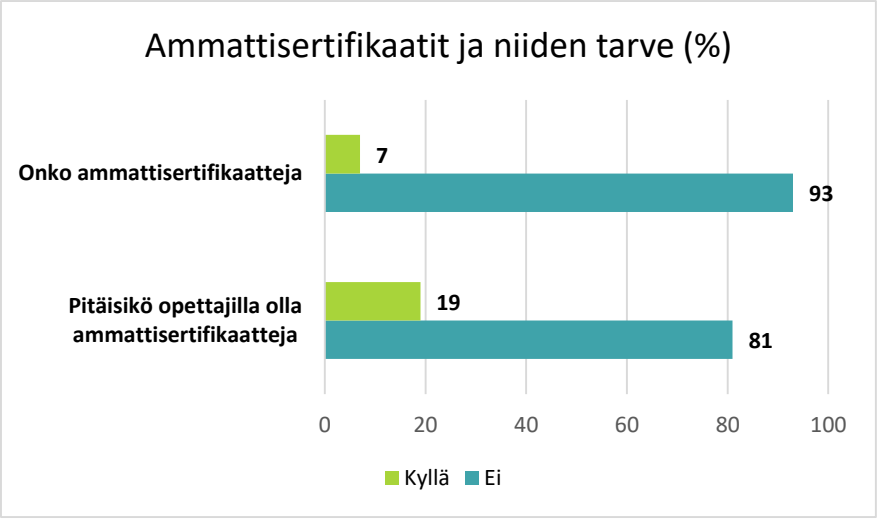
Kuva 5: Opettajien opettamat kurssit (%)

3 Tulokset

Tässä luvussa käsitellään kyselyn (54 vastausta) tuloksia, ja näiden perusteella suoritettuja analyysejä. Kyselyn pohjalta tunnistetaan opettajien esille nostamia kyberturvallisuustaitoja ja -osaamisia, joita olisi hyvä sisällyttää osaksi laajempaa kyberturvallisuusopetusta.

3.1 Opettajien ammattisertifikaattien nykytilanne ja tarve

Kyberturvallisuushankkeen aikana toteutetun yrityskyselyn (Majanoja et al., 2024b) kautta nousi esille jatkuvan oppimisen tärkeys ja tutkintoon valmistumisen jälkeisen osaamisen ylläpitämisen merkitys ICT-alan tehtävissä. Ohjelmointi, ohjelmistotuotanto ja kyberturvallisuus ovat aloja, jotka ovat nopeasti kehittyviä ja muuttuvia, jolloin työelämässä toimivien tulee pysyä ajan tasalla uusimmista muutoksista ja teknisistä kehityksistä. Kuva 6 esittää opettajien ammatti-sertifikaattien määrän ja opettajien kokeman tarpeen ammattisertifikaateille.



Kuva 6: Opettajien ammattisertifikaattien määrä ja tarve (%)

Vastaukset osoittavat, että ohjelmoinnin ja ohjelmistotuotannon opettajilla ei pääsääntöisesti ole ammattisertifikaatteja. Vastauksissa ilmoitetut ammattisertifikaatit olivat: 1) Scrum Master, 2) ISO/IEC 25010 and 29119 trainer -sertifikaatit, 3) Data security-sertifikaatti, ja 4) Lean Six Sigma -sertifikaatti. Osalle ammattisertifikaatit eivät olleet millään tavalla tuttuja, eivätkä jotkut opettajat olleet edes tietoisia ammattisertifikaateista.

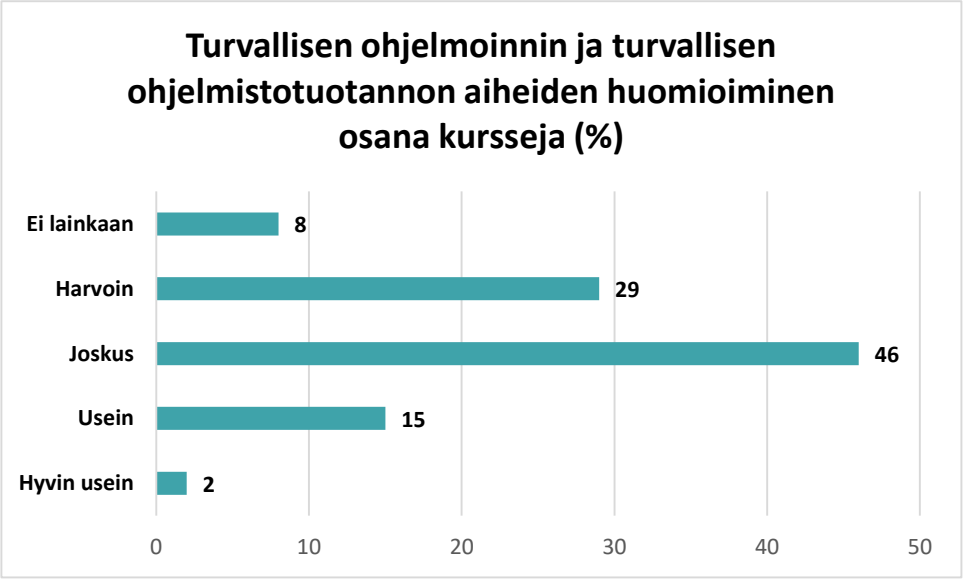
Vastauksista käy ilmi, että yliopisto-opettajien ammattisertifikaattien tarpeesta on varauksellisia näkemyksiä. Moni vastaaja pitää jatkuvaa ammatillista kehittymistä tärkeänä, mutta kokee, ettei sertifiointi ole aina paras tai tarpeellinen tapa sen saavuttamiseen. Useat kommentoivat, että erityisesti kaupallisten toimijoiden tarjoamat sertifikaatit eivät välttämättä tuo lisäarvoa yliopistoympäristössä, koska ne usein keskittyvät tiettyihin tuotteisiin eivätkä laajempaan opetussisältöön. Sen sijaan tietoturvaan liittyvät sertifikaatit, kuten esimerkiksi ISO27001, saattavat olla hyödyllisiä erityisesti opettajille, jotka vastaavat syventävistä tai erikoistuneista kursseista.

Muutamat vastaajat toteavat, että sertifiointi voisi vaikeuttaa opetuksen järjestämistä, erityisesti peruskurssien kohdalla. Peruskursseissa kokemusperäinen osaaminen voi riittää, ja vaikka yliopistojen opetushenkilökunnan jatkuva lisäkoulutus on tarpeellista, se ei vaadi sertifikaatteja. Osa koki, että sertifikaatit olisivat sinänsä hyödyksi, mutta riittävä kokemus ja osaaminen riittää. Osa koki, että koska meillä on yliopistokoulutus, rinnakkaisia järjestelmiä ei tulisi rohkaista. Yliopistoympäristön koetaan nojaavan tutkimusperustaiseen ja ajan hermolla olevaan tietoon, joten sertifikaatit eivät välttämättä tarjoaisi lisäarvoa. Kommenteissa mainittiinkin, että jos opettaja on päteväksi todettu, sertifikaatti ei muuta asiaa. Joissakin tapauksissa, joissa on olemassa viranomaismääräyksiä tai alan käytännön standardeja, sertifikaateista voisi olla hyötyä, mutta tällaiset tilanteet nähdään poikkeuksina. Lisäksi tuli esille myös kommentteja, että vaikka sertifikaatteja ei vaadittaisikaan, olisi hyödyksi ja tarpeellista tuntea sertifikaattien sisältö, jotta niitä pysyy ottamaa esille osana opetusta.

Useat vastaajat myös huomauttivat, että yliopistotyönantajalta ei tällä hetkellä saa tukea sertifikaattien hankintaan, mikä rajoittaa niiden saavutettavuutta tai mahdollisuuksia sertifikaattien suorittamiseen. Jos työnantaja mahdollistaisi sertifikaattien suorittamisen, useampi ilmaisi halukkuutta niiden suorittamiselle. Osa vastaajista kuitenkin tunnistaa, että vaikka sertifikaatit eivät ole välttämättömiä, ne voisivat olla eduksi kyberturvallisuusalan opetuksessa, ohjelmoinnissa ja projektinhallinnassa, ja opettajille olisi hyödyksi olla tietoisia soveltuvien sertifikaattien sisällöistä. Mainintoja saivat esimerkiksi ITIL- ja Scrum-sertifikaatit, jotka pitäisi olla kaikilla ICT-puolen opettajilla. Kokonaisuudessaan sertifikaatit voisivat olla hyödyllisiä joillekin opettajille riippuen heidän opetusalastaan, mutta yleisesti opettajat kokevat, että ne eivät ole välttämättömiä yliopisto-opettajille.

3.2 Turvallisen ohjelmoinnin tai ohjelmistotuotannon käsittely kursseilla

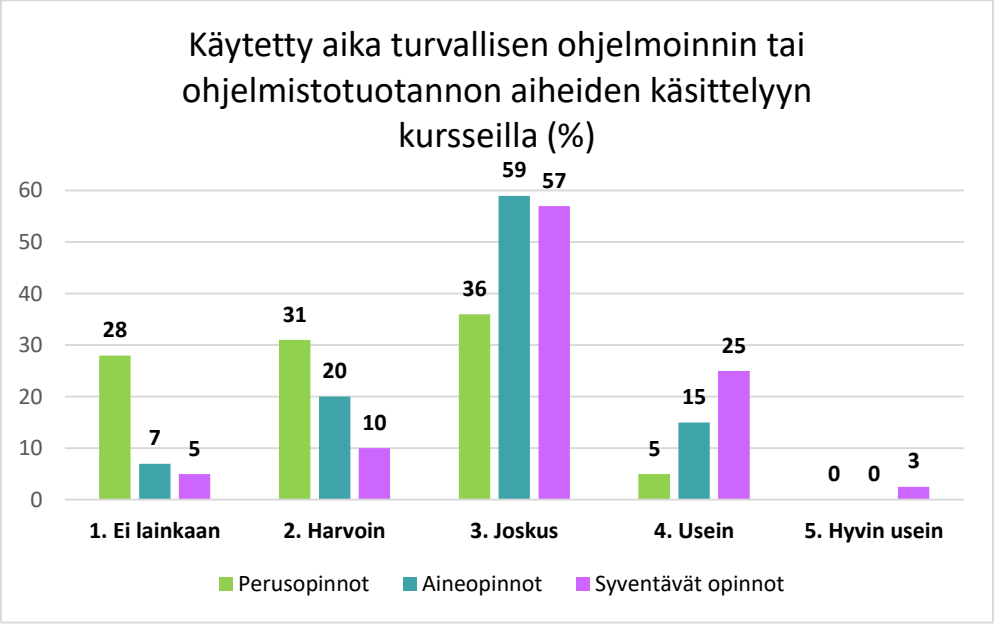
Kysymys 5 kartoitti, miten paljon ohjelmoinnin ja ohjelmistotuotannon opettajat pystyvät huomioimaan turvallisen ohjelmoinnin tai ohjelmistotuotannon aiheita kurssien suunnittelussa ja toteutuksessa. Vastausten pohjalta on havaittavissa, että n. 40 % ei huomioi turvallisen ohjelmoinnin tai ohjelmistotuotannon näkökulmia, n. 46 % pystyy joskus ottamaan huomioon ja vain 17 % huomioi usein turvallisen ohjelmoinnin tai ohjelmistotuotannon näkökulmia osana kurssien suunnittelua ja toteutusta (Kuva 7).



Kuva 7: Turvallisen ohjelmoinnin tai ohjelmistotuotannon aiheiden huomioiminen kurssien suunnittelussa ja toteutuksessa (%)

Sama havainto on löydettävissä, kun tarkasteltiin yliopistojen tarjoamia ohjelmoinnin ja ohjelmistotuotannon kursseja (havainnointi tehtiin samassa yhteydessä, kun koostettiin kyselyn vastaanottajalistaa). Kurssien nimien pohjalta oli mahdollista tunnistaa kaksi kurssia, jotka suoraan kohdistuivat tietoturvanäkökulmiin. Tampereen yliopisto tarjoaa kurssin Secure Programming, 5 op (syventävät opinnot) ja Turun yliopisto tarjoaa kurssin Privacy and Security for Software Systems, 5 op (syventävät opinnot). Muillakin kursseilla tietoturvanäkökulmia nostetaan esille, mutta kurssin nimen perusteella turvallinen ohjelmointi tai ohjelmistokehitys ei tule suoraan esille.

Kysymys 6 pyrki kartoittamaan tarkemmin, miten paljon aikaa kurssien opettajat käyttävät turvalliseen ohjelmointiin/turvalliseen ohjelmistokehitykseen liittyvien aiheiden käsittelyyn perusopintojen, aineopintojen ja syventävien opintojen yhteydessä (Kuva 8). Kyselyn vastauksista on nähtävissä, että varsinkaan perusopinnoissa ei turvallisen ohjelmoinnin ja ohjelmistokehityksen näkökulmia tule esille. Aineopinnoissa ja syventävissä opinnoissa turvallisen ohjelmoinnin tai ohjelmistotuotannon näkökulmia tuodaan joskus esille, mutta ei mitenkään systemaattisesti. Tämä myös viittaa siihen sitä, että turvallisen ohjelmoinnin tai ohjelmistotuotannon näkökulmia ei ole systemaattisesti rakennettu osaksi kursseja ja kurssimateriaaleja. Syventävissä opinnoissa turvallisen ohjelmoinnin tai ohjelmistotuotannon näkökulmia tuodaan esille, mutta ei systemaattisesti.



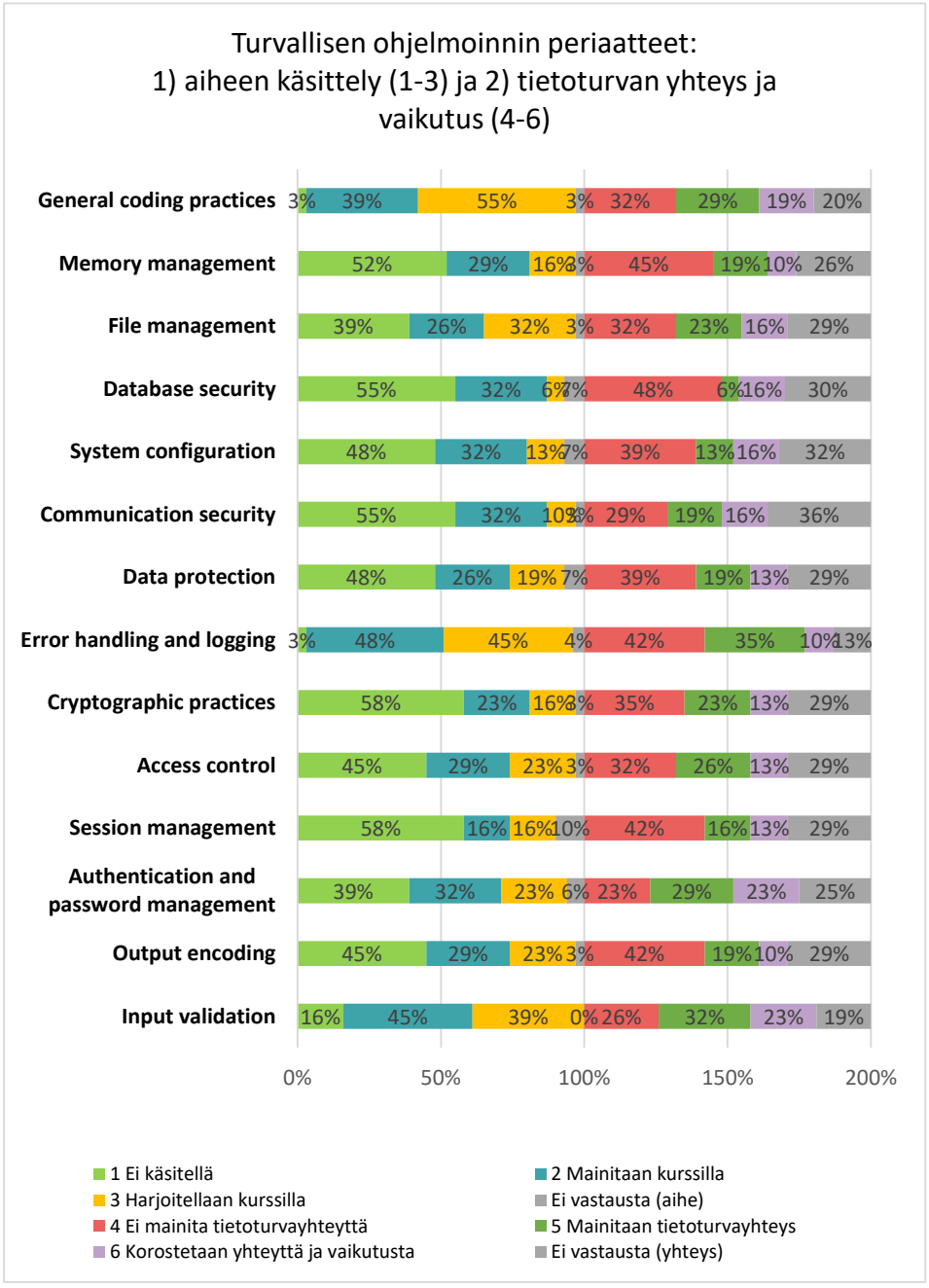
Kuva 8: Turvallisen ohjelmoinnin tai ohjelmistotuotannon aiheiden käsittelyyn käytetty aika kursseilla (%)

3.2.1 Ohjelmoinnin kurssit

Kun tarkastellaan OWASP:in pohjalta koostettuja tietoturvanäkökulmia (Kuva 9), voidaan havaita, että ohjelmoinnin kursseilla (%-arvoja opettajien antamista vastauksista 1) aiheen käsittely kurssilla: ei käsitellä, mainitaan kurssilla, harjoitellaan; 2) tietoturvan yhteyden ja vaikutuksen mainitseminen kurssilla: ei mainita, mainitaan tietoturvayhteys kurssilla, korostetaan tietoturvayhteyttä ja vaikutusta) aiheen käsittelyn yhteydessä ei useinkaan tuoda esille tietoturvaa tai tietoturvayhteyttä. Näiden osalta on merkittävä riski, että opiskelijat eivät ymmärrä tietoturvan vaikutuksia näillä alueilla. Huomioitavaa: osa vastaajista on jättänyt joko molemmat kohdat tai jommankumman täyttämättä. Tämä puuttuva tieto on lisätty kohtiin ”Ei vastausta - aihe” tai ”Ei vastausta – yhteys” (Kuva 9).

Eniten käsiteltyjä aihealueita ovat:

- **General coding practices** (ei käsitellä 3 %, mainitaan kurssilla 39 % ja, harjoitellaan kurssilla 55 %; ei mainita tietoturvayhteyttä 32 %, mainitaan tietoturvayhteys 29 %, korostetaan tietoturvayhteyttä ja vaikutusta 19 %). Tulos osoittaa, että yleiset ohjelmointikäytännöt ovat hyvin keskeisiä kursseilla, mutta aiheen käsittelyn yhteydessä tietoturvayhteyttä ei aina tuoda esille.
- **Error handling and logging** (ei käsitellä 3 %, mainitaan kurssilla 48 % ja, harjoitellaan kurssilla 45 %; ei mainita tietoturvayhteyttä 42 %, mainitaan tietoturvayhteys 35 %, korostetaan tietoturvayhteyttä ja vaikutusta 10 %). Aihetta käsitellään usein kurssilla ja sitä myös harjoitellaan (14 %). Tämä aihealue koetaan tärkeänä tuoda esille ohjelmoinnin kursseilla. Aihe on myös tärkeä tietoturvan kannalta, koska virheenkäsittely ja virhelokien ylläpito auttavat virheiden jäljittämisessä ja turvallisuudessa. Kuitenkin tietoturvayhteyttä ei aina tuoda esille aiheen käsittelyn yhteydessä.
- **Input validation** (ei käsitellä 16 %, mainitaan kurssilla 45 % ja, harjoitellaan kurssilla 39 %; ei mainita tietoturvayhteyttä 26 %, mainitaan tietoturvayhteys 32 %, korostetaan tietoturvayhteyttä ja vaikutusta 23 %). Aihetta käsitellään usein ja sitä myös harjoitellaan kursseilla. Tietoturvan kannalta syötteiden tarkistus on keskeinen tekijä estämään hyökkäyksiä. Tämä yhteys mainitaan usein ja sen vaikutusta myös tuodaan esille. Kuitenkin jonkin verran tämän yhteyden esille tuominen jää puuttumaan aiheen käsittelyn yhteydessä.



Kuva 9: Turvallisen ohjelmoinnin aiheiden käsittely sekä tietoturvan yhteyden ja vaikutuksen huomioiminen kursseilla (%). Akselin 1) aiheen käsittely ja 2) tietoturvan yhteys ja vaikutus ovat molemmat 100 %, jolloin kokonaisprosenttimäärä on 200 %.

Vaihtelevasti käsiteltävät aihealueet ovat:

- **Authentication and password management** (ei käsitellä 39 %, mainitaan kurssilla 32 % ja, harjoitellaan kurssilla 23 %; ei mainita tietoturvayhteyttä 23 %, mainitaan tietoturvayhteys 29 %, korostetaan tietoturvayhteyttä ja vaikutusta 23 %). Aihe mainitaan varsin usein kurssilla ja sitä harjoitellaan (7 %). Lisäksi tietoturvayhteys tuodaan usein esille. Kuitenkin varsin usein aihetta ei käsitellä. Autentikointi ja salasanojen hallinta ovat tietoturvan peruspilareita, joten aiheen syvempi huomioiminen ja esille nostaminen aiheen käsittelyn yhteydessä voisi olla perusteltua.
- **File management** (ei käsitellä 39 %, mainitaan kurssilla 26 % ja, harjoitellaan kurssilla 32 %; ei mainita tietoturvayhteyttä 32 %, mainitaan tietoturvayhteys 23 %, korostetaan tietoturvayhteyttä ja vaikutusta 16 %). Aihe mainitaan kohtalaisesti kurssilla ja sitä myös harjoitellaan, mikä osoittaa, että sen merkitys tunnistetaan. Tiedostohallinta on tärkeä osa tietoturvaa, erityisesti käyttöoikeuksien ja tietojen säilyttämisen näkökulmasta
- **Output encoding** (ei käsitellä 45 %, mainitaan kurssilla 29 % ja, harjoitellaan kurssilla 23 %; ei mainita tietoturvayhteyttä 42 %, mainitaan tietoturvayhteys 19 %, korostetaan tietoturvayhteyttä ja vaikutusta 10 %). Aihealue mainitaan kursseilla kohtalaisen usein, mutta sitä harjoitellaan vähemmän. Vaikka aihe on tärkeä esimerkiksi XSS-hyökkäysten estämisessä, sen käsittely kursseilla on vaihtelevaa. Myös tietoturvayhteyden maininta jää usein puuttumaan.
- **Access control** (ei käsitellä 45 %, mainitaan kurssilla 29 % ja, harjoitellaan kurssilla 23 %; ei mainita tietoturvayhteyttä 32 %, mainitaan tietoturvayhteys 26 %, korostetaan tietoturvayhteyttä ja vaikutusta 13 %). Aihe mainitaan kursseilla ja harjoitellaan jonkin verran, mutta aihetta tai vaikutusta ei käsitellä kovin laajasti. Tämä on tärkeä tietoturva-alue, erityisesti käyttöoikeuksien hallinnan ja valtuutuksen kannalta.
- **Data protection** (ei käsitellä 48 %, mainitaan kurssilla 26 % ja, harjoitellaan kurssilla 19 %; ei mainita tietoturvayhteyttä 39 %, mainitaan tietoturvayhteys 19 %, korostetaan tietoturvayhteyttä ja vaikutusta 13 %). Aihe mainitaan kurssilla ja sitä harjoitellaan jonkin verran, mutta se jätetään usein myös käsittelemättä (15 %). Tietosuojan ja yksityisyyden käsittely on tärkeää varsinkin nykyisten tietosuoja-asetusten, kuten GDPR, näkökulmasta. Tämä aihe voisi hyötyä lisäharjoituksista ja syvällisemmästä käsittelystä kursseilla.
- **System configuration** (ei käsitellä 48 %, mainitaan kurssilla 32 % ja, harjoitellaan kurssilla 13 %; ei mainita tietoturvayhteyttä 39 %, mainitaan

tietoturvayhteys 13 %, korostetaan tietoturvayhteyttä ja vaikutusta 16 %). Aihe mainitaan kursseilla, mutta sitä harjoitellaan. Usein aihe ja siihen liittyvä tietoturvayhteys jää kokonaan käsittelemättä. Systeemikonfiguraatioiden turvallisuus on keskeinen osa turvallista järjestelmähallintaa.

Vähän käsiteltäviä tai harjoiteltavia aihealueita ovat:

- **Memory management** (ei käsitellä 52 %, mainitaan kurssilla 29 % ja, harjoitellaan kurssilla 16 %; ei mainita tietoturvayhteyttä 45 %, mainitaan tietoturvayhteys 19 %, korostetaan tietoturvayhteyttä ja vaikutusta 10 %). Aihe mainitaan vaihtelevasti kurssilla ja harjoitellaan jonkin verran, mutta tietoturvanäkökulma jää kuitenkin kursseilla usein kokonaan käsittelemättä. Muistinhallinnan puutteet voivat johtaa tietoturvaongelmiin, kuten puskurin ylivuotoihin, joten sen syvempi käsittely olisi perusteltua.
- **Session management** (ei käsitellä 58 %, mainitaan kurssilla 16 % ja, harjoitellaan kurssilla 16 %; ei mainita tietoturvayhteyttä 42 %, mainitaan tietoturvayhteys 16 %, korostetaan tietoturvayhteyttä ja vaikutusta 13 %). Aihetta käsitellään ja harjoitellaan vähän, ja tietoturvayhteys jää usein mainitsematta. Session management on tärkeä, koska se estää luvattoman pääsyn käyttäjän tietoihin ja suojaa istuntojen kaappaamiselta.
- **Cryptographic practices** (ei käsitellä 58 %, mainitaan kurssilla 23 % ja, harjoitellaan kurssilla 16 %; ei mainita tietoturvayhteyttä 35 %, mainitaan tietoturvayhteys 23 %, korostetaan tietoturvayhteyttä ja vaikutusta 13 %). Aihe on tärkeä tietoturvan kannalta, koska käytännöt suojaavat arkaluontoisia tietoja estäen luvattoman pääsyn, manipuloinnin ja tietovuodot. Kuitenkin aihetta ei mainita tai aihe jää ilman käsittelyä ohjelmoinnin kursseilla, ja sitä ei useinkaan harjoitella,
- **Communication security** (ei käsitellä 55 %, mainitaan kurssilla 32 % ja, harjoitellaan kurssilla 10 %; ei mainita tietoturvayhteyttä 29 %, mainitaan tietoturvayhteys 19 %, korostetaan tietoturvayhteyttä ja vaikutusta 16 %). Aihe mainitaan vaihtelevasti kurssilla, vaikka aihe on tärkeä, koska se suojaa tietoliikenteen salassa pitämisen, eheyden ja autentikoinnin, estäen tietojen vuotamisen ja väärinkäytön.
- **Database security** (ei käsitellä 55 %, mainitaan kurssilla 32 % ja, harjoitellaan kurssilla 6 %; ei mainita tietoturvayhteyttä 48 %, mainitaan tietoturvayhteys 6 %, korostetaan tietoturvayhteyttä ja vaikutusta 16 %). Aihe mainitaan vaihtelevasti kurssilla, mutta tietoturvayhteyden esille tuominen jää usein puuttumaa. Tämä osoittaa, että tietokantaturvallisuuden osaamista voisi vahvistaa.

Ohjelmoinnin kursseilla yleisiä ohjelmointikäytäntöjä ja syötteiden tarkastusta käsitellään kattavasti. Monet tietoturvan kannalta oleelliset perustekijät saattavat kuitenkin jäävät kursseilla vähemmälle huomiolle joko teoreettisena käsittelynä tai käytännön harjoitteluna. Keskeisiä kehityskohteita olisivat erityisesti tietosuojan, käyttöoikeuksien hallinnan, muistinhallinnan ja autentikoinnin aiheet, jotka voisivat hyötyä laajemmasta ja syvällisemmästä käsittelystä käytännön harjoituksineen. Tämä tukisi opiskelijoiden valmiuksia ymmärtää ja toteuttaa turvallisia ohjelmistokäytäntöjä eri osa-alueilla. Myös monet tietoturvan kannalta keskeiset aiheet, kuten kryptografia, verkkoliikenteen turvallisuus ja istunnon hallinta, saattavat vaatia enemmän huomiota ja käytännön harjoittelua kurssisisällöissä.

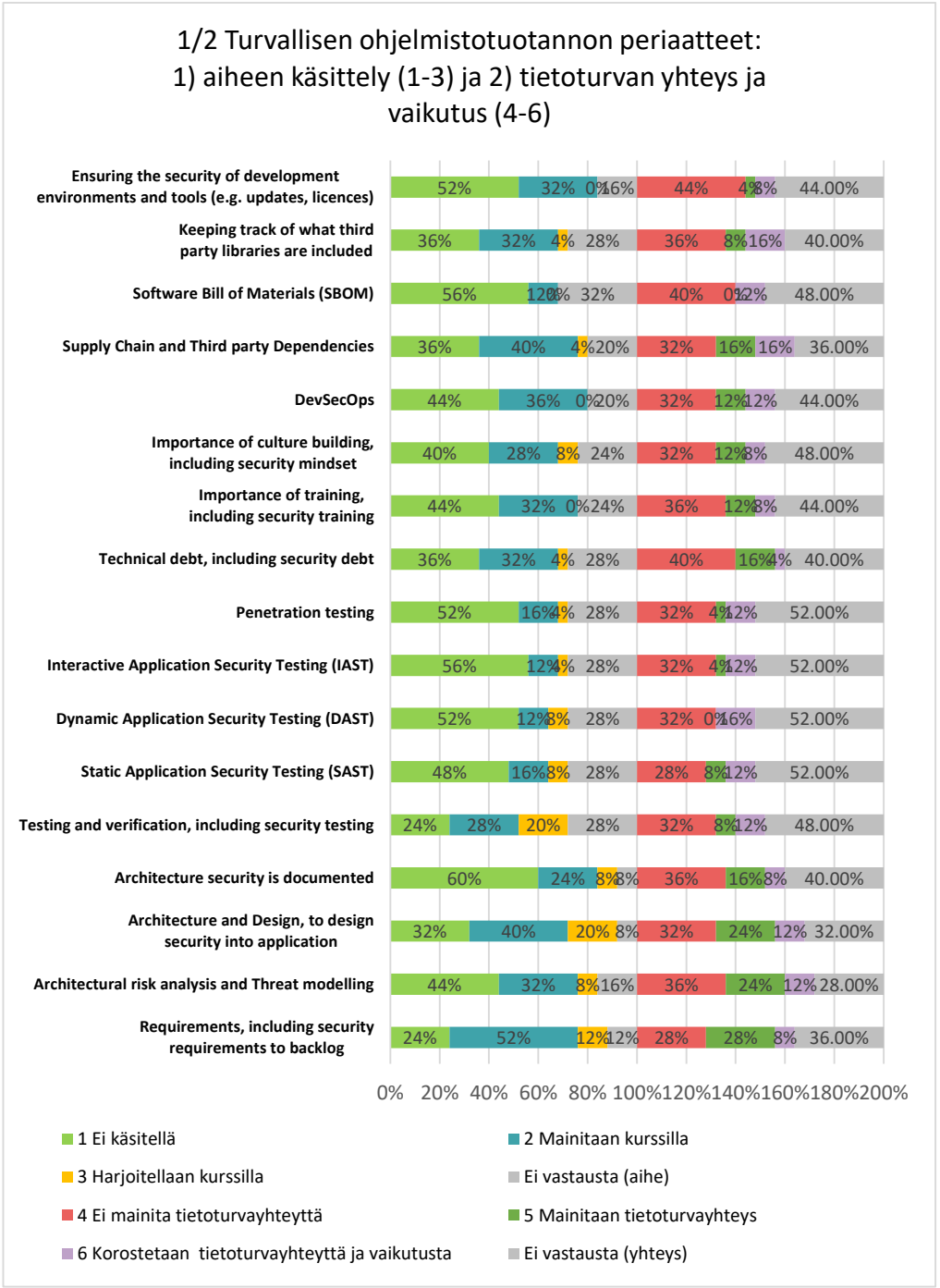
Useilla kursseilla tietoturva-aiheiden turvallisuusyhteys ei tule ilmi lainkaan. Useat vastaajat ovat jättäneet vastaamatta varsinkin tietoturvan yhteyden ja vaikutuksen osioon, joka myös viittaa siihen, että kyseisien aiheiden osalta tietoturvayhteyttä ei tuoda esille. Tietyillä aihealueilla, kuten virheenkäsittelyssä, yleisissä ohjelmointikäytännöissä ja käyttöoikeuksien hallinnassa, turvallisuusyhteys mainitaan, mutta sen merkitystä ei korosteta riittävästi. Vain harvoilla kursseilla tietoturvayhteys on vahvasti korostettu. Esimerkiksi syötteiden validointi ja tunnistautuminen saavat huomiota, mutta muut keskeiset aiheet jäävät vähemmälle huomiolle. Turvallisuutta koskevien vaikutusten ymmärrystä olisi hyvä mahdollisuuksien mukaan lisätä kursseilla. Tämä voisi parantaa opiskelijoiden valmiuksia kohdata tietoturvariskejä ja ymmärtää tietoturvatoimien käytännön merkityksen.

3.2.2 Ohjelmistotuotannon kurssit

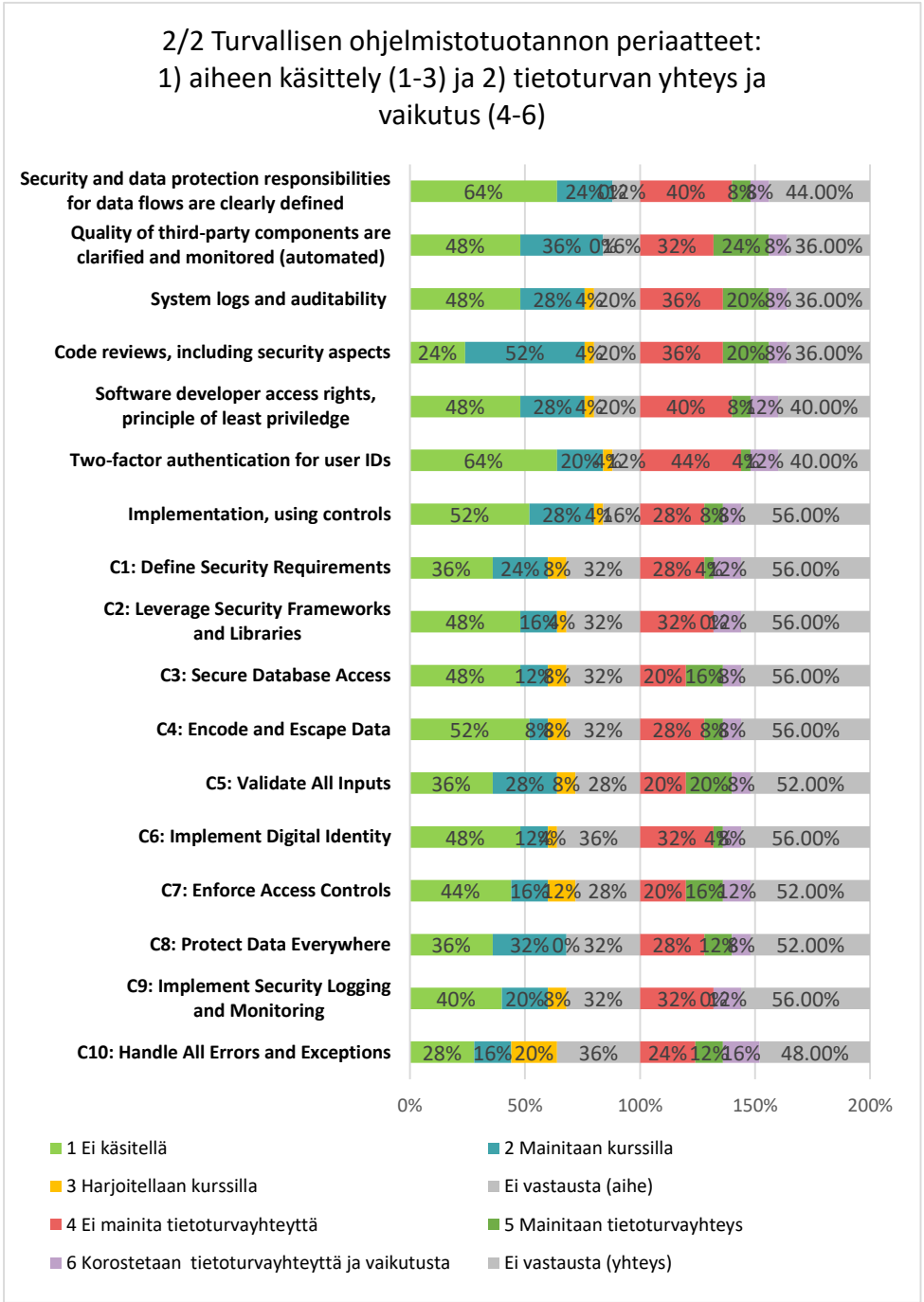
Kun tarkastellaan OWASP:in ja DVV:n pohjalta koostettuja tietoturvanäkökulmia (Kuva 10 ja Kuva 11), voidaan havaita, että ohjelmistotuotannon kursseilla (%-arvoja opettajien antamista vastauksista 1) aiheen käsittely kurssilla: ei käsitellä, mainitaan kurssilla, harjoitellaan; 2) tietoturvan yhteyden ja vaikutuksen mainitseminen kurssilla: ei mainita, mainitaan tietoturvayhteys kurssilla, korostetaan tietoturvayhteyttä ja vaikutusta) aiheen käsittelyn yhteydessä ei useinkaan tuoda esille tietoturvaa tai tietoturvayhteyttä. Näiden aiheiden osalta on merkittävä riski, että opiskelijat eivät ymmärrä tietoturvan vaikutuksia näillä alueilla. Huomioitavaa: osa vastaajista on jättänyt joko molemmat kohdat tai jommankumman täyttämättä. Tämä puuttuva tieto on lisätty kohtiin ”Ei vastausta - aihe” tai ”Ei vastausta – yhteys” (Kuva 10 ja Kuva 11).

Eniten käsiteltyjä aihealueita ovat:

- **Code reviews, including security aspects** (ei käsitellä 24 %, mainitaan kurssilla 52 % ja, harjoitellaan kurssilla 4 %; ei mainita tietoturvayhteyttä 36 %, mainitaan tietoturvayhteys 20 %, korostetaan tietoturvayhteyttä ja vaikutusta 8 %). Koodin tarkistaminen ja verifikaatio turvallisuusnäkökulmasta on esillä kursseilla, mikä on tärkeää turvallisten ohjelmistojen kehityksessä. Aihetta ei kuitenkaan harjoitella ohjelmistotuotannon kursseilla harjoitella.
- **Testing and verification, including security testing** (ei käsitellä 24 %, mainitaan kurssilla 28 % ja, harjoitellaan kurssilla 20 %; ei mainita tietoturvayhteyttä 32 %, mainitaan tietoturvayhteys 8 %, korostetaan tietoturvayhteyttä ja vaikutusta 12 %). Turvallisuustestaus on vaihtelevasti edustettuna kursseilla, joka on laadunvarmistuksen ja tietoturvanäkökulmien integroimista osaksi kehitysprosessia. Kuitenkin merkittävä osa kursseista ei käsittele testausta tai verifikaatiota huomioiden tietoturvanäkökulmat.
- **Requirements, including security requirements to backlog** (ei käsitellä 24 %, mainitaan kurssilla 52 % ja, harjoitellaan kurssilla 12 %; ei mainita tietoturvayhteyttä 28 %, mainitaan tietoturvayhteys 28 %, korostetaan tietoturvayhteyttä ja vaikutusta 8 %). Turvallisuusvaatimusten määrittely ja niiden sisällyttäminen backlogiin on keskeinen aihe, mikä edistää turvallisuuskysymysten huomioimista projektin alusta lähtien.
- **Architecture and Design, to design security into application** (ei käsitellä 32 %, mainitaan kurssilla 40 % ja, harjoitellaan kurssilla 20 %; ei mainita tietoturvayhteyttä 32 %, mainitaan tietoturvayhteys 24 %, korostetaan tietoturvayhteyttä ja vaikutusta 12 %). Suunnittelun ja arkkitehtuurin turvallisuuden käsittely on mukana kursseilla, joka on lähtökohta turvallisten järjestelmien rakentamisessa.



Kuva 10: 1/2 Turvallisen ohjelmistotuotannon aiheiden käsittely sekä tietoturvan yhteyden ja vaikutuksen huomioiminen kursseilla (%). Akselin 1) aiheen käsittely ja 2) tietoturvan yhteys ja vaikutus ovat molemmat 100 %, jolloin kokonaisprosenttimäärä on 200 %.



Kuva 11: 2/2 Turvallisen ohjelmistotuotannon aiheiden käsittely sekä tietoturvan yhteyden ja vaikutuksen huomioiminen kursseilla (%). Akselin 1) aiheen käsittely ja 2) tietoturvan yhteys ja vaikutus ovat molemmat 100 %, jolloin kokonaisprosenttimäärä on 200 %.

Vaihtelevasti käsiteltävät aihealueet. Nämä aiheet mainitaan melko monilla kursseilla, mutta harjoittelu on rajoitettua tai niitä ei käsitellä tietoturvayhteyttä.

- **Supply Chain and Third-party Dependencies** (ei käsitellä 36 %, mainitaan kurssilla 40 %, harjoitellaan kurssilla 4 %; ei mainita tietoturvayhteyttä 32 %, mainitaan tietoturvayhteys 16 %, korostetaan tietoturvayhteyttä ja vaikutusta 16 %). Kolmannen osapuolen riippuvuudet ja toimitusketjun hallinta mainitaan suhteellisen usein, mutta niiden harjoittelua voisi lisätä, sillä nämä ovat keskeisiä tietoturvauhkien hallinnassa.
- **DevSecOps** (ei käsitellä 44 %, mainitaan kurssilla 36 %, harjoitellaan kurssilla 0 %; ei mainita tietoturvayhteyttä 32 %, mainitaan tietoturvayhteys 12 %, korostetaan tietoturvayhteyttä ja vaikutusta 12 %). DevSecOps on huomioitu kursseilla konseptina, mutta käytännön soveltaminen puuttuu. Tämä aihe on erityisen tärkeä jatkuvassa kehitys- ja toimitusprosessissa.
- **Technical debt, including security debt** (ei käsitellä 36 %, mainitaan kurssilla 32 %, harjoitellaan kurssilla 4 %; ei mainita tietoturvayhteyttä 40 %, mainitaan tietoturvayhteys 16 %, korostetaan tietoturvayhteyttä ja vaikutusta 4 %). Teknisen velan ja tietoturvavelan käsite on merkittävä pitkän aikavälin turvallisuuden ja koodin laadun hallinnan kannalta, mutta se on pääosin teoreettisesti käsitelty. Teknisen velan käsittely jää ohjelmistotuotannon kursseilla vähäiseksi.
- **Keeping track of what third party libraries are included** (ei käsitellä 36 %, mainitaan kurssilla 32 %, harjoitellaan kurssilla 4 %; ei mainita tietoturvayhteyttä 36 %, mainitaan tietoturvayhteys 8 %, korostetaan tietoturvayhteyttä ja vaikutusta 16 %). Kolmannen osapuolen kirjastojen seuranta on tärkeää haavoittuvuuksien välttämiseksi.
- **Importance of culture building, including security mindset** (ei käsitellä 40 %, mainitaan kurssilla 28 %, harjoitellaan kurssilla 8 %; ei mainita tietoturvayhteyttä 32 %, mainitaan tietoturvayhteys 12 %, korostetaan tietoturvayhteyttä ja vaikutusta 8 %). Laatukulttuurin, mukaan lukien turvallisuuskulttuurin ja -asenteen, merkitystä käsitellään jonkin verran, mutta kulttuurillisen turvallisuusajattelun kehittäminen jää vähäiseksi, mikä olisi kuitenkin hyödyllistä turvallisuusajattelun juurruttamisessa yritysten käytäntöihin opiskelijoiden siirtyessä työelämään.
- **Importance of training, including security training** (ei käsitellä 44 %, mainitaan kurssilla 32 %, harjoitellaan kurssilla 0 %; ei mainita tietoturvayhteyttä 36 %, mainitaan tietoturvayhteys 12 %, korostetaan tietoturvayhteyttä ja vaikutusta 8 %). Koulutuksen ja osaamisen

ylläpitämisen (esim. jatkuvan oppimisen kautta) tärkeyttä korostetaan ohjelmistotuotannon kurssien aikana varsin vähän. Toki aiheen harjoittelu on haasteellista, mutta aiheen tuominen esille voisi tuoda opiskelijoille paremman käsityksen osaamisen ylläpitämisen tärkeydestä.

- **Architectural risk analysis and Threat modelling** (ei käsitellä 44 %, mainitaan kurssilla 32 %, harjoitellaan kurssilla 8 %; ei mainita tietoturvayhteyttä 36 %, mainitaan tietoturvayhteys 24 %, korostetaan tietoturvayhteyttä ja vaikutusta 12 %). Aihe on tärkeä, koska se auttaa tunnistamaan ja minimoimaan järjestelmän rakenteellisia haavoittuvuuksia ennen toteutusta, mikä parantaa tietoturvaa merkittävästi.

Vähän käsiteltäviä tai harjoiteltavia aihealueita ovat:

- **System logs and auditability** (ei käsitellä 48 %, mainitaan kurssilla 28 %, harjoitellaan kurssilla 4 %; ei mainita tietoturvayhteyttä 36 %, mainitaan tietoturvayhteys 20 %, korostetaan tietoturvayhteyttä ja vaikutusta 8 %). Järjestelmälokien hallinta ja auditoinnin mahdollistaminen ovat tietoturvan tärkeitä komponentteja, mutta aihetta käsitellään varsin vähän. Aihetta voisi vahvistaa lisäämällä harjoittelua, sillä lokit ovat kriittisiä mm. tietoturvapoikkeamien jäljittämisessä.
- **Software developer access rights, principle of least privilege** (ei käsitellä 48 %, mainitaan kurssilla 28 %, harjoitellaan kurssilla 4 %; ei mainita tietoturvayhteyttä 40 %, mainitaan tietoturvayhteys 8 %, korostetaan tietoturvayhteyttä ja vaikutusta 12 %). Pääsynhallinta vähentää tietomurtojen ja haitallisten toimintojen riskiä.
- **Quality of third-party components are clarified and monitored (automated)** (ei käsitellä 48 %, mainitaan kurssilla 36 %, harjoitellaan kurssilla 0 %; ei mainita tietoturvayhteyttä 32 %, mainitaan tietoturvayhteys 24 %, korostetaan tietoturvayhteyttä ja vaikutusta 8 %). Kolmannen osapuolen komponenttien laadun seuranta on tärkeää toimitusketjun turvallisuuden kannalta. Lisäksi olisi tärkeää oppia hyödyntämään automatisointia. Aihetta ei kuitenkaan kursseilla käsitellä. Lisäksi automatisoinnin tuomista osaksi erilaisia harjoituksia voisi lisätä.
- **Static Application Security Testing (SAST)** (ei käsitellä 48 %, mainitaan kurssilla 16 %, harjoitellaan kurssilla 8 %; ei mainita tietoturvayhteyttä 28 %, mainitaan tietoturvayhteys 8 %, korostetaan tietoturvayhteyttä ja vaikutusta 12 %). Staattinen sovellusturvallisuuden testaus on haavoittuvuuksien tunnistamisessa kooditasolla, mutta aihe kaipaisi laajempaa käsittelyä.

- **Dynamic Application Security Testing (DAST)** (ei käsitellä 52 %, mainitaan kurssilla 12 %, harjoitellaan kurssilla 8 %; ei mainita tietoturvayhteyttä 32 %, mainitaan tietoturvayhteys 0 %, korostetaan tietoturvayhteyttä ja vaikutusta 16 %). DAST on dynaamisen testauksen muoto, mutta sitä käsitellään vähän kursseilla.
- **Interactive Application Security Testing (IAST)** (ei käsitellä 56 %, mainitaan kurssilla 12 %, harjoitellaan kurssilla 4 %; ei mainita tietoturvayhteyttä 32 %, mainitaan tietoturvayhteys 4 %, korostetaan tietoturvayhteyttä ja vaikutusta 12 %). IAST on dynaamista testausta syvemmälle menevä testaustapa, mutta sitä käsitellään vähän kursseilla, mikä voi jättää aukkoja turvallisuustestauksen kattavuuteen.
- **Penetration testing** (ei käsitellä 52 %, mainitaan kurssilla 16 %, harjoitellaan kurssilla 4 %; ei mainita tietoturvayhteyttä 32 %, mainitaan tietoturvayhteys 4 %, korostetaan tietoturvayhteyttä ja vaikutusta 12 %). Penetraatiotestausta, osana kokonaistestausta ja validointimenetelmiä, käsitellään jonkin verran, mutta sen käsittely tai harjoittelu osana ohjelmistotuotannon testauksen kursseja on vähäistä. Tämä on kuitenkin tärkeä käytäntö haavoittuvuuksien löytämiseksi tuotantoympäristöistä, mutta kurssin sisältö kuuluu enemmän tietoturvakurssien puolelle kuin yleisiin ohjelmistotuotannon laadunvarmistus- ja testauskäytäntöjen aihealueisiin.
- **Ensuring the security of development environments and tools (e.g., updates, licenses)** (ei käsitellä 52 %, mainitaan kurssilla 32 %, harjoitellaan kurssilla 0 %; ei mainita tietoturvayhteyttä 44 %, mainitaan tietoturvayhteys 4 %, korostetaan tietoturvayhteyttä ja vaikutusta 8 %). Kehitysympäristön ja -työkalujen turvallisuus ei ole laajasti käsitelty aihe, vaikka se on tärkeä osa turvallisuuden varmistamista kaikissa kehitysvaiheissa.
- **Software Bill of Materials (SBOM)** (ei käsitellä 56 %, mainitaan kurssilla 12 %, harjoitellaan kurssilla 0 %; ei mainita tietoturvayhteyttä 40 %, mainitaan tietoturvayhteys 0 %, korostetaan tietoturvayhteyttä ja vaikutusta 12 %). SBOM auttaa seuraamaan sovelluksen komponentteja ja vähentämään toimitusketjun riskejä, mutta tämä on yksi vähiten käsitellyistä aiheista.
- **Architecture security is documented** (ei käsitellä 60 %, mainitaan kurssilla 24 %, harjoitellaan kurssilla 8 %; ei mainita tietoturvayhteyttä 36 %, mainitaan tietoturvayhteys 16 %, korostetaan tietoturvayhteyttä ja vaikutusta 8 %). Arkkitehtuurin tietoturvan dokumentointi jää vähälle huomiolle, vaikka se olisi tärkeä osa tietoturvallisuuden ylläpitoa ja suunnittelua.

- **Two-factor authentication for user IDs** (ei käsitellä 64 %, mainitaan kurssilla 20 %, harjoitellaan kurssilla 4 %; ei mainita tietoturvayhteyttä 44 %, mainitaan tietoturvayhteys 4 %, korostetaan tietoturvayhteyttä ja vaikutusta 12 %). Monivaiheista tunnistautumista käsitellään vain harvoilla kursseilla, vaikka se on tärkeä tietoturvakäytäntö käyttäjien turvallisuuden takaamiseksi.
- **Security and data protection responsibilities for data flows are clearly defined** (ei käsitellä 64 %, mainitaan kurssilla 24 %, harjoitellaan kurssilla 0 %; ei mainita tietoturvayhteyttä 40 %, mainitaan tietoturvayhteys 8 %, korostetaan tietoturvayhteyttä ja vaikutusta 8 %). Tietovirtojen turvallisuusvastuiden selkeyttäminen on osa tietosuojakäytäntöjä, mutta jää vähälle huomiolle kursseilla.

Implementation, using controls ja sen alakohdat (C1-C10) ovat kokonaisuutena laajalti mainittu aihealue ohjelmistoturvallisuudessa, mutta harjoittelu jää usein vähäiseksi:

- **Implementation, using controls** (ei käsitellä 52 %, mainitaan kurssilla 28 %, harjoitellaan kurssilla 4 %; ei mainita tietoturvayhteyttä 28 %, mainitaan tietoturvayhteys 8 %, korostetaan tietoturvayhteyttä ja vaikutusta 8 %). Kontrollien käyttö ohjelmistototeutuksessa on marginaalinen osa kurssien sisältöä, eikä siihen ole riittävästi aikaa ja resursseja käytännön harjoittelun osalta.
- **C1: Define Security Requirements** (ei käsitellä 36 %, mainitaan kurssilla 24 %, harjoitellaan kurssilla 8 %; ei mainita tietoturvayhteyttä 28 %, mainitaan tietoturvayhteys 4 %, korostetaan tietoturvayhteyttä ja vaikutusta 12 %). Tämä vaihe on kuitenkin tärkeä tietoturvallisten ohjelmistojen kehityksen alkuvaiheessa, sillä se määrittää ohjelmiston tietoturvatavoitteet.
- **C2: Leverage Security Frameworks and Libraries** (ei käsitellä 48 %, mainitaan kurssilla 16 %, harjoitellaan kurssilla 4 %; ei mainita tietoturvayhteyttä 32 %, mainitaan tietoturvayhteys 0 %, korostetaan tietoturvayhteyttä ja vaikutusta 12 %). Tämä osa-alue keskittyy olemassa olevien tietoturvakehysten ja kirjastojen hyödyntämiseen ohjelmistokehityksessä.
- **C3: Secure Database Access** (ei käsitellä 48 %, mainitaan kurssilla 12 %, harjoitellaan kurssilla 8 %; ei mainita tietoturvayhteyttä 20 %, mainitaan tietoturvayhteys 16 %, korostetaan tietoturvayhteyttä ja vaikutusta 8 %). Tietokantayhteyksien suojaus on keskeinen osa ohjelmiston tietoturvaa, sillä se estää tunkeutumiset ja tietovuodot tietokannasta.
- **C4: Encode and Escape Data** (ei käsitellä 52 %, mainitaan kurssilla 8 %, harjoitellaan kurssilla 8 %; ei mainita tietoturvayhteyttä 28 %, mainitaan tietoturvayhteys 8 %, korostetaan tietoturvayhteyttä ja vaikutusta 8 %).

Tietojen koodaus ja erikoismerkkien käsittely suojaa esimerkiksi SQL- ja XSS-hyökkäyksiltä.

- **C5: Validate All Inputs** (ei käsitellä 36 %, mainitaan kurssilla 28 %, harjoitellaan kurssilla 8 %; ei mainita tietoturvayhteyttä 20 %, mainitaan tietoturvayhteys 20 %, korostetaan tietoturvayhteyttä ja vaikutusta 8 %). Syötteiden validointi on tärkeä tietoturvatoimenpide, joka estää haitallisen tiedon käsittelyn.
- **C6: Implement Digital Identity** (ei käsitellä 48 %, mainitaan kurssilla 12 %, harjoitellaan kurssilla 4 %; ei mainita tietoturvayhteyttä 32 %, mainitaan tietoturvayhteys 4 %, korostetaan tietoturvayhteyttä ja vaikutusta 8 %). Tämä käsittää käyttäjän digitaalisen identiteetin hallinnan, mukaan lukien tunnistautuminen ja käyttäjätunnusten hallinta.
- **C7: Enforce Access Controls** (ei käsitellä 44 %, mainitaan kurssilla 16 %, harjoitellaan kurssilla 12 %; ei mainita tietoturvayhteyttä 20 %, mainitaan tietoturvayhteys 16 %, korostetaan tietoturvayhteyttä ja vaikutusta 12 %). Pääsynhallinta on keskeinen keino rajoittaa käyttäjien oikeuksia ja suojata arkaluontoista tietoa.
- **C8: Protect Data Everywhere** (ei käsitellä 36 %, mainitaan kurssilla 32 %, harjoitellaan kurssilla 0 %; ei mainita tietoturvayhteyttä 28 %, mainitaan tietoturvayhteys 12 %, korostetaan tietoturvayhteyttä ja vaikutusta 8 %). Tietojen suojaaminen kaikissa vaiheissa, kuten siirron ja tallennuksen aikana, on kriittinen tietoturvatoimenpide.
- **C9: Implement Security Logging and Monitoring** (ei käsitellä 40 %, mainitaan kurssilla 20 %, harjoitellaan kurssilla 8 %; ei mainita tietoturvayhteyttä 32 %, mainitaan tietoturvayhteys 0 %, korostetaan tietoturvayhteyttä ja vaikutusta 12 %). Lokien ja valvonnan avulla voidaan tunnistaa tietoturvaloukkaukset ja epäilyttävät toiminnot.
- **C10: Handle All Errors and Exceptions** (ei käsitellä 28 %, mainitaan kurssilla 16 %, harjoitellaan kurssilla 20 %; ei mainita tietoturvayhteyttä 24 %, mainitaan tietoturvayhteys 12 %, korostetaan tietoturvayhteyttä ja vaikutusta 16 %). Virheiden ja poikkeusten käsittely vähentää tietoturva-aukkojen riskiä ja parantaa ohjelmiston toimintavarmuutta.

Tietoturvayhteyden käsittely ohjelmistotuotannon kursseilla vaihtelee suuresti eri aihealueiden osalta. Vastaajista n. puolet on jättänyt vastaamatta varsinkin tietoturvan yhteyden ja vaikutuksen osioon, joka viittaa siihen, että kyseisien aiheiden osalta tietoturvayhteyttä ja vaikutusta ei tuoda esille. Monet keskeiset aihealueet, kuten monivaiheinen tunnistautuminen, kehitysympäristöjen turvallisuus ja ohjelmistokehittäjien käyttöoikeudet, eivät juuri tule ohjelmistotuotannon kursseilla esille. Tämä voi osoittaa puutteita erityisesti käytännön tietoturvakäytäntöjen integroinnissa, mikä voi johtaa siihen, että opiskelijat eivät saa riittäviä valmiuksia riskien hallintaan. Joidenkin aiheiden tietoturvayhteys mainitaan teoreettisella tasolla, mutta siihen ei syvennytä käytännön sovellusten kautta. Esimerkiksi

kooditarkastusten ja kolmannen osapuolen riippuvuuksien hallinnan yhteydessä saatetaan mainita yhteys tietoturvaan, mutta nämä aiheet eivät välttämättä saa riittävästi huomiota konkreettisina tietoturvatoimenpiteinä. Joissakin aiheissa, kuten kolmannen osapuolen kirjastojen seurannassa ja hyökkäystestauksessa, tietoturva korostuu. Näitä aiheita käsitellään kuitenkin vähän. Vaikka tietoturva mainitaan monissa ohjelmistotuotannon kursseilla käsiteltävissä aiheissa, sen käsittely on usein pinnallista, ja konkreettinen harjoittelua puuttuu. Nykyinen painotus ei välttämättä takaa, että opiskelijat ymmärtäisivät tietoturvan yhteyden ohjelmistokehityksen aktiviteettien yhteydessä, jossa tietoturva integroituu eri osa-alueisiin antaen valmiuksia kehittää turvallisia ohjelmistoja.

Ohjelmoinnin ja ohjelmistotuotannon kursseilla tietoturvanäkökulmat käsitellään varsin vaihtelevasti, mutta kummassakin mahdollisia kehityskohteita tietoturva-yhteyden vahvistamiseksi. Ohjelmoinnin kursseilla keskeiset aiheet, kuten syötteiden validointi, virheenkäsittely, ja yleiset ohjelmointikäytännöt, saavat enemmän huomiota. Ohjelmistotuotannon kursseilla puolestaan käsitellään enemmän laajempia, kehitysprosessiin kuuluvia tietoturvan osa-alueita, kuten kolmannen osapuolen riippuvuudet, toimitusketjun hallinta, ja vaatimusten määrittely.

- Ohjelmoinnin kursseilla tietoturvan käsittely keskittyy enemmän ohjelmoinnin turvallisiin käytäntöihin (esim. virheenkäsittely, syötteiden validointi). Tietoturvayhteyttä ei kuitenkaan aina mainita kattavasti.
- Ohjelmistotuotannon kursseilla tietoturvayhteys saatatetaan mainita osana kehitysprosessin vaiheita, mutta usein tämä jää täysin käsittelemättä. Ohjelmistotuotannon kursseilla tietoturvan näkökulmat kohdistuvat eniten prosessin hallintaan ja arkkitehtuuriin liittyviin kysymyksiin, kuten toimitusketjun turvallisuus ja tietoturvavaatimusten määrittely. On kuitenkin huomioitava, että ohjelmistotuotannon kursseja on hyvin monenlaisia (vrt. ohjelmointi), jolloin tietoturvanäkökulman ottaminen osaksi aiheen käsittelyä voi olla haastavaa. Tästä syystä OWASP:in tai DVV:n turvallisen ohjelmistotuotannon näkökulmat eivät välttämättä nouse edes esille kurssien sisällöissä.
- Monet tietoturvayhteydet jäävät mainitsematta tai pinnallisiksi. Ohjelmoinnin kursseilla muistinhallinta, tiedostojen hallinta, ja kryptografiset käytännöt jäävät vähemmälle huomiolle, vaikka nämä ovat tärkeitä tietoturvauhkien ehkäisemiseksi Ohjelmistotuotannon kursseilla kaksivaiheinen tunnistautuminen, kehitysympäristön turvallisuus, ja arkkitehtuurin tietoturvan dokumentointi jäävät usein käsittelemättä, vaikka ne ovat keskeisiä ohjelmiston tietoturvan kannalta.

Ohjelmoinnin ja ohjelmistotuotannon kursseilla on eroja tietoturvanäkökulmien käsittelyssä. Ohjelmoinnin opetuksessa tietoturvayhteys on vahvempi käytännön ohjelmointikäytännöissä, mutta laajemmat järjestelmätason turvallisuusaiheet jäävät vähemmälle. Ohjelmistotuotannon opetuksessa käsitellään enemmän tietoturvaa vaatimusten, prosessien ja arkkitehtuurin tasolla, mutta käytännön toteutus jää vähemmälle. Kummankin osa-alueen tietoturvaopetusta voitaisiin vahvistaa syvemmällä tietoturvayhteyden korostamisella.

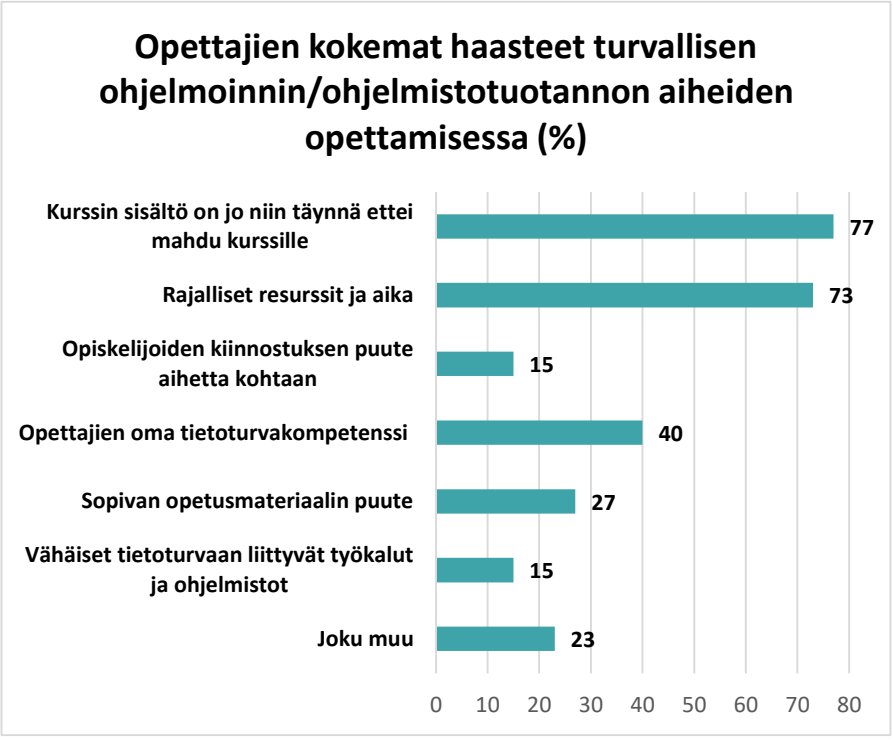
Tietoturva-aiheiden lisääminen nykyisiin kursseihin voi olla haasteellista. Tietoturvateemojen laaja-alaisuuden vuoksi erilliset Secure Programming ja Secure Software Development -kurssit voisivat olla hyödyllisiä opiskelijoille, jolloin he pystyisivät integroimaan tietoturvaosaamisen kokonaiskuvaan. Tällainen malli antaisi opiskelijoille valmiuksia kohdata käytännön tietoturvahaasteita ohjelmistokehityksessä, ja niiden sisällyttäminen opetussuunnitelmaan voisi lisätä koulutuksen arvoa ja relevanssia työelämän näkökulmasta.

Tietoturvaosaaminen on oma eritysalansa, joka vaatii aiheeseen perehtyneisyyttä. Erilliset tietoturvakurssit mahdollistaisivat syvällisemmän käsittelyn, jossa voitaisiin pureutua käytännön harjoituksiin, tietoturvateknologioihin ja teoreettisiin käsitteisiin, jolloin muiden kurssien sisällöt ja tavoitteet eivät vaarantuisi, joita perinteisten ohjelmointi- tai ohjelmistotuotantokurssien sisältöjen laajentaminen saattaisi aiheuttaa (mm. aikataulupaineet, jos jotain lisätään, niin se on jotain toisesta aiheesta pois). Tällaisissa kursseissa voisi kattaa kokonaisvaltaisesti tietoturvan perustaidot ohjelmointiin ja ohjelmistotuotannon näkökulmista sekä toteuttaa käytännön tietoturvaharjoitukset. Perusohjelmointikurssit voivat säilyä ytimekkäinä ja keskittyä ydinasioihin, kun taas tietoturvasta kiinnostuneet tai siihen suuntautuvat opiskelijat voivat syventää osaamistaan tietoturvan erityispiirteisiin erillisillä kursseilla.

Nykyään tietoturvataidot ovat tärkeitä lähes jokaisella ohjelmistokehityksen alalla, joten erilliset kurssit voivat tuoda esiin erityisosaamista, josta on hyötyä työmarkkinoilla. Secure Programming -kurssi voisi keskittyä turvallisiin ohjelmointikäytäntöihin ja uhkien torjumiseen kooditasolla, kun taas Secure Software Development -kurssi kattaisi tietoturvan koko ohjelmistokehityksen elinkaaren ajan. Tällöin erilliset tietoturvakurssit voisivat joustavasti mukautua uusiin uhkiin ja työkaluihin sekä käytäntöihin ilman, että muiden kurssien sisältöä tarvitsee jatkuvasti päivittää tai muuttaa.

3.3 Opettajien kokemat haasteet ja mitä jää puuttumaan ohjelmoinnin tai ohjelmistotuotannon kursseilta

Opettajat kokevat useita merkittäviä haasteita tietoturvanäkökulmien integroimisessa ohjelmoinnin ja ohjelmistotuotannon kursseille (Kuva 12). Suurin osa opettajista (77 %) kokee, että kurssien nykyinen sisältö on jo niin täynnä, ettei tietoturva-aiheiden lisääminen ole mahdollista ilman, että jokin muu sisältö jää pois. Lisäksi 73 % mainitsi aikarajoitteet ja resurssipulan ongelmaksi, mikä tekee tietoturvan syvällisen käsittelyn vaikeaksi kurssiaikatauluissa. Opettajien mukaan monet opiskelijat ovat aloittelijoita, eikä heillä ole tarpeeksi perustietoja ohjelmoinnista tai järjestelmien toiminnasta, jotta he ymmärtäisivät tietoturvan perusperiaatteita. Esimerkiksi puskurin ylivuotojen tai syötteiden turvallisen käsittelyn opettaminen voi olla haastavaa, kun opiskelijoilla ei ole taustatietoa niiden merkityksestä. Opettajien mukaan on haastavaa liittää tietoturva luontevasti kurssin muuhun substanssiin, koska tietoturva on monesti itsenäinen aihealue. Erityisesti ohjelmoinnin peruskursseilla tietoturva ei aina tunnu istuvan kurssin ytimeen, jossa keskiössä ovat perustason ohjelmointitaidot.



Kuva 12: Opettajien kokemat haasteet turvallisen ohjelmoinnin/ohjelmistotuotannon aiheiden opettamisessa (%)

Noin 40 % opettajista mainitsi oman tietoturvaosaamisensa rajallisuuden haasteeksi. Tähän vaikuttaa se, että tietoturva on oma erityisaiheensa, joka vaatii syvällistä perehtyneisyyttä. Kuitenkin ohjelmoinnin ja ohjelmistotuotannon opettajat joutuvat pitämään itsensä ajan tasalla monista muistakin aiheista, kuten ohjelmointityökalujen kehitys, prosessien ja käytäntöjen kehittyminen. Opettajat myös seuraavat useita aihealueita, jolloin tietoturva on vain yksi aihe monien muiden joukossa, mukaan lukien laatu, yksityisyys, käytettävyys, kestävyys, vihreät näkökulmat, jne., jotka myös liittyvät omaan alaan ja opetettavaan aihealueeseen. Lisäksi 27 % kokee, että sopivien opetusmateriaalien puute vaikeuttaa tietoturvan integrointia kurssisisältöihin. Tietoturvaharjoitusten toteuttaminen esimerkiksi penetraatiotestauksen ja verkkoliikenteen analysoinnin muodoissa vaatisi erityisiä laite- ja verkkoympäristöjä, ja yliopistojen yhteiset verkot ja rajoitetut resurssit tekevät tällaisten harjoitusten järjestämisestä haastavaa.

”Joku muu” -kohdan avoimissa vastauksissa nousi esille, että perusopintojen tasolla opettajat kokevat tietoturva-aiheiden syvällisen käsittelyn olevan haastavaa, koska opiskelijat ovat vasta aloittamassa ohjelmoinnin perusteiden oppimista. Yleisesti koetaan, että opiskelijoilla ei vielä ole riittäviä taitoja ymmärtää tietoturvan monimutkaisia peruskäsitteitä. Opettajat nostivatkin esille, että "*Kurssi keskittyy ohjelmointiin, ei tietoturvaan. Jos et osaa ohjelmoida, ei ole hyötyä puhua tietoturvallisesta ohjelmoinnista*." Opettajat toteavatkin, että peruskurssit ovat "neutraaleja ja geneerisiä" ja että tietoturvan lisääminen näihin kursseihin olisi mahdollista vain, jos kurssivalikoimaa tarkastellaan strategisesti kokonaisuutena.

Aineopinnoissa opiskelijat ovat edenneet pidemmälle, ja tietoturva-aiheiden lisääminen onkin luontevampaa. Kuitenkin monet opettajat kokevat haasteita aineopintojen kurssisisältöjen suhteen. Koska kurssit ovat jo valmiiksi laajoja, tietoturvan lisääminen vaatisi joidenkin muiden sisältöjen poistamista tai uudelleenjärjestelyä. Lisäksi opettajat toivat esille, että kursseille olisi samalla tavalla tarvetta lisätä muitakin erilaisia näkökulmia (toiveita lisäämiselle esitetty esimerkiksi laitoksen tai oppiaineen taholta), kuten laatu, yksityisyys, kestävyys, tekoäly, jne., mutta näiden lisääminen on samalla tavalla erittäin haasteellista kuin tietoturva-aiheiden lisääminen, koska ”*jos jotain lisätään niin jotain pitää myös ottaa pois*”.

Opettajat mainitsivat myös, että opiskelijoiden taustatiedot ja osaaminen ovat hyvin erilaisia, mikä tekee tietoturva-aiheiden käsittelystä haastavaa. Erityisesti mainittiin, että osa opiskelijoista saattaa olla kiinnostunut syvällisemmästä tietoturvasta, kuten salausalgoritmeista, kun taas toisia kiinnostaa enemmän tietoturva osana ohjelmistoprosesseja. Tämän vuoksi tietoturvan käsittely kurssilla voi jäädä pintapuoliseksi.

Syventävien opintojen kohdalla opettajat kokevat, että opiskelijat ovat valmiita oppimaan tietoturvan käytäntöjä ja konsepteja. Useat opettajat ehdottavat erillistä kurssia tietoturvallisesta ohjelmistokehityksestä, joka voisi keskittyä

uhkamallinnukseen, penetraatiotestaukseen ja arkkitehtuuritason tietoturvaan. Kuitenkin tähän liittyy haasteita, kuten sopivan opetusmateriaalin ja resurssien puute. Opettajat mainitsivat tämän rajoitteen suoraan: *"Aika ei riitä sen syvälliseen läpikäyntiin, kun kurssien ydinmateriaali vie suurimman osan ajasta."*

Kysymykseen ”Mitä mielestäsi jää ohjelmoinnin ja ohjelmistokehityksen kursseilta puuttumaan, joka rakentaisi tietoturvaymmärryksen yhteyttä ohjelmistokehittäjille” vastauksista käy ilmi, että ohjelmoinnin ja ohjelmistotuotannon kursseilta puuttuu merkittäviä tietoturvayhteyksiä. Esille tulikin, että ”*Käytäntö jää helposti olemattomaksi, sillä tietoturvakomponentti vaatii tietynlaisen osaamistason sen sovelluskohteesta, eikä välttämättä yksittäisen kurssin aikana sopivaa tasoa saavuteta, varsinkin jos tietoturvalle pitää uhrata osa ajasta. Tällöin tietoturva jää hieman teoreettiselle tasolle, eikä sitä välttämättä osata yhdistää kurssin muihin teemoihin kovin tiiviisti.*” Eri opintotasojen (perusopinnot, aineopinnot ja syventävät opinnot) välillä ilmenee erityisiä haasteita ja kehittämisalueita, joiden avulla tietoturvaymmärrystä voitaisiin vahvistaa. Opettajien avoimissa vastauksissa tuotiin esiin havaintoja sekä konkreettisia ehdotuksia ja haasteita tietoturvan integroinnissa osaksi kurssisisältöjä.

Perusopintojen osalta useat vastaajat kommentoivat, että tietoturva-asioiden käsittely on hyvin rajallista, ja monet peruskurssit keskittyvät pääasiassa ohjelmoinnin ydintaitoihin. Opettajat kokivat, että tietoturva-aiheiden syvällinen käsittely saattaisi olla tässä vaiheessa haastavaa ja mahdollisesti liian vaativaa opiskelijoille, koska heiltä puuttuu perusosaaminen ja eivät pysty vielä liittämään tietoturva-aiheita laajempaan kokonaiskuvaan.

Moni opettaja mainitsi, että tietoturva-aiheita ei käsitellä perusopinnoissa juuri lainkaan. Vastauksista löytyi useampia mainintoja, että *"Perusopinnoissa emme taida puhua näistä lainkaan. Kaikki jää puuttumaan."* Tämä osoittaa, että tietoturvaan liittyviä aiheita ei juurikaan tuoda esiin ohjelmoinnin perusteissa. Useampi vastaaja oli sitä mieltä, että tietoturva-aspektien tuominen perusopintoihin saattaa olla haastavaa, koska opiskelijat ovat vielä alkuvaiheessa. Eräs vastaaja totesi, että *"opiskelijat eivät ole vielä riittävän kokeneita ymmärtääkseen tietoturva-aiheita syvällisemmin"*, mikä viittaa siihen, että tietoturva-aiheet koetaan vaikeiksi sisällyttää perustason kurssille, koska on niin paljon muitakin asioita käsiteltävänä. Jotkut vastaajat huomauttivat, että peruskurssien oppimistavoitteet eivät kata tietoturvaa. Tietoturvanäkökulmaa ei juuri linkitetä ohjelmoinnin peruskäsitteisiin. Esimerkiksi haavoittuvuuksien, kuten syötteiden validoinnin, mainittiin jäävän liian vähälle.

Aineopinnoissa tietoturvaan liittyviä aiheita käsitellään jonkin verran enemmän, mutta opettajien mukaan opetuksessa on kehittämismahdollisuuksia. Tietoturvaa pidettiin tärkeänä aineopintojen tasolla, koska opiskelijat siirtyvät yhä monimutkaisempiin ohjelmistokehitystehtäviin. Moni opettaja korosti, että aineopintoihin tulisi sisällyttää enemmän tietoturvan käytännön soveltamista,

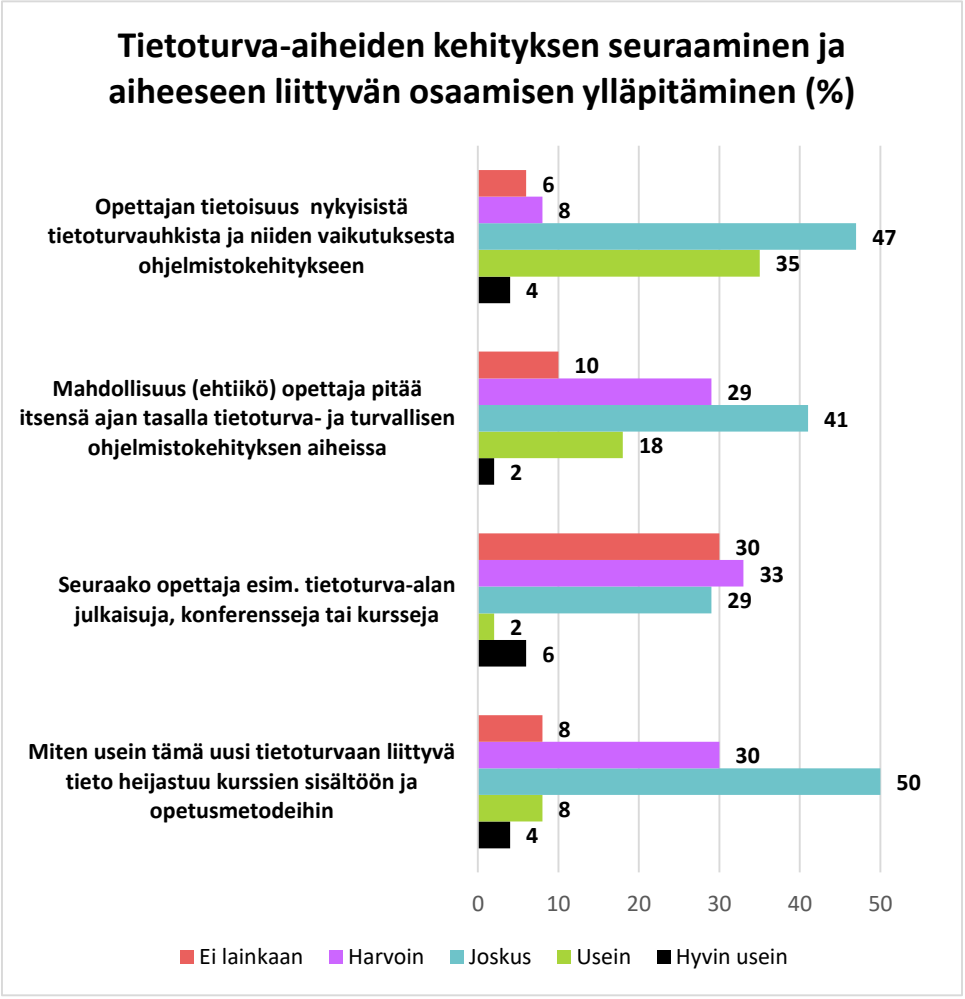
erityisesti projektitöiden ja harjoitustöiden kautta: "*aineopintojen kursseilla tietoturvan perusteet jäävät vähälle huomiolle, vaikka ne olisivat oleellisia turvallisessa ohjelmistokehityksessä*". Opettajien mukaan aineopintokursseilla tulisi käsitellä tietoturva-asioiden perustaitoja, kuten syötteiden validointia, käyttöoikeuksien hallintaa ja tietoturvatestausta: ”*aineopintojen projektitöissä tulisi olla tietoturvayhteyksiä, jolloin opiskelijat pääsisivät soveltamaan oppejaan konkreettisesti"*. Moni vastaaja toi esiin käytännön harjoitusten puutteen. Eräs vastaaja ehdotti, että aineopintokursseille voitaisiin lisätä esimerkiksi *"uhkamallinnusharjoituksia ja tietoturvatestausta, jotka lisäisivät opiskelijoiden ymmärrystä käytännön tietoturvasta"*. Moni opettaja koki, että aineopinnoissa ei ole riittävästi aikaa tai resursseja tietoturvan kattavaan käsittelyyn.

Syventävissä opinnoissa opiskelijoilla on paremmat valmiudet omaksua monimutkaisempia tietoturvakäytäntöjä, ja monet opettajat pitävät erillisiä tietoturvakursseja tärkeinä syventävällä tasolla. Syventävien opintojen osalta nousivat esiin seuraavat näkökulmat: Useat vastaajat mainitsivat, että syventävissä opinnoissa tulisi olla erillinen tietoturvakurssi/kursseja tai -moduuli: *"syventävissä opinnoissa tarvittaisiin oma kurssi turvalliselle ohjelmistokehitykselle, jotta aiheeseen voitaisiin paneutua kunnolla"*. Syventävien opintojen vastauksissa toistui tarve kokonaisvaltaiselle tietoturvanäkökulmalle. Tämä tarkoittaa tietoturvan huomioimista koko ohjelmistokehityksen elinkaaren ajan. Esimerkiksi tietoturvatestauksen menetelmien, kuten penetraatiotestauksen ja automatisoidun testauksen, opetus mainittiin tarpeellisena. Opettajat mainitsivat, että syventävien kurssien tulisi kattaa uhkamallinnus ja systemaattinen tietoturvatestaus osana ohjelmistokehitystä. Syventävissä opinnoissa tulisi myös käsitellä ohjelmistojen arkkitehtuuritason tietoturvaa, mukaan lukien turvallisen arkkitehtuurin suunnittelu ja tietoturvan dokumentointi.

Vastausten perusteella tietoturva jää usein hajanaiseksi osaksi ohjelmoinnin ja ohjelmistokehityksen opetusta. Perus- ja aineopinnoissa tietoturvaa käsitellään pinnallisesti, kun taas syventävissä opinnoissa kaivataan syvällisempää, kokonaisvaltaista ymmärrystä tietoturvasta. Kyselyn vastauksissa useat opettajat tukevat ajatusta erillisistä kursseista, jotka keskittyvät turvalliseen ohjelmointiin ja turvalliseen ohjelmistotuotantoon. Useat opettajat kuitenkin kokevat tietoturvan lisäämisen kurssien sisällöksi haastavaksi resurssien, aikarajoitteiden ja sopivien materiaalien puutteen vuoksi. Perusopinnoissa tietoturvaa pidetään liian haastavana aiheena, aineopinnoissa sen integrointi kärsii kurssien laajuuden takia, ja syventävissä opinnoissa tarvittaisiin erityisiä resursseja ja harjoitusympäristöjä. Opettajat kokevat, että tietoturvakoulutusta olisi mahdollista kehittää, mutta tämä vaatisi lisäresursseja, strategista suunnittelua ja mahdollisesti erillisiä tietoturvakursseja, joissa aiheisiin voitaisiin syventyä perusteellisesti.

3.4 Opettajien oma tietoturva-aiheisiin käyttämä aika ja mahdollisuus ylläpitää aiheeseen liittyvää osaamistaan

Vastausten pohjalta n. 50–85 % opettajista kokee seuraavansa tietoturvauhkia ja niiden vaikutuksia ohjelmointiin ja ohjelmistokehitykseen joskus tai usein (Kuva 13). Harvemmin tai ei lainkaan seuraavia opettajia on n. 15 %. Tämä osoittaa, että suurin osa opettajista pysyy jollain tasolla tietoisena tietoturvauhista, mutta osa ei kiinnitä tietoturva-aihepiiriin huomiota säännöllisesti.



Kuva 13: Opettajien mahdollisuus tietoturva-aiheiden kehityksen seuraamiseen ja aiheeseen liittyvän osaamisen ylläpitämiseen (%)

Useat opettajat kokevat pystyvänsä päivittämään osaamistaan joskus (n. 40 %), ja osa päivittää osaamistaan usein tai hyvin usein (n. 20 %). Harvoin tai ei lainkaan on n. 30 %, mikä kertoo, että lähes kolmasosalla opettajista on rajalliset mahdollisuudet pysyä ajan tasalla aihepiiristä. Tämä viittaa mahdollisesti haasteisiin ajan ja resurssien suhteen.

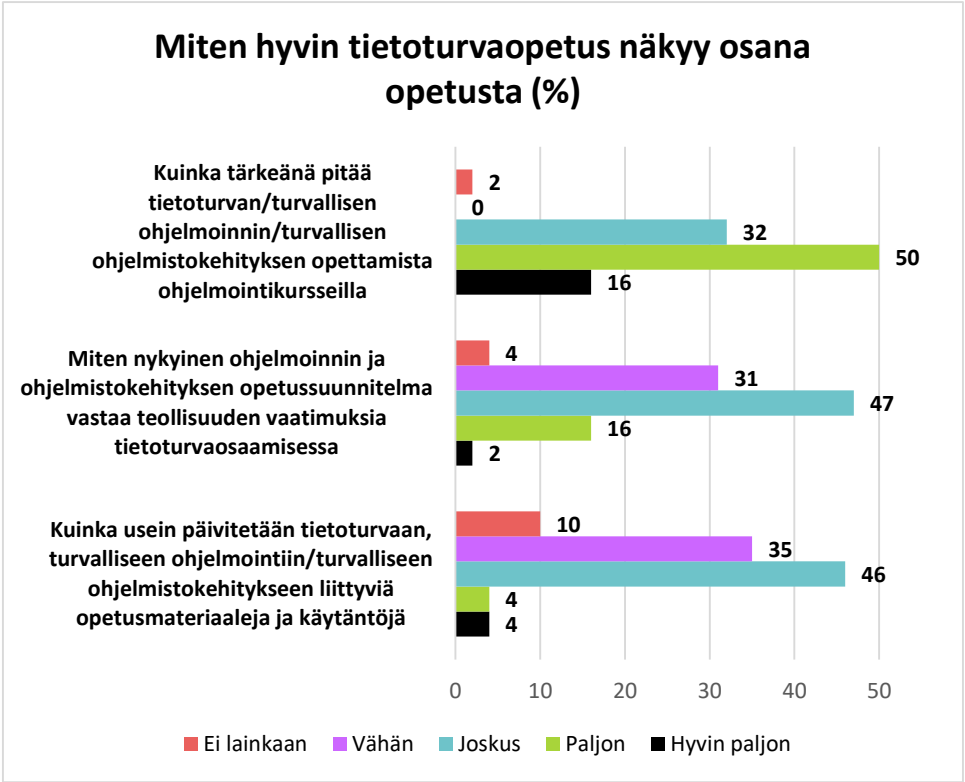
Aihealueen seuraamisen (esim. alan julkaisuja, konferensseja tai kursseja) osalta opettajista n. 60 % seuraa harvoin tai ei lainkaan. Kun taas n. 30 % seuraa joskus ja n. 8 % usein tai hyvin usein. Tasainen jakauma viittaa siihen, että alan aktiivinen seuraaminen jakautuu melko tasaisesti, mutta merkittävä osa opettajista ei seuraa aihetta säännöllisesti.

Vain n. 12 % opettajista kokee, että uusi tietoturvatieto heijastuu usein tai hyvin usein kurssien sisällöissä tai opetusmetodeissa, kun taas n. 40 % katsoo sen heijastuvan harvoin tai ei lainkaan. Enemmistö, eli n. 50 %, kertoo uusimman tiedon heijastuvan opetukseen joskus. Tämä osoittaa, että vaikka uutta tietoa pyritään jonkin verran integroimaan kursseille, sen käytännön toteutus jää monella opettajalla satunnaiseksi. Vaikka monet opettajat ovat tietoisia tietoturvan kehityksestä ja pyrkivät päivittämään osaamistaan, opettajat kokevat ajan ja resurssien puutteen rajoittavan alan uusimpien tietojen ja kehityksen integrointia opetukseen.

Suurin osa opettajista pitää tietoturvan ja turvallisen ohjelmistokehityksen opettamista tärkeänä tai erittäin tärkeänä (n. 65 %) tai jonkin verran tärkeänä (32 %) (Kuva 14). Tämä korostaa vahvaa tarvetta ja halua sisällyttää tietoturva opetukseen. Kuitenkin opettajilla on haasteena se, että on monta muutakin yhtä tärkeää aihetta, jotka myös pitäisi sisällyttää osaksi kursseja.

Suurin osa opettajista kokee, että nykyinen opetussuunnitelma vastaa huonosti (35 %) ja joskus/kohtalaisesti (47 %) teollisuuden tarpeisiin tietoturvaosaamisen osalta. Vain n. 20 % pitää opetussuunnitelmaa hyvin teollisuuden vaatimuksiin vastaavana. Tämä osoittaa selkeää näkemystä siitä, että nykyinen opetussisältö ei täysin vastaa työelämän odotuksia.

Opettajista vain 8 % päivittää tietoturvaan liittyvää materiaalia usein ja 46 % tekee sitä joskus, ja n. 45 % päivittää näitä sisältöjä harvoin tai ei lainkaan. Tämä viittaa siihen, että tietoturva-aiheiden päivittäminen osaksi kursseja ja kurssimateriaaleja kohtaa haasteita, mahdollisesti ajan ja resurssien rajallisuuden takia. Opettajat tunnistavat tietoturvaopetuksen tärkeäksi tietoturvaopetusta tärkeänä, mutta nykyinen opetussuunnitelma ja resurssit eivät täysin tue sen integroimista opintoihin teollisuuden odotusten mukaisella tasolla. Lisäksi ala on hyvin nopeasti kehittyvä ja muuttuva, ja tästä syystä opetus ei välttämättä pysy täysin ajan tasalla nopeasti muuttuvassa tietoturvaympäristössä.



Kuva 14: Tietoturva-aiheiden näkyminen osana opetusta (%)

Avoimista vastauksista nousi esille, että useat opettajat mainitsivat ajan ja resurssien rajallisuuden suurimpana esteenä tietoturva-aiheiden päivittämiselle ja syvälliselle käsittelylle kursseilla. Lisäksi tietoturvan syvempi integrointi osaksi kurssia olisi ristiriidassa muiden oppimistavoitteiden kanssa: *"Tietoturva-asiat ovat kursseillani relevanteista näkökulmista prioriteettijärjestyksessä loppupäässä, ja koen että niiden painotus rikkoisi kurssien fokusta."*

Jotkut opettajat kokevat, että tietoturvan merkitys on kasvanut entistä tärkeämmäksi, mutta he myös kokevat, että sen opettaminen voi olla haastavaa opiskelijoiden vähäisen pohjatiedon vuoksi. Tämä ristiriita tärkeänä pidetyn aiheen ja opiskelijoiden rajallisten valmiuksien välillä saattaa vaikuttaa opettajien motivaatioon. Esimerkiksi eräs opettaja toi esille opiskelijoiden tietoturvatietoisuuden tason merkityksen. Opettajat kokivat, että opiskelijoiden perusosaamisen puutteet tekevät tietoturvan syvällisestä käsittelystä haastavaa. Eräs opettaja mainitsi, että tietoturvaan liittyvät aiheet jäävät opiskelijoille vaikeiksi ymmärtää ilman vahvempaa

pohjaa: *"Voisin tehdä turvallisen ohjelmoinnin eteen paljon enemmän, jos opiskelijoilla olisi olennaisesti parempi perusta, jonka päälle rakentaa."*

Vastauksista ilmeni tarve laajemmalle tietoturva-aiheiden koordinoinnille opetussuunnitelmassa. Erityisesti ohjelmointikursseilla nähtiin olevan potentiaalia käsitellä tietoturvaan liittyviä aiheita, mutta nykyisessä kurssirakenteessa ajan puute rajoittaa tietoturvan käsittelyä: *"Tietoturva-aiheiden opettamista pitäisi koordinoida laajemmin kaikkien kurssien, erityisesti ohjelmointikurssien välillä."* Tietoturva-alan jatkuva kehitys ja uusien uhkien ilmaantuminen vaatisivat aktiivista seurantaa, mutta osa opettajista ei koe ehtivänsä pysyä mukana. Tietoturva-aiheiden kiinnostavuus vaihtelee opiskelijoiden keskuudessa, ja tämä voi heijastua myös opettajien motivaatioon. Erään opettajan mukaan tietoturva-aiheita pidetään joskus liian erityisalan tietona, mikä saattaa vähentää kiinnostusta sekä opiskelijoiden että joidenkin opettajien osalta.

Joidenkin opettajien mukaan tietoturva olisi tärkeää sisällyttää opetukseen olennaisilta osilta, mutta turhaa tai liiallista tietoturvapainotusta tulisi välttää. Tämä tasapaino nähtiin tärkeänä, jotta tietoturvaan liittyvät aihepiirit eivät vaikuttaisi oppilaiden keskittymiseen perusasioihin. Osalla opettajista on vahva kiinnostus ja motivaatio sisällyttää tietoturva opetukseen, mutta tämä motivaatio saattaa jäädä hyödyntämättä ajan ja resurssien puutteen vuoksi. Monet kokevat aiheen tärkeäksi, mutta kokevat, että sen syvällinen käsittely vaatii erikoisosaamista ja lisäresursseja, joita heillä ei välttämättä ole käytettävissä. Tämä voi vähentää motivaatiota, kun he tuntevat, etteivät pysty toteuttamaan aihetta opetuksessa toivotulla tavalla.

Tekoälyn lisääntynyt käyttö ohjelmoinnissa ja ohjelmistokehityksessä on tuonut uusia haasteita tietoturvan opettamiseen, mikä vaikuttaa myös opettajiin. Eräs opettaja mainitsi huolensa siitä, että tekoälyn käyttö alustavien ohjelmistoversioiden luomisessa saattaa kasvattaa tietoturvahaavoittuvuuksien riskiä, mikä asettaa uudenlaista painetta tietoturvaopetukselle. Tämä saattaa motivoida opettajia panostamaan tietoturvaan, mutta samalla se voi myös lisätä heidän kokemaansa kuormitusta ja haastavuutta aiheen opettamisessa.

3.5 Ideoita ja tarpeita, miten kehittää kyberturvallisuusopetusta kokonaisuutena

Opettajien näkemyksistä ja ideoista nousee esiin tapoja, joilla kyberturvallisuusopetusta voitaisiin kehittää. Vastaukset korostavat sekä tarvetta tietoturvan syvälliselle integroitumiselle osaksi opetusta että tuoda lisää käytännönläheisiä keinoja, joiden kautta tietoturvataitoja voidaan vahvistaa.

Esille nousseita ehdotuksia olivat:

- **Erilliset tietoturvakurssit ja syventävät opinnot.** Useat opettajat painottivat erillisten syventävien tietoturvakurssien merkitystä. Heidän mielestään yksittäisten tietoturva-aiheiden lisääminen nykyisiin kursseihin ei ole riittävää (eikä välttämättä edes toimivaa), vaan tarvitaan secure programming ja secure software development -tyyppiset kurssit, joissa tietoturva-aiheita voidaan käsitellä kokonaisvaltaisesti. Tämä mahdollistaisi myös kehittyneempien aiheiden, kuten riskien arvioinnin ja uhkamallinnuksen, syvällisen käsittelyn. *"Tarvitaan omat secure programming ja software development -kurssit,"* totesi useampikin opettaja.
- **Tietoturvan integrointi eri kursseille.** Monet opettajat ehdottivat, että tietoturva tulisi liittää kaikkien ohjelmistotuotannon kurssien sisältöön, jolloin tietoturva käsitellään aina kurssin omassa kontekstissa. Esimerkiksi tietokantakursseilla voitaisiin käydä läpi SQL-injektioita ja C-kursseilla puskuriylivuotojen riskejä. Näin opiskelijat saisivat käsityksen siitä, kuinka tietoturva liittyy erilaisiin teknisiin aiheisiin. Kuten yksi opettaja tiivisti: *"Yleisimmät ongelmat osaksi niitä käsitteleviä kursseja."*
- **Käytännön harjoitukset ja projektimuotoiset kurssit.** Opettajien mukaan tietoturvan oppimista tulisi tukea käytännön harjoituksilla, joissa opiskelijat voivat tunnistaa ja korjata sovellusten tietoturva-aukkoja. Projektimuotoisilla kursseilla opiskelijat voisivat esimerkiksi työskennellä auditoinnin parissa, tunnistaa sovellusten heikkouksia ja ehdottaa parannuksia. Ehdotettiin myös harjoituksia, joissa osa opiskelijoista kehittää sovelluksen ja toinen osa pyrkii löytämään siitä haavoittuvuuksia, mikä auttaisi heitä ymmärtämään tietoturvan merkitystä konkreettisesti. Opettajat nostivatkin esille, että tietoturvaopetus kaipaisi enemmän käytännön harjoituksia, joissa opiskelijat voisivat tunnistaa ja korjata haavoittuvuuksia sekä harjoitella turvallisia ohjelmointikäytäntöjä konkreettisissa tilanteissa. *"Jokin projektimuotoinen kurssi, jossa tunnistetaan jonkin auditoitavan sovelluksen tai oman sovelluksen heikkouksia ja korjataan niitä."*
- **Tietoturvaan liittyvien taitojen määrittely ja oppimistavoitteet.** Monet opettajat kokivat tärkeäksi määritellä, mitkä tietoturvaan liittyvät taidot jokaisen opiskelijan tulisi hallita, jotta nämä tavoitteet voitaisiin jakaa eri kursseille. Näiden

taitojen, kuten autentikointi, autorisointi, syötteen validointi ja penetraatiotestauksen alkeet, tulisi olla jokaisen ohjelmistokehittäjän perusosaamista: *"Autentikointi, autorisointi, syötteen validointi/sanitointi ovat tärkeintä alkeisoppia"*.

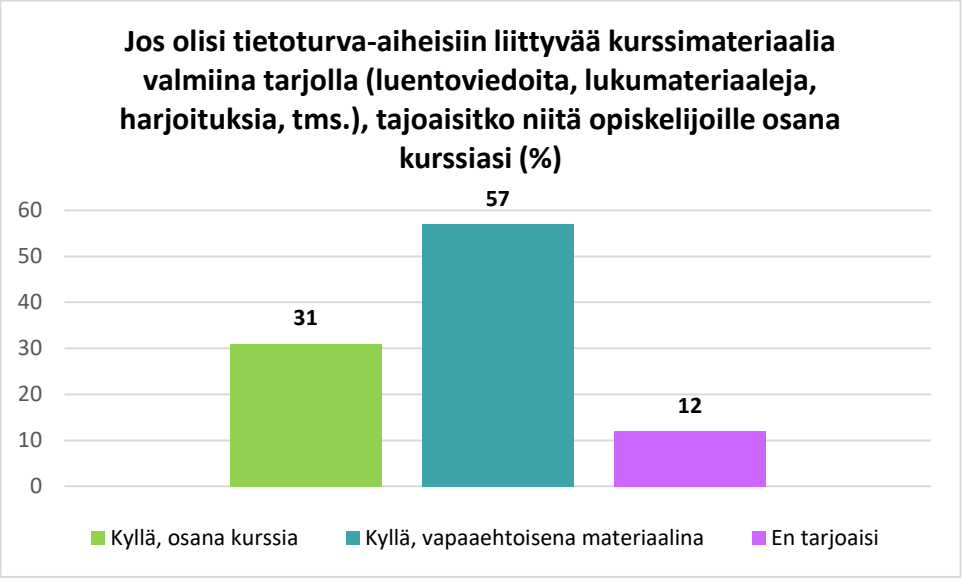
- **Eettisten kysymysten käsittely ja kyberpsykologia.** Tietoturvan opettamisessa tulisi käsitellä myös ohjelmistoeettisyyttä, tekoälyn etiikkaa ja ihmisten haavoittuvuuksia sekä kyberpsykologiaa. Opettajien mielestä opiskelijoiden on tärkeää ymmärtää, kuinka eettinen kypsyys ja yksilön ymmärrys vaikuttavat turvallisten järjestelmien kehittämiseen: ”*Teknisen opetuksen lisäksi on erittäin keskeistä käsitellä eettisiä näkökulmia opiskelijoiden kanssa*.”
- **Työkalut ja käytännöt tietoturvallisuuden varmistamiseksi.** Opettajat ehdottivat keskittymistä tiettyihin keskeisiin tekniikoihin ja työkaluihin, jotka auttaisivat tietoturvallisuuden varmistamisessa, kuten autentikointi, autorisointi, syötteen validointi, tietokantojen suojaus ja yleisimmät hyökkäysmenetelmät. Näin opiskelijat saisivat konkreettisia työkaluja tietoturvan hallintaan, ja heille muodostuisi perusvalmiudet suojautua tavallisimmilta hyökkäyksiltä.
- **Käytännön esimerkit ja tosielämän tarinat (yhteistyö yritysten kanssa).** Opettajat ehdottivat työelämän esimerkkien ja tietoturvatapausten käyttöä opetuksessa, jotta opiskelijat saisivat konkreettisen käsityksen tietoturvariskien vakavuudesta: *"Käytännön eli tosielämän kauhutarinoita aiemmista tapahtumista. Julkisuudesta (lehdet, mediat) ja alan julkaisusta löytyy esimerkkejä."* Käytännön esimerkit ja julkisuudessa olleet tapaukset tarjoavat mahdollisuuden analysoida tietoturvaongelmia syvällisemmin ja tuovat ajankohtaisen näkökulman opetukseen. *"Mitä tuoreempi, sen parempi esimerkki,"* kommentoi yksi opettaja. Lisäksi yritysten edustajien kautta tulevat käytännön asiat ja esimerkit ovat erittäin tärkeitä opiskelijoiden asiayhteyksien integroinnissa.
- **Negatiivinen testaus ja turvallisuusriskien arviointi.** Negatiivinen testaus mainittiin keinona, jolla opiskelijoita voitaisiin opettaa tunnistamaan mahdollisia turvallisuusriskejä koko ohjelmistokehitysprosessin ajan. Opettajat korostivat negatiivisen testauksen tärkeyttä, sillä se auttaisi opiskelijoita näkemään, kuinka erilaiset testausmenetelmät voivat paljastaa tietoturva-aukkoja ja ennaltaehkäistä haavoittuvuuksia. *"Negatiivista testausta mukaan joka vaiheeseen!"*

- **Kansainvälisten suositusten hyödyntäminen.** Opettajat mainitsivat myös kansainväliset suositukset, kuten ACM- ja IEEE-ohjeistukset, jotka tarjoavat linjauksia tietoturvan opetuksesta. Näitä suosituksia voitaisiin hyödyntää turvallisuuteen liittyvien kurssien suunnittelussa ja kehittämisessä, mikä voisi tuoda opetukseen selkeyttä ja johdonmukaisuutta. Näiden suositusten avulla voitaisiin luoda vahvempi ja yhdenmukaisempi tietoturvaopetuksen rakenne, joka perustuisi alan parhaisiin käytäntöihin. *"Veikkaan, että suositusten Computer Science ja Software Engineering security-osuudet vastaavat tähänkin."*
- **Innostus ja motivaatio opettajilla.** Muutamat opettajat toivoivat, että tietoturvakurssit opettaisi joku, jolla on aitoa kiinnostusta ja motivaatiota aiheeseen. Tämä voisi varmistaa, että opiskelijat saavat innostavan ja ajantasaisen opetuksen tietoturvasta.
- **Tietoturvattomien ohjelmointikielten välttäminen.** Eräs opettaja ehdotti, että opetuksessa tulisi pyrkiä käyttämään sellaisia ohjelmointikieliä ja työkaluja, joissa on parempi tietoturvataso sisäänrakennettuna. C- ja C++-kielten käyttöä tulisi välttää opetuksessa tietoturvasyistä, koska ne koetaan haavoittuviksi. "*Kaikilla tasoilla voisi opettaa, ettei enää koskaan ja missään käytettäisi tietoturvattomia ohjelmointikieliä, kuten C/C++.*"
- **Oppimistavoitteiden ja tietoturvan osa-alueiden koordinaatio kurssien välillä.** Jotkut opettajat ehdottivat, että eri kursseilla käsiteltävät tietoturva-aiheet tulisi koordinoida siten, ettei samoja asioita käsitellä useaan kertaan eri kursseilla, vaan oppimistavoitteet ja tietoturva-aiheet täydentävät toisiaan. Tämä lähestymistapa voisi auttaa luomaan kattavan tietoturvakoulutuksen, joka etenee loogisesti kurssien välillä. "*Erityisen tärkeää olisi koordinoida harjoituksia eri kurssien välillä, ettei samaa asiaa treenata liian monta kertaa (samalla tasolla tai tavalla)*."
- **Hackathonit ja tietoturvakilpailut.** Opettajat ehdottivat, että tietoturvakilpailut, kuten hackathonit ja capture the flag -haasteet, voisivat olla hyvä tapa innostaa opiskelijoita tietoturvaan liittyvissä opinnoissa. Tämäntyyppiset kilpailut tarjoavat opiskelijoille mahdollisuuden oppia hauskalla ja motivoivalla tavalla, ja ne voisivat lisätä opiskelijoiden kiinnostusta tietoturvaan. "*Varsinkin syventävissä opinnoissa voisi olla enemmän hackathon, capture the flag yms. kisoja ja haasteita*."

Opettajien näkemykset korostavat tietoturvan merkitystä osana laajempaa ohjelmoinnin ja ohjelmistotuotannon opetusta. Useat ehdotukset nostavat esille käytännön harjoittelun merkityksen, erillisten tietoturvakurssien (secure programming/software development) toteuttamisen, eettisten kysymysten käsittelyn (sisältäen myös kyberpsykologian) sekä kansainvälisten suositusten hyödyntämisen.

Kun tarkastellaan opettajien vastauksia ulkoisen opetusmateriaalin käytöstä tietoturva-aiheiden opetuksessa, vastausten jakauma on seuraava (kuva 15):

- 31 % opettajista on valmis tarjoamaan ulkoista materiaalia osana kurssia.
- 57 % opettajista olisi valmis käyttämään ulkoista materiaalia vapaaehtoisena aineistona opiskelijoille.
- 12 % opettajista ei tarjoaisi ulkoista materiaalia.



Kuva 15: Valmiin opetusmateriaalin hyödyntäminen kursseilla (%)

Opettajat, jotka valitsivat ”En tarjoaisi”, ovat avoimissa vastauksissa nostaneet esille, että he ovat avoimia ja valmiita käyttämään ulkoista opetusmateriaalia, mikäli sen laatu ja sisältö vastaisivat kurssin tavoitteita ja soveltuisivat hyvin kurssiin. Materiaalin pitäisi olla selkeästi laadukasta ja tarkoitukseen sopivaa, jotta sen käyttö olisi perusteltua. *"Harkitsisin materiaalin sisällöstä ja laadusta riippuen."*

Valmiin opetusmateriaalin integroiminen osaksi kurssia koetaan haasteelliseksi, koska usein materiaalin täytyy mukautua kurssin erityispiirteisiin. Osa opettajista koki, että materiaalin muokkaaminen kurssiin sopivaksi voi olla yhtä työlästä kuin aineiston luominen itse. *"Yleensä asiat pitää sovittaa kurssiin, eikä valmiin aineiston sovittaminen ole helpompaa kuin asioiden esittäminen omin sanoin kurssin kontekstissa."*

Erilaisten aineistojen yhdistäminen kurssille saattaa johtaa sillisalaattimaiseen rakenteeseen, mikä voi heikentää oppimiskokemusta. Opettajat ovat huolissaan siitä, että monista lähteistä peräisin oleva sisältö voi hämmentää opiskelijoita ja vaikeuttaa kurssin kokonaisrakenteen ymmärtämistä. *"Eri puolilta tulevien aineistojen yhdistäminen tuppaa tekemään kursseista sillisalaattia."*

Tietoturva-alan materiaalin ajantasaisuus on tärkeä tekijä, ja useat opettajat mainitsivat, että aiheeseen liittyvä materiaali vanhenee nopeasti. Tämä asettaa haasteita materiaalin jatkuvalle käytölle, koska alalla tapahtuu nopeaa kehitystä, joka voi tehdä aiemmista aineistoista vanhentuneita. *"Materiaali vanhentuu nopeasti."*

Joidenkin opettajien mielestä ulkoista materiaalia voitaisiin tarjota opiskelijoille vapaaehtoisena, mikäli se osoittautuu hyödylliseksi ja validiksi kurssin läpikäynnin jälkeen. Tämä mahdollistaisi lisämateriaalin tarjoamisen ilman pakollista sitoutumista sen käyttöön. *"Kyllä vapaaehtoisena, jos materiaali vaikuttaa läpikäynnin jälkeen validilta ja jotenkin kurssiin sopivalta."*

Jotkut opettajat huomauttivat, että tietoturva ei ole oppimistavoitteena kaikilla kursseilla, kuten ohjelmoinnin peruskursseilla. Tämä voi vaikuttaa siihen, kuinka paljon tietoturvaan liittyvää opetusmateriaalia halutaan sisällyttää näille kursseille. *"Tietoturva ei ole osa oppimistavoitteita ohjelmoinnin tai ohjelmistokehityksen peruskursseilla."*

3.6 Opettajien esille nostamia kommentteja tai palautetta

Vapaassa palautekentässä opettajat nostivat esille seuraavia kommentteja ja palautteita:

- **Tietoturva osana laajempaa opetuskokonaisuutta.** Tietoturva-aiheiden opetus ei saisi olla irrallinen osa koulutusta, vaan sen tulisi olla integroitu osaksi muita aihepiirejä. Tämä tukee tarvetta tietoturvan laajempaan integroitumiseen opetussuunnitelmassa: *"Eihän tämän pitäisi olla irrallaan muusta koulutuksesta."*
- **Resurssien ja rahoituksen tasapaino eri aihepiirien välillä.** Osa opettajista varoitti tietoturvaan liittyvän opetuksen liiallisesta painottamisesta muiden tärkeiden aiheiden kustannuksella. He korostivat, että tietoturvaa ei tulisi priorisoida liikaa opetuksessa ja tutkimuksessa, vaan on tärkeää huomioida myös muiden aiheiden resurssitarpeet. *"Aihepiirin ylipainottamista tulee välttää opetuksessa, tutkimuksessa, ja erityisesti näiden rahoituksessa."* Ohjelmoinnin ja ohjelmistotuotannon kurssien haasteena onkin se, että on monta muutakin tärkeää aihetta, jotka pitäisi tietoturvan lisäksi ottaa osaksi tai huomioida kurssien aikana. Jos kuitenkin näitä alkaa liikaa painottaa, kurssin ydinasian opettaminen voi vaarantua.
- **Yhteistyö ja aihepiirin syvempi osaaminen keskitetyissä ohjelmissa.** Ehdotettiin, että yksi tai kaksi yliopistoa voisi tarjota tietoturvaan keskittyvän koulutusohjelman, jotta asiantuntemus keskittyisi sinne, missä sitä on eniten. Tällainen malli voisi tarjota syvempää tietoturvaosaamista kuin hajautettu koulutusmalli kaikissa yliopistoissa.
- **Trendien vaikutus tietoturvaopetukseen.** Joidenkin opettajien mukaan tietoturva keskittyy liikaa trendikkäisiin työkaluihin ja WWW-pohjaisiin asiakas-palvelin-järjestelmiin. Opettajat kaipasivat laajempaa näkökulmaa tietoturvan koko kirjoon, joka ylittää nykyiset muoti-ilmiöt.
- **Opiskelijoiden valmiudet ja perustaidot.** Opettajat ilmaisivat huolensa siitä, että opiskelijoiden opiskelutaidot ja abstraktin ajattelun taidot ovat heikentyneet verrattuna aiempiin vuosikymmeniin. He toivoivat vahvempaa pohjakoulutusta, erityisesti lukioiden tasolla, jotta opiskelijat olisivat valmiimpia käsittelemään monimutkaisia tietoturva-aiheita. *"Olisi tärkeää saada lukioiden tuottamat opiskelutaidot, abstraktien asioiden miettimistaidot ja niin edelleen takaisin 1990-luvun tasolle."*

- **Ajanpuute ja opetuksen ajoittaminen.** Moni opettaja mainitsi jatkuvan ajanpuutteen haasteena. Erityisesti ensimmäisen vuoden opinnoissa aikataulutus koettiin ongelmalliseksi, sillä osa sisällöistä nähtiin vähemmän tärkeinä, ja niihin käytetty aika voisi olla hyödyllisempää muissa aiheissa. *"Ikuinen ajanpuute pitäisi ratkaista. Ainakin meillä ensimmäisen vuoden syksyn opinnoissa on turhan löysä aikataulu sisältöön nähden."*
- **Syventävien kurssien käytännönläheisyys tai sen puute.** Opettajat toivoivat, että syventävillä kursseilla ei keskityttäisi vain harjoituksiin, vaan niissä tulisi olla myös käytännön esimerkkejä ja ohjeita, jotka valmistavat opiskelijoita työelämään. Tämä toive liittyy siihen, että tietoturvan tulisi olla sovellettavissa konkreettisiin tilanteisiin. *"Syventävillä kursseilla ei pitäisi keskittyä vain "harjoituksiin" vaan myös käytännön esimerkkeihin ja ohjeisiin sekä käytänteisiin."*
- **Ajanpuutteen vaikutus omaan perehtymiseen.** Osa opettajista mainitsi, ettei heillä ole riittävästi aikaa perehtyä syvällisesti kyberturvaan, mutta he luottivat siihen, että heidän yliopistossaan on tarjolla omia opintojaksoja, jotka kattavat tämän osa-alueen: *"En itse ehdi perehtymään kyberasioihin, mutta meillä on niille omia opintojaksojaan."*
- **Erillisten secure programming ja secure software development kurssien toteuttaminen.** Opettajat kannattivat erillisten kurssien toteuttamisen, jossa pystytään kokonaisuutena tarkastelemaan aiheita paremmin ja rakentamaan teeman ympärille soveltuvat harjoitukset. Jos aiheita ryhdytään liikaa tuomaan muille kursseille ilman systemaattista suunnitelmaa ja integraatiota kurssien välille, aiheista tulee vajavaista ja näyttäytyy sekavalta opiskelijoille. Tästä syystä asiaan paneutuvat kurssit voivat keskittyä rakentamaan näkökulmat ja integraation aiheiden välille paremmin.

Lisäksi useampi opettaja läpi koko kyselyn nosti esille haasteita opiskelijoiden osaamisessa ja kyvyssä oppia ja omaksua ohjelmoinnin tai ohjelmistotuotannon aiheita. Opettajat toivat esiin useita näkemyksiä opiskelijoiden oppimisen tasosta ja siihen liittyvistä haasteista.

Useat opettajat olivat huolissaan opiskelijoiden perustaitojen heikkenemisestä, erityisesti abstraktien asioiden käsittelyssä ja ajattelussa. He kokivat, että nykyopiskelijoilla ei ole samanlaista valmiutta omaksua monimutkaisia ja teoreettisia aiheita kuin aiempina vuosina. Tämä koettiin erityisen ongelmalliseksi tilanteissa, joka vaatii kykyä ymmärtää monimutkaisia, abstrakteja konsepteja. Opettajat mainitsivat, että opiskelijat eivät aina osaa omaksua tietoa itsenäisesti tai käsitellä laajoja materiaalikokonaisuuksia. Tämä rajoittaa heidän kykyään opiskella syvällisiä

aiheita, ja se vaikuttaa oppimisen laatuun. Erityisesti koettiin, että opiskelijat eivät enää ole tottuneita lukemaan ja sisäistämään pidempiä tekstejä tai kokonaisia kirjoja: ”*Tässäkin olisi tärkeää lähettää päättäjille viestiä, että lukioiden tuottamat opiskelutaidot, abstraktien asioiden miettimistaidot ja niin edelleen olisi tärkeää saada nostettua takaisin 1990-luvun tasolle. Olisi tärkeää, että opiskelijat pystyisivät lukemaan ja omaksumaan helppotajuisen 100-sivuisen suomenkielisen kirjan."*

Opettajat kokivat, että monilla opiskelijoilla on puutteita ohjelmoinnin ja tietotekniikan perustaidoissa, mikä vaikeuttaa ohjelmoinnin opettamista, mukaan lukien tietoturva-aiheet. Kun perustaidot eivät ole riittävän vahvoja, opiskelijoiden on vaikea hahmottaa, miten esimerkiksi tietoturva liittyy osaksi laajempaa ohjelmistokehitystä. Tämä puute tekee syvällisempien tietoturvakonseptien opettamisesta haastavaa.

Jotkut opettajat havaitsivat, että opiskelijat eivät aina näe tietoturvan merkitystä omassa työssään tai tulevassa ammatissaan. Tämä voi johtua siitä, että tietoturva koetaan liian tekniseksi tai kaukaiseksi. Opettajat kokivat haasteelliseksi motivoida opiskelijoita tietoturvaopintoihin, jos he eivät ymmärrä aiheen konkreettista sovellettavuutta työelämässä.

Opettajat korostivat, että tietoturva vaatii vahvan pohjakoulutuksen, johon kuuluu riittävä osaaminen ohjelmoinnissa ja teknisissä perusteissa. Heidän mielestään opiskelijoiden oppimispolun tulisi olla johdonmukainen, ja tietoturvan perustaitojen tulisi rakentua asteittain jo perusopintojen aikana. Tämä vaatisi opetussuunnitelman kehittämistä siten, että perustaidot opittaisiin jo opintojen alkuvaiheessa.

Useat opettajat toivoivat, että opiskelijat pystyisivät paremmin soveltamaan teoreettista tietoa käytännön tilanteissa. Tietoturva vaatii abstraktin tiedon lisäksi kykyä soveltaa opittua käytännössä, ja opettajat kokivat, että tämä siirtymä teoriasta käytäntöön on joillekin opiskelijoille vaikeaa. Tämä ongelma tuli esiin erityisesti syventävien kurssien osalta, joissa opiskelijoilta odotetaan valmiuksia ratkaista käytännön ongelmia itsenäisesti.

Nämä näkemykset tuovat esille, että osa opettajista kokee opiskelijoiden oppimisen tason haasteelliseksi. He peräänkuuluttavat vahvempia perustaitoja, parempia opiskelutaitoja, ja johdonmukaisempaa oppimispolkua, jotta opiskelijat voisivat oppia aiheita syvällisemmin ja soveltaa niitä käytännössä.

4 Yhteenveto

Tässä raportissa kuvattiin ohjelmoinnin ja ohjelmistotuotannon kurssien opettajille suunnatun kyselyn tuloksia. Kysely toteutettiin Turun yliopiston ohjelmistotekniikan ja kyberturvallisuusteknologian tutkimusyksiköiden toimesta kyberturvallisuus-hankkeen aikana (hankkeeseen osallistuu yhdeksän suomalaista yliopistoa, jotka tarjoavat kyberturvallisuusalan koulutusta). Turun yliopiston toimesta toteutettiin opettajakysely, jonka tarkoituksena oli kartoittaa ohjelmoinnin ja ohjelmistotuotannon opettajien näkemyksiä tietoturva-aiheiden opettamisesta ja huomioimisesta osana ohjelmoinnin ja ohjelmistotuotannon kurssien aiheita. Kartoitus toteutettiin 26.8.2024-13.9.2024, ja kyselyyn vastasi 54 opettajaa. Kyselyn pohjaa rakensivat yrityksille suunnattu kyberturvallisuuskoulutuksen kehittämisen osaamistarvekartoitus (Majanoja et al., 2024b) sekä yliopistojen kyberturvallisuus-alan koulutuksien sisällön tarkastelun kautta, joka toteutettiin Turun yliopiston kehittämän arviointityökalun kautta (Majanoja et al., 2024a).

Kyselyyn vastanneiden opettajien vastaukset osoittavat, että tietoturvan opetus on heille aiheena tärkeää, mutta käytännössä siihen liittyy monia haasteita. Tietoturva nähdään merkittävänä osa-alueena erityisesti ohjelmistokehityksen ja ohjelmoinnin opetuksessa, sillä sen merkitys on kasvanut nopeasti muuttuvan teknologian ja kyberuhkien yleistymisen myötä. Useat opettajat ovat kuitenkin kokeneet, että tietoturvan integrointi olemassa oleviin kursseihin on vaikeaa, ja monet pohtivat, kuinka tietoturvaopetusta voitaisiin kehittää niin, että se vastaa sekä opiskelijoiden valmiuksia että työelämän tarpeita.

Yksi keskeinen ja eniten esille nostettu haaste on resurssien, kuten ajan ja resurssien/budjetin puute, joka vaikeuttaa tietoturvan tehokasta integroimista kurssien sisältöihin tai uusien kurssien toteuttamiselle. Monet opettajat kokevat myös, että tietoturva on oma erityisalansa, joka vaatii syvällistä asiantuntemusta ja jatkuvaa päivitystä, sillä uhkakuvat ja turvallisuusmenetelmät kehittyvät jatkuvasti. Lisäksi tietoturvaopetukseen liittyy usein tarve erityisosaamiselle, jota kaikilla opettajilla ei välttämättä ole. Tämä asettaa paineita niille opettajille, jotka haluaisivat käsitellä tietoturvaa syvällisemmin, mutta eivät koe omaavansa riittävää tietoturvaosaamista.

Perusopintojen osalta monet opettajat kommentoivat, että tietoturva-aiheiden käsittely on hyvin rajallista, ja useimmat peruskurssit keskittyvät pääasiassa ohjelmoinnin ydintaitoihin. Tietoturvaopetuksen syvällisempi käsittely tässä vaiheessa voisi olla liian haastavaa opiskelijoille, joilta puuttuu perusosaaminen ja ymmärrys ohjelmistokehityksen laajemmasta kokonaisuudesta, ja sen johdosta opiskelijat eivät pysty liittämään asioita laajempaan kontekstiin. Monet opettajat mainitsivat, että tietoturva-asioita ei juurikaan käsitellä perusopinnoissa, ja osa vastaajista katsoo, että aihe on liian monimutkainen opiskelijoille, joilla ei vielä ole riittävää teknistä pohjatietoa.

Aineopinnoissa tietoturvaan liittyviä aiheita käsitellään jonkin verran enemmän, mutta opettajien mukaan opetuksessa on merkittäviä kehittämismahdollisuuksia. Tietoturvaa pidetään tärkeänä aineopintojen tasolla, koska opiskelijat siirtyvät yhä monimutkaisempiin ohjelmistokehitystehtäviin. Moni opettaja korostaa, että aineopintojen tasolla olisi hyödyllistä sisällyttää tietoturva käytännön soveltamisen kautta esimerkiksi projektitöihin. Opiskelijat voisivat tällöin harjoitella turvallisten ohjelmistojen rakentamista ja oppia tunnistamaan mahdollisia tietoturva-aukkoja harjoitusprojektien kautta.

Syventävissä opinnoissa tietoturvan opetusta pidetään entistä tärkeämpänä, koska opiskelijoilla on tässä vaiheessa paremmat valmiudet käsitellä tietoturvan monimutkaisia käytäntöjä ja konsepteja. Opettajat ehdottavat, että tietoturvalle tulisi olla omia erillisiä kursseja, joissa keskityttäisiin aiheeseen syvemmin. Ehdotuksena nousi esille kaksi kurssia: Secure Programming ja Secure Software Development -kurssit. Nämä kurssit käsittelisivät ohjelmointiin sekä ohjelmistotuotantoon liittyviä näkökulmia kokonaisuutena, sisältäen mm. uhkamallinnusta, penetraatiotestausta, tietoturva-arkkitehtuuria ja muita tietoturvan osa-alueita. Tämä antaisi opiskelijoille mahdollisuuden perehtyä tietoturvaan kokonaisvaltaisesti ja syvällisesti ilman, että se rikkoo muiden kurssien ydinsisältöjä ja oppimistavoitteita.

Erilliset tietoturvakurssit voisivat tarjota opiskelijoille myös käytännön harjoituksia ja kokemusta, jota he eivät muuten saisi osana muita kursseja. Tietoturvan syvällinen opetus vaatii erikoistumista, ja monet opettajat kokevat, että tietoturva tulisi opettaa niiden toimesta, jotka ovat perehtyneet aiheeseen ja pystyvät pitämään opetuksen ajan tasalla jatkuvasti muuttuvien uhkakuvien ja teknologioiden osalta.

Monet opettajat kokevat, että tietoturvaopetus kärsii resurssien, erityisesti ajan ja budjetin, puutteesta. Monissa yliopistoissa tietoturva-aiheisiin ei ole varattu riittävästi aikaa, ja budjetit eivät aina riitä tarjoamaan erityisiä tietoturvaharjoituksia tai -ympäristöjä, kuten penetraatiotestauksen tai verkkoliikenteen analyysin toteuttamiseen. Ajanpuute vaikeuttaa myös opettajien mahdollisuuksia pysyä ajan tasalla alan kehityksessä ja uusissa uhkakuvissa. Erityisesti ensimmäisen vuoden kursseilla aikataulutus koetaan ongelmalliseksi, koska peruskursseilla on niin paljon

käsiteltäviä aiheita ja uusien aiheiden lisääminen voi siirtää kurssin ydinasian käsittelyä sivuun. Lisäksi ohjelmoinnin ja ohjelmistotuotannon kursseilla aikahaaste on laajempi, koska on paljon erilaisia aiheita ja näkökulmia, joita myös pitäisi liittää osaksi kursseja mm. laatu, yksityisyys, kestävyys, vihreät näkökulmat, käytettävyys, tekoäly, ja tällöin tietoturva on vain yksi aihe monien muiden aiheiden joukossa. Kuitenkin, jos jokin uusi aihealue tai näkökulma lisätään kurssin sisältöön, se on pois jostain nykyisestä kurssilla käsiteltävästä aiheesta, näkökulmasta tai harjoituksista. Ajan ja resurssien puute vaikeuttaa myös opettajien mahdollisuuksia käyttää ulkoista materiaalia, sillä materiaalin vanheneminen ja jatkuva päivittäminen on haasteellista. Opettajat ovat kiinnostuneita tarjoamaan opiskelijoille laadukasta tietoturvaan liittyvää aineistoa, mutta materiaalin täytyy olla ajantasaista, laadukasta ja helposti integroitavissa kurssin sisältöön.

Opettajat ehdottavat useita kehitysehdotuksia, joilla kyberturvallisuusopetusta voitaisiin laajemminkin yliopistoissa parantaa ja tuoda lähemmäksi työelämän vaatimuksia. Näihin kuuluvat muun muassa erillisten kyberturvallisuuskurssien tarjoaminen, jotka keskittyvät juuri tietoturvanäkökulmiin ohjelmoinnin ja ohjelmistotuotannon näkökulmista; käytännön harjoitusten lisääminen, sekä eettisten kysymysten sekä kyberpsykologian käsitteleminen osana opetusta. Opettajat uskovat, että tietoturva/kyberturvallisuus tulisi käsitellä omassa kontekstissa, jolloin opiskelijat voivat oppia ymmärtämään sen merkityksen ja tarpeen eri teknisissä aiheissa. Useat nostivat esille tarpeen lisätä käytännönläheisiä harjoituksia, joissa opiskelijat pääsevät työskentelemään konkreettisten tietoturvakysymysten parissa. Tällaisia voisivat olla esimerkiksi harjoitustyöt, joissa opiskelijat tunnistavat tietoturva-aukkoja ja tekevät uhkamallinnuksia tai harjoittelevat turvallisten koodauskäytäntöjen käyttöä. Lisäksi ehdotettiin, että syventävien kurssien tulisi sisältää käytännön esimerkkejä ja ohjeita, jotka valmistavat opiskelijoita kohtaamaan tietoturvan haasteita työelämässä. Myös yritysyhteistyötä tulisi lisätä, jolloin yritysten kautta tulevat vierailijat toisivat työelämäyhteyttä ja merkitystä yliopistossa opetetuille aiheille.

Tietoturvaopetus on tärkeä, mutta haastava osa ohjelmoinnin ja ohjelmistokehityksen koulutusta. Tietoturvaan liittyvät asiat tulisi integroida osaksi kurssien sisältöjä opiskelijoiden taitotason mukaisesti. Erillisten tietoturvakurssien tarjoaminen ja käytännönläheisten oppimismenetelmien lisääminen voisivat auttaa vastaamaan työelämän odotuksiin tietoturvataitojen osalta. Tietoturvaopetuksen kehittäminen edellyttää lisäresursseja, strategista suunnittelua ja tarvittavien opetusmateriaalien saatavuutta. Tietoturvan ajantasainen ja monipuolinen opetus vaatii tiivistä yhteistyötä, riittäviä resursseja ja selkeää strategiaa siitä, miten tietoturvaan liittyvät oppimistavoitteet voidaan integroida eri kurssien sisältöihin ja opintojen tasoille.

Lähteet

DVV. (2024). Turvallisen sovelluskehityksen käsikirja - Sovelluskehitysopas - DVV external Confluence. https://wiki.dvv.fi/pages/viewpage.action?pageId=230470940 (2024-11-01)

ENISA (2022). European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework (2024-11-01)

Kiravuo, T., Timlin, P., Kemppainen, K., Eronen, J., & Seppänen, S. (2023). Ohjelmisto-turvallisuuden tila 2023. In Traficomin tutkimuksia ja selvityksiä. Traficom. https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/ohjelmistoturvallisuuden-tila-2023 (2024-11-01)

Majanoja, A.-M., Hakkala, A., Lehto, J., & Virtanen, S. (2024a). Suomen kyberturvallisuus-koulutusta tarjoavien yliopistojen koulutuksen osaajaprofiilit ja kurssien painotusalat. Reports from the Faculty of Technology no. 1, Turun yliopisto, Suomi, 2024.

Majanoja, A.-M., Ekqvist, J., Hakkala, A., & Virtanen, S. (2024b). Kyberturvallisuus-koulutuksen kehittäminen Suomessa: yritysten osaamistarvekartoitus. Reports from the Faculty of Technology no. 2, Turun yliopisto, Suomi, 2024.

Nai Fovino, I., Neisse, R., Hernandez Ramos, J., Polemi, N., Ruzzante, G., Figwer, M., & Lazari, A. (2019). A Proposal for a European Cybersecurity Taxonomy. JRC Technical Reports JRC118089, Publications Office of the European Union, Luxembourg. https://data.europa.eu/doi/10.2760/106002 (2024-10-08)

OWASP. (2024a). OWASP Developer Guide | Secure Development and Integration | OWASP Foundation. https://owasp.org/www-project-developer-guide/draft/foundations/secure_development/ (2024-11-01)

OWASP. (2024b). OWASP Secure Coding Practices - Quick Reference Guide | Secure Coding Practices | OWASP Foundation. https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/02-checklist/05-checklist (2024-11-01)

Liitteet

Liite 1: Ohjelmoinnin ja ohjelmistotuotannon opettajille suunnattu kysely

1. Mikä yliopisto on pääasiallinen työnantajasi? (Aalto-yliopisto, Helsingin yliopisto, Jyväskylän yliopisto, Lappeenranta-Lahden yliopisto, Oulun yliopisto, Tampereen yliopisto, Turun yliopisto, Vaasan yliopisto, Åbo Akademi).
2. Monivalintakysymys: minkä tasoisia ohjelmointikursseja/ ohjelmistokehityksen kursseja opetat? (Perusopinnot, Aineopinnot, Syventävät opinnot).
3. Onko sinulla suoritettuna ammattisertifikaatteja? Jos on, mitä sertifikaatteja? (Kyllä/Ei)
4. Koetko, että opettajilla pitäisi olla ammattisertifikaatteja? (Kyllä, mitä sertifikaatteja, Ei, kuvaa tarkemmin)
5. Miten hyvin tällä hetkellä pystyt huomioimaan turvallisen ohjelmoinnin/turvallisen ohjelmistokehityksen aiheita kurssien suunnittelussa ja toteutuksessa? (Ei lainkaan, Harvoin, Joskus, Usein, Hyvin usein)
6. Kuinka paljon aikaa nykyisissä kursseissa käytetään turvallisen ohjelmoinnin/turvallisen ohjelmistokehitykseen liittyvien aiheiden käsittelyyn? (Kurssien tasot: Perusopinnot, Aineopinnot, Syventävät opinnot; Vastausvaihtoehdot: Ei lainkaan, Harvoin, Joskus, Usein, Hyvin usein)
7. Opetatko ohjelmoinnin kursseja? (Kyllä/Ei) Huom! Kyllä-vastauksen valinnan jälkeen avautuu uusi kysymys, Kysymys 8. OWASP:in Secure Programming Practices listaus, jonka kautta tarkastellaan, miten paljon ehditään käsitellä turvallisen ohjelmoinnin periaatteita ohjelmoinnin kursseilla.
8. Millä tasolla kursseillasi käsitellään turvallisen ohjelmoinnin periaatteita? Valitse soveltuvat kaksi (2) kohtaa samasta kysymyksestä/riviltä: 1) aiheen käsittelystä (1-3) ja 2) tietoturvan yhteydestä ja vaikutuksesta (4-6) Kategoriat perustuvat OWASP Secure Programming Practices listaukseen.

- Vastausvaihtoehdot: 1. Ei käsitellä, 2. Mainitaan kurssilla, 3. Harjoitellaan kurssilla, 4. Ei mainita security-yhteyttä, 5. Mainitaan security-yhteys aiheen käsittelyn yhteydessä, 6. Korostetaan security-yhteyttä ja vaikutusta.

- Kategoriat: Input validation, Output encoding, Authentication and password management, Session management, Access control, Cryptographic practices, Error handling and logging, Data protection, Communication security, System configuration, Database security, File management, Memory management, General coding practices

9. Opetatko ohjelmistotuotannon/ohjelmistokehitykseen liittyviä kursseja? (Kyllä/Ei) Huom! Kyllä-vastauksen valinnan jälkeen avautuu uusi kysymys, Kysymys 10. OWASP:in Project Developer Guide ja DVV:n Turvallisen ohjelmistokehityksen käsikirjaan pohjautuva listaus, jonka kautta tarkastellaan miten paljon ehditään käsitellä turvallisen ohjelmistokehityksen periaatteita kursseilla.

10. Millä tasolla kursseillasi käsitellään turvallisen ohjelmistokehityksen periaatteita? Valitse soveltuvat kaksi (2) kohtaa samasta kysymyksestä/riviltä: 1) aiheen käsittelystä (1-3) ja 2) tietoturvan yhteydestä ja vaikutuksesta (4-6). Kategoriat perustuvat OWASP Project developer guide ohjeistukseen sekä Digi- ja väestötietoviraston Turvallisen ohjelmistokehityksen käsikirjaan.

    - Vastausvaihtoehdot: 1. Ei käsitellä, 2. Mainitaan kurssilla, 3. Harjoitellaan kurssilla, 4. Ei mainita security-yhteyttä, 5. Mainitaan security-yhteys aiheen käsittelyn yhteydessä, 6. Korostetaan security-yhteyttä ja vaikutusta.

    - Kategoriat: Requirements, including security requirements to backlog; Architectural risk analysis and Threat modelling; Architecture and Design, to design security into application; Architecture security is documented; Implementation, using controls; C1: Define Security Requirements, C2: Leverage Security Frameworks and Libraries; C3: Secure Database Access; C4: Encode and Escape Data; C5: Validate All Inputs C6: Implement Digital Identity; C7: Enforce Access Controls; C8: Protect Data Everywhere; C9: Implement Security Logging and Monitoring; C10: Handle All Errors and Exceptions; Testing and verification, including security testing; Static Application Security Testing (SAST); Dynamic Application Security Testing (DAST); Interactive Application Security Testing (IAST); Penetration testing; Technical debt, including security debt; Importance of training, including security training; Importance of culture building, including security mindset; DevSecOps; Supply Chain and Third party Dependencies; Software Bill of Materials (SBOM); Keeping track of what third party libraries are included; Ensuring the security of development environments and tools (e.g. updates, licences); Security and data protection responsibilities for

data flows are clearly defined; Quality of third-party components are clarified and monitored (automated); System logs and auditability; Code reviews, including security aspects; Software developer access rights, principle of least priviledge; Two-factor authentication for user IDs

11. Kysymyksien 6–10 pohjalta: mitä mielestäsi jää ohjelmoinnin ja ohjelmistokehityksen kursseilta puuttumaan, joka rakentaisi tietoturvaymmärryksen yhteyttä ohjelmistokehittäjille? (Esimerkiksi tietoturvalliset ohjelmointikäytännöt, haavoittuvuuksien tunnistaminen ja korjaaminen, salaus, käyttöoikeuksienhallinta, tietoturvatestaus jne.) (Tekstikenttä: Perusopinnot, Aineopinnot, Syventävät opinnot)

12. Millaisia haasteita koet tietoturvaan/turvallisen ohjelmoinnin/turvallisen ohjelmistokehitykseen liittyvien aiheiden opettamisessa? (Valitse kaikki sopivat vaihtoehdot) (Vastausvaihtoehdot: Kurssin sisältö on jo niin täynnä ettei mahdu kurssille, Rajalliset resurssit ja aika, Opiskelijoiden kiinnostuksen puute aihetta kohtaan, Opettajien oma tietoturvakompetenssi, Sopivan opetusmateriaalin puute, Vähäiset tietoturvaan liittyvät työkalut ja ohjelmistot, Joku muu, kerro tarkemmin)

13. Minkälaisia haasteita tai ongelmia koet turvallisen ohjelmoinnin/turvallisen ohjelmistotuotannon opettamisessa kursseilla?

Seuraavilla kysymyksillä pyritään arvioimaan, kuinka paljon tietoturvaan liittyvää tietämystä ylläpidetään, miten hyvin ehtii seuraamaan uusimpia tietoturvaan liittyviä aiheita sekä onko uutta tietoa mahdollista sisällyttää kursseihin.

14. Miten paljon tietoturva-aiheiden kehitystä ehdit seuraamaan ja ylläpitämään aiheeseen liittyvää osaamista? Vastausvaihtoehdot: Ei lainkaan, Harvoin, Joskus, Usein, Hyvin usein
    - Ehditkö pitää itsesi ajan tasalla tietoturva- ja turvallisen ohjelmistokehityksen aiheissa??
    - Seuraatko esim. tietoturva-alan julkaisuja, konferensseja tai kursseja?
    - Miten usein tämä uusi tietoturvaan liittyvä tieto heijastuu kurssien sisältöön ja opetusmetodeihin?
15. Miten tietoturvaopetus näkyy osana nykyistä opetusta? Vastausvaihtoehdot: Ei lainkaan, Vähän, Joskus, Usein, Hyvin usein
    - Kuinka tärkeänä pidät tietoturvan/turvallisen ohjelmoinnin/turvallisen ohjelmistokehityksen opettamista ohjelmointikursseilla?

- Miten mielestäsi nykyinen ohjelmoinnin ja ohjelmistokehityksen opetussuunnitelma vastaa teollisuuden vaatimuksia tietoturvaosaamisessa?
- Kuinka usein päivität tietoturvaan, turvalliseen ohjelmointiin/turvalliseen ohjelmistokehitykseen liittyviä opetusmateriaaleja ja käytäntöjä?

16. Kerro tarkemmin kysymysten 14–15 perusteella vastauksistasi, pohdinnoistasi, haasteistasi ja tarpeistasi.

Seuraavien kysymyksien kautta pyrimme tunnistamaan hyviä ideoita kyberturvallisuuteen/turvalliseen ohjelmointiin/turvalliseen ohjelmistokehitykseen liittyviä aiheita ja harjoituksia, joita olisi hyvä käsitellä kursseilla kehittäen ohjelmistokehittäjien osaamista.

Näitä kyselyssä koottuja ajatuksia ja ideoita käytetään OKM:n kyberturvallisuushankkeessa koulutuksien ja kurssien sisältöjen kehittämiseen.

17. Ideointia ja tarpeita: Ideaalitilanteessa, mitä turvallisen ohjelmoinnin/turvallisen ohjelmistokehityksen aiheita ohjelmoinnin ja/tai ohjelmistotuotannon kursseilla olisi hyvä opettaa? Kerro myös kurssin taso (perus, aine, syventävä)

18. Ideointia ja tarpeita: Ideaalitilanteessa, minkälaisia turvallisen ohjelmoinnin/turvallisen ohjelmistokehityksen harjoituksia voisi tuoda osaksi ohjelmoinnin ja ohjelmistokehityksen kursseja?

19. Jos olisi tietoturva-aiheisiin liittyvää kurssimateriaalia valmiina tarjolla (luentovideoita, lukumateriaaleja, harjoituksia, tms.), tajoaisitko niitä opiskelijoille osana kurssiasi? (Vastausvaihtoehdot: Kyllä, osana kurssia, Kyllä, vapaaehtoisena materiaalina, En tarjoaisi, kerro tarkemmin)

20. Muita kommentteja tai asioita, joita haluat ottaa esille ja kyberkoulutushankkeen pohdittavaksi?

University of Turku
Reports from the Faculty of Technology

1. **Anne-Maarit Majanoja, Antti Hakkala, Jari Lehto & Seppo Virtanen**. Suomen kyberturvallisuuskoulutusta tarjoavien yliopistojen koulutuksen osaajaprofiilit ja kurssien painotusalat. 2024.
2. **Anne-Maarit Majanoja, Jani Ekqvist, Antti Hakkala & Seppo Virtanen**. Kyberturvallisuuskoulutuksen kehittäminen Suomessa: yritysten osaamistarve-kartoitus. 2024.
3. **Anne-Maarit Majanoja, Antti Hakkala, Ville Leppänen & Seppo Virtanen**. Tietoturva ohjelmoinnin ja ohjelmistotuotannon kursseilla Suomen yliopistoissa – nykytila ja opettajien näkemykset. 2024.