UNIVERSITY OF TURKU
Faculty of Technology

Suomen kyberturvallisuus-koulutusta tarjoavien yliopistojen koulutuksen osaajaprofiilit ja kurssien painotusalat

Anne-Maarit Majanoja, Antti Hakkala, Jari Lehto, Seppo Virtanen

Reports from the Faculty of Technology No. 1

University of Turku, Finland, 2024

UNIVERSITY
OF TURKU
Faculty of Technology

Reports from the Faculty of Technology No. 1
University of Turku, Finland, 2024

Teknillisen tiedekunnan raportteja nro 1
Turun yliopisto, 2024

ISBN 978-951-29-9916-3 (PDF)
ISSN 2984-360X (Online)

TIIVISTELMÄ

Tekijät: Anne-Maarit Majanoja[1,*], Antti Hakkala[1], Jari Lehto[1], Seppo Virtanen[1]
Otsikko: Suomen kyberturvallisuuskoulutusta tarjoavien yliopistojen koulutuksen osaajaprofiilit ja kurssien painotusalat
Julkaisun tiedot: Reports from the Faculty of Technology No. 1, University of Turku, Finland, 2024, 94 pages

Tässä raportissa kuvataan Kansallisen kyberturvallisuuskoulutuksen yhteistyöverkoston rakentaminen -hankkeen työvaihe 2:n aikana toteutettu selvitys hankkeeseen osallistuvien yliopistojen kyberturvallisuusalan koulutuksen sisällöistä. Tarkastelun kohteena oli, miltä kyberturvallisuuskoulutus näyttää kokonaisuutena suhteutettuna eurooppalaiseen kyberturvallisuusroolitukseen ja avainosaamisiin, sekä mitä aiheita Suomen yliopistojen kyberturvallisuuskoulutuksessa katetaan. Arviointi perustui työvaihe 2:n aikana toteutettuun koulutuksen sisältöjen arviointityökaluun, jossa linkitettiin eurooppalaiset kyberturvallisuusroolien avainosaamiset (ENISA) ja eurooppalainen kyberturvallisuustaksonomia (JRC) kursseilla käsiteltäviin aiheisiin. Tämän arviointityökalun pohjalta luotiin tietokanta ja verkkosivusto yliopistojen kurssitietojen syöttämistä varten.

Tarkastelun perusteella kyberturvallisuusalan kursseja tarjotaan useissa yliopistoissa, mutta kurssien määrä vaihtelee merkittävästi. Työvaihe 2:n aikana kerättiin tiedot yhteensä 82 kurssista. Tämän perusteella on nähtävissä, että Suomessa eniten kyberturvallisuusalan kursseja tarjoavat Jyväskylän yliopisto ja Turun yliopisto (n. 20 - 30 kurssia kumpikin). Oulun yliopisto ja Tampereen yliopisto tarjoavat n. 10 -15 kurssia kumpikin, muut yliopistot tarjoavat yksittäisiä kursseja. Asteikolla 0 (ei käsitellä lainkaan) – 3 (käsittelyn keskiössä) pisteytettynä kurssien opettajat katsovat, että toteutuksissa teorian syvyys on välillä 1,2–2,2 ja käytännön harjoitusten toteutuksen syvyys välillä 1,5–2. Harjoituksissa käsiteltävien aiheiden määrä on selkeästi vähäisempi verrattuna teoreettisten aiheiden käsittelyyn. Yksi keskeinen löydös on, että käytännön harjoituksia tulisi kehittää lisää, jotta ne kattaisivat enemmän aiheita ja mahdollistaisivat syvällisemmän käytännön harjoittelun jo opintojen aikana.

Suomen kyberturvallisuuskoulutus painottuu vahvasti CISO- (Chief Information Security Officer) ja Cyber Incident Responder -rooleihin. Koulutukset kattavat laajan kirjon kyberturvallisuusosaamista, painottuen teknisiin taitoihin ja täydentäen niitä operatiivisilla, strategisilla ja hallinnollisilla taidoilla. Useiden yliopistojen koulutustarjonnassa on toistuvia sisällöllisiä yhteneväisyyksiä, mikä osoittaa yhteisymmärrystä perustaitojen tarpeellisuudesta. Yliopistojen välistä yhteistyötä perusopetuksen osalta voisi harkita, mutta kurssien osallistujamäärät, tutkintorakenteiden vaatimukset ja aikataulut voivat estää tämän.

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

Raportissa tuodaan esille myös kyberturvallisuustaksonomian aiheita, jotka ovat vähiten käsiteltyjä yliopistoissa, kuten tietoturvatestaus, riskienhallinta, tietoturvakäytäntöjen noudattaminen ja tekoälyyn liittyvät näkökulmat. Kehitysehdotuksena suositellaan käytännön harjoitusten lisäämistä, erityisesti tietoturvatestauksessa, sekä lyhytkurssien ja täydennyskoulutuksen kehittämistä työelämän tarpeisiin. Myös ajasta ja paikasta riippumattomien kurssien nykyistä laajempaa toteutusta kannattaa harkita. Yritysyhteistyö on tärkeää, ja kurssien rakentaminen yhteistyössä alan toimijoiden kanssa voisi tehostaa koulutusta ja varmistaa, että opetuksen sisältö vastaa ajankohtaisia ja tulevaisuuden tarpeita.

AVAINSANAT: Kyberturvallisuuskoulutus, Koulutuksen kehittäminen, Kyberturvallisuusroolit, Taksonomia, Opetuksen kehittämisen arviointityökalu

Sisällys

1 Johdanto

Kansallisen kyberturvallisuuskoulutuksen yhteistyöverkoston rakentamisen hankkeeseen osallistuu yhdeksän suomalaista yliopistoa, joissa järjestetään kyberturvallisuusalan koulutusta. Hankkeen rahoittajana toimii Suomen opetus- ja kulttuuriministeriö. Hankeaika on 1.1.2023-31.12.2025.

Hankkeeseen osallistuvat yliopistot ovat:
- Jyväskylän yliopisto
- Turun yliopisto
- Tampereen yliopisto
- Vaasan yliopisto
- Lappeenrannan-Lahden teknillinen yliopisto
- Helsingin yliopisto
- Aalto-yliopisto
- Oulun yliopisto
- Åbo Akademi

Hanke jakautuu neljään työvaiheeseen. Tämä raportti on yksi Turun yliopiston johdolla toteutettavaan työvaiheeseen 2 liittyvistä tuotoksista. Osana työvaiheessa suoritettavaa koulutustarveanalyysiä tässä raportissa selvitetään yliopistojen nykyisen koulutustarjonnan sisältö peilaten sitä Euroopan komission yhteisen tutkimus-keskuksen (European Commission Joint Research Centre, JRC) määrittämään kyberturvallisuustaksonomiaan (JRC Cybersecurity Taxonomy) (Nai Fovino et al., 2019) ja Euroopan unionin kyberturvallisuusviraston (European Union Agency for Cybersecurity, Enisa) määrittämiin kyberturvataitojen osaajaprofiileihin (ECSF role profiles) (European Union Agency for Cybersecurity ECSF, 2022). Koulutustarveanalyysin osana suoritetaan myös erillinen yrityksille suunnattu osaamistarvekartoitus. Yrityksille suunnatun tarvekartoituksen tuloksia käsitellään työvaihe 2:n toisessa raportissa (Majanoja et al., 2024). Tämän raportin ja yritysten osaamistarvekartoituksen tulosten perusteella pystytään tunnistamaan potentiaalisia korkeakoulujen koulutussisältöjen kehittämissuuntia. Hankkeen koulutustarveanalyysiosa toteutettiin 1.6.2023 - 30.6.2024. Työvaihe 2 jatkuu koulutustarveanalyysiin perustuvalla nykyisten ja uusien kurssien ja koulutuskokonaisuuksien kehittämisellä, ja näiden kurssien ja koulutuskokonaisuuksien toteuttamisella hankesuunnitelman mukaisesti.

Työvaihe 2:n yhteydessä toteutettiin koulutuksen sisältöjen kehittämisen arviointityökalu. Aiemman tutkimuksen pohjalta ja tämän hankkeen aikana jatkokehitetty koulutuksen sisällön arviointityökalu on suunniteltu tukemaan kyberturvallisuuskurssien sisällöllistä kehittämistä. Työkalun avulla on mahdollista arvioida ja tarkastella kurssien sisältöjä kyberturvallisuustaksonomian kautta, mikä edistää opetussuunnitelmien täsmentämistä ja niiden relevanssin varmistamista työelämän vaatimuksiin nähden. Lisäksi työkalun kautta saatavat tulokset mahdollistavat suoran kommunikaation opiskelijoiden kanssa, linkittäen opetussisällöt selkeästi eurooppalaiseen kyberturvallisuusalan rooleihin, edistäen opiskelijoiden ymmärrystä koulutuksen ja työelämän yhteyksistä. Arviointityökalua ei ole suunniteltu tai tarkoitettu yliopistojen väliseen vertailuun tai paremmuusjärjestyksen määrittämiseen. Tässä raportissa tuloksia ja havaintoja esitetään koko Suomen tasolla ja yksittäisten yliopistojen osalta aakkosjärjestyksessä. Yksittäisten yliopistojen osalta tässä raportissa suoritetaan yliopistokohtainen tarkempi tarkastelu vain siinä tapauksessa, että arviointityökaluun on saatu vähintään yhdeksän kurssin sisältötiedot kyseisestä yliopistosta. Jos yliopisto on toimittanut sisältötiedot alle yhdeksästä kurssista, huomioidaan tiedot ainoastaan kansallista kokonaisuutta tarkasteltaessa. Vähintään yhdeksän kurssin sisältötiedot toimittivat Jyväskylän yliopisto, Oulun yliopisto, Tampereen yliopisto ja Turun yliopisto.

2 Arviointityökalun määrittäminen sekä käytetyt viitekehykset, standardit ja taksonomiat

Tässä luvussa käydään läpi hankkeessa käytetyt eurooppalaiset viitekehykset, taksonomiat ja kyberturvallisuusroolit (Luku 2.1). Luvussa 2.2 esitellään tutkimuksen ja hankkeen aikana kehitetty kyberturvallisuuskurssien sisältöjen tarkasteluun kehitetty viitekehys. Luku 2.3 esittelee kurssitietojen keräämiseen kehitetyn työkalun ja miten kurssitiedot kerättiin hankkeeseen osallistuneilta yliopistoilta. Luvussa 2.4 esitetään hankkeen aikana kerätyt kurssimäärät yliopistokohtaisesti sekä se, miten kukin yliopisto/vastuuopettaja on arvioinut kurssin teoria- ja harjoitusten toteutuksen tason.

2.1 Käytetyt eurooppalaiset taksonomiat ja kyberturvallisuusalan roolikuvaukset

Eurooppalainen kyberturvallisuustaitojen kehys (ECSF). ENISA:n (Euroopan unionin kyberturvallisuusvirasto) kehittämä Euroopan kyberturvallisuustaitojen kehys (ECSF) on suunniteltu tukemaan kyberturvallisuusammattilaisten rooliprofiilien määrittelyä ja kuvaamista Euroopassa. Tämä kehys auttaa ymmärtämään ja määrittämään tarvittavia taitoja ja kompetensseja, jotka liittyvät kuhunkin kyberturvallisuusrooliin. ECSF:n tavoitteena on luoda yhteinen ymmärrys kyberturvallisuusammattilaisten rooleista, tehtävistä, taidoista ja osaamisvaatimuksista, mikä helpottaa kyberturvallisuuskoulutusohjelmien suunnittelua ja kyberturvallisuustaitojen tunnistamista. (ENISA, 2022; European Union Agency for Cybersecurity ECSF, 2022)

ECSF sisältää 12 tyypillistä kyberturvallisuusammattilaisten rooliprofiilia, joiden tehtävät, taidot ja osaamisvaatimukset on määritelty tarkasti: Chief Information Security Officer (CISO), Cyber Incident Responder, Cyber Legal, Policy & Compliance Officer, Cyber Threat Intelligence Specialist, Cybersecurity Architect, Cybersecurity Auditor, Cybersecurity Educator, Cybersecurity Implementer, Cybersecurity Researcher, Cybersecurity Risk Manager, Digital Forensics

Investigator, Penetration Tester (European Union Agency for Cybersecurity ECSF, 2022). Kehys edistää myös kyberturvallisuuskoulutuksen yhdenmukaistamista ja tukee kyberturvallisuustyövoiman kehittämistä koko Euroopassa. Tämä kehys toimii myös viitekehyksenä, jota voidaan käyttää apuna EU:n laajuisten kyberturvallisuus-strategioiden ja -toimenpiteiden suunnittelussa.

JRC:n kyberturvallisuustaksonomia. JRC:n (Euroopan komission yhteinen tutkimuskeskus) kehittämä kyberturvallisuuden taksonomia on suunniteltu yhtenäistämään kyberturvallisuuden terminologiat, määritelmät ja toimialueet koko EU:ssa. Taksonomia auttaa luokittelemaan kyberturvallisuusosaamista ja edistämään yhteistyötä EU:n kyberturvallisuuslaitosten välillä. Taksonomia koostuu neljästä ulottuvuudesta: toimialueista, sektoreista, teknologioista ja käyttö-tapauksista. Se sisältää standardeja, säädöksiä ja parhaita käytäntöjä, ja sen ovat validoineet EU:n kyberturvallisuustoimijat, kuten Euroopan kyberturvallisuusjärjestö (ECSO). (Nai Fovino et al., 2019)

JRC:n taksonomia on keskeinen osa Euroopan kyberturvallisuusverkoston kehittämistä. Sen tarkoituksena on parantaa EU:n kyberturvallisuusvalmiuksia tarjoamalla jäsennelty kehys olemassa olevan asiantuntemuksen ja resurssien tunnistamiseen ja hyödyntämiseen Euroopassa (Nai Fovino et al., 2019).

JRC:n "A Proposal for a European Cybersecurity Taxonomy" -dokumentissa on esitetty 15 päätason aihealuetta (domain) kattaen laajan kirjon kyberturvallisuuden osa-alueita, jotka ovat oleellisia tutkimuksen, koulutuksen ja teollisuuden tarpeiden osalta (Nai Fovino et al., 2019). Näiden 15 päätason aihealueen lisäksi lisättiin tässä tutkimuksessa/arviointityökalun kehittämisvaiheessa mukaan uutena päätason aihealueenakohta 16, Artificial intelligence and machine learning. Tämä määriteltiin ENISA:n AI/ML-raporttien pohjalta: ENISA Report – Securing Machine Learning Algorithms (ENISA, 2021) ja Multilayer Framework for Good Cybersecurity Practices for AI (ENISA, 2023). On perusteltua lisätä AI/ML JRC:n kyberturvallisuuden taksonomian aihealuelistaan, koska AI/ML-teknologiat ovat keskeisiä kyberuhkien havaitsemisessa ja torjunnassa, kyberhyökkääjät hyödyntävät niitä, ne mahdollistavat monien kyberturvallisuustehtävien automaation ja tuovat mukanaan uusia eettisiä ja lainsäädännöllisiä haasteita. Lisäksi AI/ML:n rooli nykyaikaisessa kyberturvallisuudessa tekee siitä tärkeän osa-alueen, joka ansaitsee oman kategoriansa taksonomiassa.

Taksonomian aihealueet (Nai Fovino et al., 2019):

1. Assurance, Audit, and Certification: 4 alakohtaa
2. Cryptology (Cryptography and Cryptanalysis): 14 alakohtaa
3. Data Security and Privacy: 9 alakohtaa
4. Education and Training: 5 alakohtaa
5. Human Aspects: 18 alakohtaa
6. Identity Management: 6 alakohtaa
7. Incident Handling and Digital Forensics: 10 alakohtaa
8. Legal Aspects: 5 alakohtaa
9. Network and Distributed Systems: 14 alakohtaa
10. Security Management and Governance: 13 alakohtaa
11. Security Measurements: 3 alakohtaa
12. Software and Hardware Security Engineering: 25 alakohtaa
13. Steganography, Steganalysis, and Watermarking: 3 alakohtaa
14. . Theoretical Foundations: 6 alakohtaa
15. Trust Management and Accountability: 12 alakohtaa
16. Artificial intelligence and machine learning: 9 alakohtaa

e-Competence Framework (e-CF). e-CF on eurooppalainen standardi, joka tarjoaa yhteisen viitekehyksen ICT-alan ammattilaisten osaamisen arvioimiseen ja kehittämiseen. e-CF on kehitetty tukemaan organisaatioita ja yksilöitä määrittelemään ja hallitsemaan ICT-osaamisvaatimuksia. Se sisältää yksityiskohtaisia kuvauksia taidoista, tietämyksestä ja asenteista, joita tarvitaan eri ICT-rooleissa. Standardi on suunniteltu olemaan joustava ja sovellettavissa eri sektoreilla ja eri kokoisissa organisaatioissa. e-CF auttaa yhdenmukaistamaan koulutusohjelmia ja ammattikuvauksia, mikä parantaa ICT-alan työntekijöiden liikkuvuutta ja työllistettävyyttä koko Euroopassa. (European Committee for Standardization, 2019)

E-kompetenssien ja ENISA:n kompetenssien yhtenäistäminen mahdollistaa johdonmukaisen lähestymistavan kyberturvallisuuden taitoihin ja osaamisiin eri sektoreilla ja maissa. Jokaiselle roolille on määritelty keskeiset kompetenssit, jotka kuvaavat tarvittavaa osaamista ja taitoja. Nämä kompetenssit vastaavat usein erilaisia e-competensseja, jotka kattavat teknologiset, hallinnolliset ja strategiset kyvykkyydet. (European Committee for Standardization, 2019)

2.2 Arviointikehyksen laatiminen: JRC:n taksonomian, ENISA:n roolien ja yliopiston kurssien yhdistäminen

Tutkimuksessa kehitetyn viitekehyksen avulla yliopistot pystyvät suunnittelemaan ja tarkastelemaan kyberturvallisuuden opetussuunnitelmiaan peilaten niitä eurooppalaisiin ammatillisiin profiileihin ja taitovaatimuksiin. Tavoitteena oli yhdistää Euroopan kyberturvallisuustaksonomia (ECT) ja European Cybersecurity Skills Framework (ECSF) yliopistojen nykyisiin opetussuunnitelmiin, tunnistaa mahdolliset puutteet ja varmistaa opetuksen laatu. Arviointikehyksen yleiskuvaus on käsitelty julkaisussa: Framework for Evaluation of Cybersecurity Curriculum Educational Content - Antti Hakkala, Anne-Maarit Majanoja, Ville Leppänen, Seppo Virtanen (2023).

ENISA:n kyberturvallisuusroolien ja JRC:n taksonomian yhdistämisen yleiskatsaus. Kyberturvallisuusroolien ja taksonomian linkitys tehtiin aluksi laajoilla taulukoilla, ja tiedot tulostettiin paperille ja järjestettiin fyysisesti seinälle paremman visualisoinnin ja ristiviittausten helpottamiseksi. Linkityksen toteutuksen kuvaus on löydettävissä julkaisusta: Framework for Evaluation of Cybersecurity Curriculum Educational Content - Antti Hakkala, Anne-Maarit Majanoja, Ville Leppänen, Seppo Virtanen (2023).

Linkityksen toteutuksen vaiheet:

1. **Keskeisten komponenttien tunnistaminen**:
    - **ENISA:n roolit:** ENISA:n kehittämä European Cybersecurity Skills Framework (ECSF) määrittelee 12 erillistä kyberturvallisuuden roolia. Jokainen rooli liittyy tiettyihin taitoihin, tietoihin, tehtäviin ja osaamisiin. Tässä roolin avainosaaminen (Key Competences) nostettiin tarkasteluun.
    - **JRC:n taksonomia:** European Cybersecurity Taxonomy (ECT) luokittelee kyberturvallisuuden tietämysalueet neljään ulottuvuuteen: teknologiat, alueet, sektorit ja käyttötapaukset. Tämä taksonomia tarjoaa rakenteellisen tavan tunnistaa ja luokitella koulutuksen kannalta keskeiset aiheet.
    - **e-CF:n kompentenssien tunnistaminen.** ENISA:n kyberturvallisuus-rooleihin on tunnistettu suoraan e-CF kuvauksia taidoista, tietämyksestä, asenteista. Nämä roolien mukaiset e-CF kompetenssit linkitettiin samalla tavalla osana roolia kuin roolin avainosaaminen.

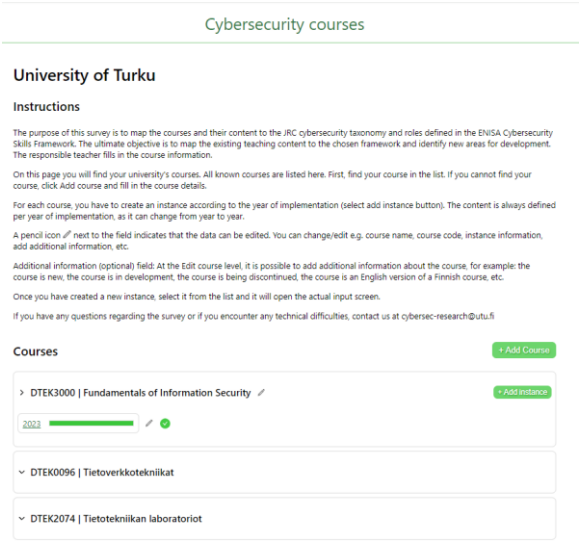
2. **Roolien ja keskeisen tietämyksen linkitys**:
    - Jokaisen ENISA:n roolin keskeiset tietämysalueet sekä e-CF kompetenssit linkitettiin ECT-taksonomian kohtiin. Tämä vaihe on keskeinen, koska siinä yhdistetään tiettyjen kyberturvallisuusroolien vaatimukset laajempiin ECT:n määrittelemiin kategorioihin.
    - Toteutettu linkitys on rooliriippuvainen, ja siinä otetaan huomioon kunkin roolin erityispiirteet, kuten hyökkäys-/puolustusorientaatio tai tekniset/lakiasiat.
    - Jokaiselle roolille on määritelty erilaisia avainosaamisia (Key Competences). Tämä avainosaaminen on määritelty ja linkitetty per rooli. Tästä syystä jokainen avainosaaminen on roolispesifinen ja avainosaaminen ei ole kaikkien roolien yhteisarvo vaan yksittäisen roolin avainosaamisen arvo.
3. **Kurssisisältöjen arviointi**:
    - Kyberturvallisuuskoulutuksen kurssisisällöt analysoitiin ja luokiteltiin.
    - Kurssisisällöt sovitettiin ECT-taksonomian kategorioihin, jotta voitiin selvittää, mitkä alueet katetaan ja kuinka laajasti.
4. **Puuteanalyysi ja arviointi**:
    - Linkitettyjen tietojen avulla voitiin tunnistaa opetussuunnitelman mahdolliset puutteet tai parannuskohteet. Opetussuunnitelma arvioitiin sen perusteella, kuinka hyvin se kattaa vaaditut tietämysalueet kullekin roolille, mikä helpotti tarvittavien muutosten ja parannusten tekemistä.

Prosessin tuloksena saatiin kattava ymmärrys siitä, kuinka hyvin nykyinen opetussuunnitelma vastaa yritysten tarpeita ja taksonomiassa esitettyjä aiheita (käytössä eurooppalainen roolimääritys ja taksonomia). Rakenteellinen lähestymistapa mahdollisti puutteiden tunnistamisen ja tarjosi systemaattisen tavan parantaa ja sovittaa opetussuunnitelmaa ammatillisten roolivaatimusten mukaiseksi.

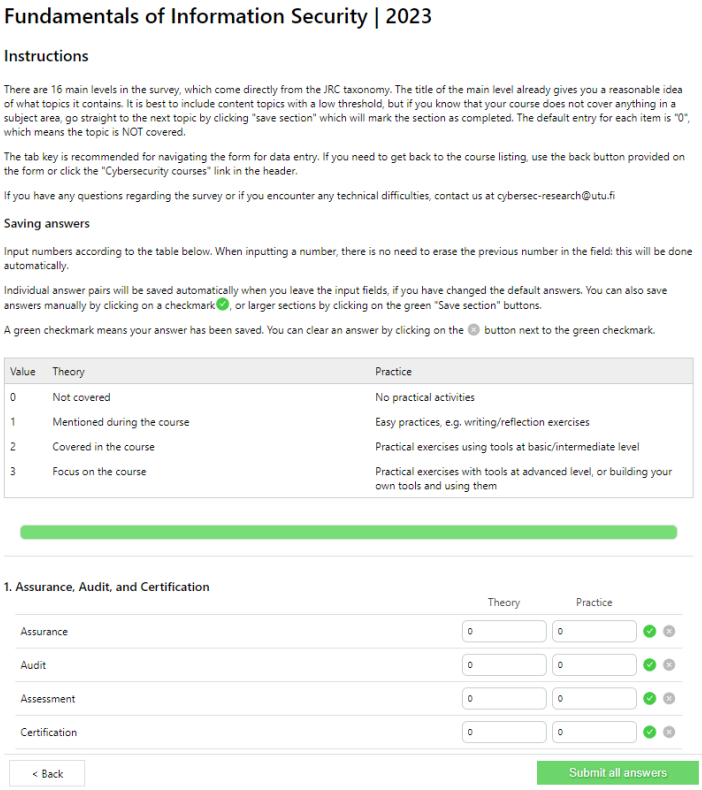
Tämän tarkastelun avulla on mahdollista varmistaa, että kyberturvallisuuden koulutusohjelmat ovat linjassa teollisuuden roolien sekä keskeiseen tietämykseen liittyvien tarpeiden kanssa (kyberturvallisuuden taksonomia), mikä valmistaa opiskelijoita paremmin tuleviin kyberturvallisuusalan urapolkuihin. Tämä systemaattinen lähestymistapa tukee myös opetussuunnitelman jatkuvaa parantamista ja koulutustulosten sovittamista kyberturvallisuusalan muuttuviin tarpeisiin.

2.3 Kyberturvallisuuskurssien datan kerääminen

Kyberturvallisuuskurssien datan keräämistä varten toteutettiin web-työkalu, jonka kautta yliopistot (käytännössä kunkin kurssin vastuuopettajat) pystyivät syöttämään kurssikohtaiset arviot kurssien teorian ja käytännön toteutuksista. Kurssien sisällöt kerättiin JRC:n taksonomian mukaisesti, sisältäen 16 päädomainia (AI/ML-lisäyksen jälkeen). Keräystyökalua varten rakennettiin tietokanta, linkitys rakennettiin kantaan roolien Key Competences (avainosaaminen) -tiedon ja JRC:n taksonomian välille aiemmin mainitun artikkelin mukaisesti. Web-työkalussa jokaiselle yliopistolle oli syötetty valmiiksi kurssit hankkeen työvaihe 1:n aikana raportoitujen tietojen mukaisesti (Kuva 1), ja vastuuopettajat syöttivät web-työkalussa kurssien osalta tiedot kurssin toteutusajankohdasta (esim. 2023/2024), mahdolliset kurssin lisätiedot (sama kurssi toteutetaan suomeksi ja englanniksi), sekä tiedot teorian ja käytännön (Kuva 2) osalta asteikolla 0–3 (Taulukko 1). Kurssien tietoja kerättiin 22.3.2024 – 2.5.2024 välisenä ajankohtana.



Kuva 1. Kurssilistausnäkymä ja uuden instanssin lisääminen arviointityökalussa



Kuva 2. Kurssin teoria ja käytäntö -arvioiden syöttäminen arviointityökalussa asteikolla 0–3

Taulukko 1. Kurssien syöttämisessä käytetty asteikko

Arvo	Teoria	Practice
0	Not covered	No practical activities
1	Mentioned during the course	Easy practices, e.g. writing/reflection exercises
2	Covered in the course	Practical exercises using tools at basic/ intermediate level
3	Focus on the course	Practical exercises with tools at advanced level, or building your own tools and using them

2.4 Suomen yliopistojen raportoimat kurssit hankkeen työvaihe 2:n aikana

Työvaihe 2:n aikana yliopistot kirjasivat Taulukon 2 osoittamat kurssimäärät työkaluun. Työvaihe 2:n aikana syötettyjen kurssimäärien pohjalta on nähtävissä (Taulukko 2 ja Taulukko 3), että Suomessa on kaksi yliopistoa, jotka tarjoavat kokonaisen kyberturvallisuusalaan suuntautuvan ylemmän tutkinnon. Suurimmat kyberturvallisuuskoulutusta tarjoavat yliopistot ovat Turun yliopisto (27 kurssia: 5 perusopintotasoista, 4 aineopintotasoista, 17 syventävää kurssia) ja Jyväskylän yliopisto (21 kurssia: 1 perusopintotasoinen, 1 aineopintotasoinen, 19 syventävää kurssia).

Taulukko 2. Työvaihe 2:n aikana syötetyt kurssitiedot yliopistokohtaisesti. ** Jos jokin kurssi oli osittain syötetty työkaluun ja lopullinen hyväksyntä oli jäänyt tekemättä, nämä kurssikirjaukset määriteltiin valmiiksi ja lopullisiksi kurssin tiedoiksi.

Yliopisto	**TP2:ssa raportoidut kurssit** **Valmis****	**TP1:ssä annettu kurssien määrä**	**Lisätieoja kursseista, joita ei ole ilmoitettu TP2:n aikana**
Jyväskylän yliopisto	21	22	
Turun yliopisto	27	27	
Tampereen yliopisto	13	16	Yksi kurssi korvattu toisella kurssilla
Oulun yliopisto	9	10	
Vaasan yliopisto	3	3	
Helsingin yliopisto	3	5	
Aalto-yliopisto	3	8	
Lappeenrannan-Lahden teknillinen yliopisto	2	3	Yksi kurssi tarjotaan sekä suomeksi että englanniksi
Åbo Akademi	1	1	

Edellisten lisäksi kaksi yliopistoa tarjoaa valinnaisia kurssikokonaisuuksia, joissa opiskelijan on mahdollista suuntautua tutkinnossaan kyberturvallisuusalalle. Tampereen yliopisto tarjoaa 13 kyberturvallisuusalan kurssia (4 perusopintotasoista, 4 aineopintotasoista, 3 syventävää kurssia) ja Oulun yliopisto 9 kurssia (2 aineopintotasoista kurssia, 7 syventävää kurssia). Tampereen yliopiston tarjoamia tuotantotalouden kyberturvallisuuden kannalta relevantteja kursseja ei ole syötetty työkaluun.

Näiden lisäksi muut viisi yliopistoa tarjoavat yksittäisiä kursseja, jotka ovat osa kansallista kyberturvallisuuden kokonaiskuvaa, mutta yksittäisten kurssien pohjalta ei ole mahdollista määrittää näille yliopistoille suuntautumis- tai painopisteitä kurssien osalta. Vaasan yliopisto syötti tiedot yhdestä perusopintotasoisesta ja kahdesta syventävästä kurssista. Helsingin yliopistolta saatiin tiedot kolmesta syventävästä kurssista. Aalto-yliopisto syötti tiedot yhdestä aineopintotasoisesta ja yhdestä syventävästä kurssista. Lappeenranta-Lahden teknillinen yliopisto toimitti tiedot yhdestä aineopintotasoisesta ja yhdestä syventävästä kurssista. Åbo Akademi raportoi yhden perusopintotasoisen kurssin.

Raportoitujen kurssien pohjalta voidaan todeta, että Suomessa kyberturvallisuuskursseja tarjotaan useissa yliopistoissa, mutta tarjonnan yliopistokohtainen määrä vaihtelee merkittävästi. Kurssien tasot jakautuvat perustason, aine- ja syventävien opintojen kesken. Perusopintotasoisia kursseja on yhteensä kahdeksan, aineopintotasoisia kursseja on 13 ja syventävien opintojen kursseja 64. Suurin osa kursseista on siis syventäviä opintoja, mikä osoittaa vahvaa panostusta erityisesti ylemmän tutkinnon edistyneeseen kyberturvallisuuden opetukseen. Perus- ja aineopintotason kursseja on vähemmän. Näitä opintoja voidaan tarjota jo osana alempaa tutkintoa. Perus- ja aineopintotasoisia kursseja lisäämällä opiskelijat voisivat rakentaa vahvan kyberturvallisuusosaamisen pohjan jo ennen siirtymistä syventäviin opintoihin, jolloin opintopolku kyberturvallisuuteen olisi kattavampi alusta lähtien ja mahdollistaisi alan osaamisen tuomisen työmarkkinoille jo valmistuessa kandidaatintutkintoon nykyistä paremmin. Toisaalta on kuitenkin huolehdittava siitä, että ylempien tutkintojen lähtötaso ei muutu liian vaativaksi kansallisen ja kansainvälisen opiskelijaliikkuvuuden mahdollistamisen kannalta ns. Bologna-mallin mukaisesti.

Taulukko 3. Arviointityökaluun raportoidut kurssit per yliopisto. Ka = keskiarvo, Md = mediaani

Yliopisto	Kurssin nimi	Instanssin vuosi	Taso	Teoria Ka.	Harjoitus Ka.	Teoria Md.	Harjoitus Md.
Aalto-yliopisto: 3 kurssia							
Aalto	Information Security	2024	intermediate	1,6	0,0	2	0
Aalto	Network Security	2024	advanced	2,3	0,0	2	0
Aalto	Platform Security	2024	advanced	1,8	2,0	2	2
Åbo Akademi: 1 Kurssi							
ÅA	Introduktion till cybersäkerhet	2025	basic	1,0	2,0	1	2

Yliopisto	Kurssin nimi	Instanssin vuosi	Taso	Teoria Ka.	Harjoitus Ka.	Teoria Md.	Harjoitus Md.
Lappeenranta-Lahden teknillinen yliopisto: 2 Kurssia							
LUT	*Foundation of Cybersecurity	2024	advanced	1,9	2,3	2	2
LUT	Cyber Security of Software Systems	2024	intermediate	1,6	1,0	2	1
Helsingin yliopisto: 3 Kurssia							
Helsinki	Cryptography in Networking	2023	advanced	1,9	1,9	2	2
Helsinki	Seminar of Advanced Topics in Networking and Security	2024	advanced	3,0	0,0	3	0
Helsinki	Trustworthy Machine Learning	2023	advanced	1,8	3,0	2	3
Jyväskylän yliopisto: 21 Kurssia							
Jyväskylä	Advanced Course on Information Security Management	2024	advanced	1,6	1,0	1	1
Jyväskylä	Anomalian havaitseminen	2024	advanced	1,4	2,0	1	2
Jyväskylä	Authentication, passwords and applied cryptography	2024	advanced	1,9	1,8	2	2
Jyväskylä	Business continuity and ICT resilience	2024	advanced	1,8	2,1	2	2
Jyväskylä	Cyber security basics	2025	intermediate	1,0	1,0	1	1
Jyväskylä	Cyber Security Psychology	2024	advanced	2,1	1,6	2	2
Jyväskylä	Information Security Management	2024	advanced	1,2	2,0	1	2
Jyväskylä	Introduction to Trusted and Confidential Computing	2024	advanced	1,5	1,8	1	1
Jyväskylä	Introductory Penetration Testing and Security Assessment	2024	advanced	2,3	2,1	2	2
Jyväskylä	Järjestelmähaavoittuvuudet (System Vulnerabilities and Security)	2024	advanced	1,5	1,5	1	1
Jyväskylä	Kansalaisen kyberturvallisuus	2024	basic	1,4	1,0	1	1
Jyväskylä	Koneoppimismenetelmiä kyberturvallisuuteen	2025	advanced	2,0	2,0	2	2
Jyväskylä	Kyberhyökkäys ja sen torjunta	2024	advanced	1,3	1,8	1	2
Jyväskylä	Kyberturvallisuuden hallinta ja johtaminen	2025	advanced	1,5	1,0	1	1
Jyväskylä	Kyberturvallisuusteknologiat	2024	advanced	1,8	2,0	2	2
Jyväskylä	Legal Aspects of Security and Privacy	2024	advanced	1,5	1,5	1	1

Yliopisto	Kurssin nimi	Instanssin vuosi	Taso	Teoria Ka.	Harjoitus Ka.	Teoria Md.	Harjoitus Md.
Jyväskylä	Privacy Engineering	2024	advanced	1,7	1,9	1	2
Jyväskylä	Privacy in light of Cybersecurity and Digitalization	2024	advanced	1,9	1,3	2	1
Jyväskylä	Teknologian kehitys ja muuttuva turvallisuus	2024	advanced	1,2	1,0	1	1
Jyväskylä	Tietoverkkoturvallisuus	2024	advanced		2,2	0	2
Jyväskylä	Trends in Cyber Security	2021	advanced	1,6	1,7	1	2
Oulun yliopisto: 9 Kurssia							
Oulu	*Cyber Security I: Ethical Hacking	2025	advanced	1,6	1,6	1,5	1,5
Oulu	Empirical Research in Computer Security	2024	advanced	2,5	2,5	2,5	2,5
Oulu	Johdatus kyberturvallisuustestaukseen	2025	intermediate	1,4	1,6	1	1
Oulu	Kryptografiset järjestelmät ja niiden heikkoudet	2025	advanced	2,3	2,2	2	2
Oulu	Kyberturvallisuus II: Pilvi- ja verkkoturvallisuus	2025	advanced	1,4	1,9	1	2
Oulu	Kyberturvallisuus III: Ohjelmisto- ja laiteturvallisuus	2025	advanced	1,7	2,0	1	2
Oulu	Security Engineering	2025	advanced	1,7	1,2	2	1
Oulu	Tietotekniikan erikoiskurssi 12 - Modern Cryptography	2025	advanced	2,0	1,9	2	2
Oulu	Yksityisyyden suoja ja käyttäjän manipulointi	2025	intermediate	1,8	1,6	2	2
Tampereen yliopisto: 13 Kurssia							
Tampere	Automaation turvallisuus	2024	advanced	1,2	2,1	1	2
Tampere	Cryptography Engineering	2024	intermediate	1,6	2,0	1	2
Tampere	Cyber Security 1	2024	basic	1,3	1,1	1	1
Tampere	Cyber Security 2: Specialization	2024	intermediate	1,9	1,0	2	1
Tampere	Digitaaliset yleistaidot, teema 5: Kyberturvallisuuden perusteet	2024	general	1,3	1,0	1	1
Tampere	Digital Shadow: Privacy and Anonymity	2024	basic	1,6	1,8	1	1,5
Tampere	Fault Tolerance and Cybersecurity in Automation	2025	advanced	1,3	2,2	1	2
Tampere	Information Systems Resilience	2024	intermediate	1,5	1,7	1	2

Yliopisto	Kurssin nimi	Instanssin vuosi	Taso	Teoria Ka.	Harjoitus Ka.	Teoria Md.	Harjoitus Md.
Tampere	Kyberturvallisuus I, suomenkielinen toteutus	2024	basic	1,4	1,7	1	2
Tampere	Post-Quantum Cryptography Engineering	2025	advanced	2,2	2,2	2,5	2,5
Tampere	Secure programming	2024	advanced	1,3	2,4	1	2,5
Tampere	Security Protocols: Helping Alice and Bob to Share Secrets	2024	intermediate	1,9	1,5	2	1
Tampere	Side-Channel Analysis	2025	advanced	1,8	1,9	2	2
Turun yliopisto: 27 Kurssia							
Turku	*Computer forensics	2025	advanced	1,8	2,0	2	2
Turku	AI & Cybersecurity MOOC	2024	basic	2,4	1,0	3	1
Turku	Algebraic Structures in Cryptography	2023	advanced	1,6	1,0	1	1
Turku	Capstone	2024	advanced	1,1	2,2	1	2
Turku	Communication Technologies and Security in IoT	2024	advanced	1,7	2,0	2	2
Turku	Cryptography I	2024	advanced	2,3	1,0	3	1
Turku	Cryptography II	2024	advanced	1,5	1,0	1	1
Turku	Digitalization and Cyber Security	2022	basic	1,0	1,0	1	1
Turku	Ethical Hacking	2024	advanced	1,4	2,1	1	2
Turku	Firewall and IPS Technology	2023	advanced	1,5	2,0	1	2
Turku	Foundations of Cryptography	2023	advanced	3,0	1,0	3	1
Turku	Fundamentals of Information Security	2023	intermediate	1,7	0,0	2	0
Turku	Human Element in Information Security	2024	advanced	1,5	2,0	1,5	2
Turku	Introduction to Cybersecurity	2024	basic	2,0	0,0	2	0
Turku	Johdatus tietoturvaan ja yksityisyyteen	2023	basic	1,0	0,0	1	0
Turku	Kyberturvallisuusteknologia	2024	intermediate	1,2	2,0	1	2
Turku	Management of Information System Security	2024	advanced	2,0	2,6	2	3
Turku	Network Infrastructure Technologies and Security	2025	advanced	1,2	0,0	1	0
Turku	Opiskelun ja työelämän tietotekniikka, Tieto- ja kyberturvallisuus	2023	general	1,2	0,0	1	0
Turku	Privacy and Security for Software Systems	2023	advanced	1,5	1,0	1	1

Yliopisto	Kurssin nimi	Instanssin vuosi	Taso	Teoria Ka.	Harjoitus Ka.	Teoria Md.	Harjoitus Md.
Turku	Protocol Processing and Security	2024	advanced	2,0	2,0	2	2
Turku	Security Engineering	2024	advanced	1,0	0,0	1	0
Turku	Selected Topics in Cryptography	2023	advanced	1,8	0,0	2	0
Turku	Special Course on Cyber Security - Cyber Security Governance	2024	advanced	1,7	1,0	2	1
Turku	System and Application Security	2023	advanced	1,4	1,3	1	1
Turku	Tietotekniikan laboratoriot	2024	intermediate	1,6	1,8	2	2
Turku	Tietoverkkotekniikat	2024	intermediate	1,2	0,0	1	0
Vaasan yliopisto: 3 Kurssia							
Vaasa	Järjestelmien turvallisuus	2024	basic	1,0	0,0	1	0
Vaasa	Management of Cyber Security	2024	advanced	1,8	0,0	2	0
Vaasa	Security of Embedded and Distributed Systems	2023	advanced	2,5	2,5	3	3

Taulukossa 3 on myös kuvattu kurssin vastuuopettajan määrittämä arvio teorian ja käytännön toteutuksen tasosta. On huomioitava, että tässä arviossa on jonkin verran yliopistokohtaisia ja vastuuopettajan omia painotuksia siinä, miten tietojen syöttäjä on arvioinut tiettyjen taksonomiassa esitettyjen asioiden käsittelyn syvyyttä. Keskimäärin kurssien toteutusten saama pistemäärä on välillä 1,5–2. Taulukosta on nähtävissä myös, että harjoituksia on vähemmän kuin teoriaa ja usein harjoitukset jäävät pienemmälle painotukselle kuin teoria. Jatkokehitystoimena erityisesti harjoitusten kehittäminen ja erilaisten käytännön harjoitusten lisääminen kehittäisi Suomen kyberturvallisuuskoulutusta eteenpäin ja toisi opiskelijoille jo opintojen aikana vahvempaa käytännön osaamisen pohjaa. Tätä harjoitusten kehittämistä voi jatkokehittää osana hankkeen seuraavia työvaihteita.

3 Tulokset

Tässä luvussa tuloksia ja havaintoja tarkastellaan kolmen kokonaisuuden kautta: 1) koko Suomen tilanne (mukana kaikkien yliopistojen kurssit), 2) kyberturvallisuuden ylemmän tutkinnon tarjoavat yliopistot (Jyväskylä ja Turku), jossa raportoitujen kurssien määrä on yli 20, 3) kurssikokonaisuuksia tutkinnon suuntaamiseen kyberturvallisuusalalle tarjoavat yliopistot (Oulu ja Tampere), jossa raportoitujen kurssien määrä on vähintään 9.

Raporttiin on lisätty myös ne taksonomian aiheet, joita on käsitelty hyvin vähän tai ei lainkaan. Näiden tarkoitus on antaa taksonomian mukaisia ideoita mahdollisista aiheista, joita ei vielä käsitellä nykyisissä kursseissa, ja näitä voi käyttää mahdollisina koulutuksen tai kurssien kehityskohteina hankkeen työvaihe 3:n aikana.

3.1 Suomen yliopistojen kyberturvallisuusopetus – kaikki raportoidut kurssit

Seuraavassa tarkastelussa on mukana kaikki raportoidut kurssit, joita tarjotaan yliopistoissa. Roolien ja avainosaamisten ja taksonomian käsittelyyn liittyvissä taulukoissa on otettu mukaan kaikki samanarvoiset tiedot.

3.1.1 Suomen yliopistojen kyberturvallisuuskoulutuksen painotus - kyberturvallisuusroolit ja avainosaaminen

Suomen kyberturvallisuuskoulutus on keskittynyt vahvasti erilaisten osaamisalueiden käsittelyyn sekä teoreettisesti että käytännön harjoitusten kautta. Suomen kyberturvallisuuskoulutuksen painopisteet ja kokonaistilanne voidaan tiivistää seuraavasti:

- Roolikohtainen painotus: Cyber Incident Responder ja CISO ovat molemmissa osioissa (teoria ja käytännön harjoitukset) saaneet huomattavasti enemmän huomiota verrattuna muihin rooleihin (Taulukko 4 ja Taulukko 5).

- Käytännön harjoitukset: Käytännön harjoitukset seuraavat teoriaosuuden painotuksia, mutta näyttävät painottuvan enemmän teknisille osaamisalueille kuten verkkojen ja käyttöjärjestelmien turvallisuuteen. Lisäksi käytännön harjoituksia on merkittävästi vähemmän kuin teoria-aiheita.
- Osaamisalueiden kattavuus: Kyberturvallisuuskoulutus kattaa laajan kirjon kyberturvallisuusosaamista alkaen teknisistä taidoista, kuten tietoverkkojen ja käyttöliittymien turvallisuudesta operatiivisiin taitoihin, kuten tapahtumien käsittelyyn, ja strategisiin taitoihin, kuten riskien hallintaan, sekä hallinnollisia taitoja, kuten kyberturvallisuussäädösten tuntemusta.
- Kurssien aihealueet: Kyberturvallisuusalan kurssit käsittelevät useita JRC:n taksonomian aihealueita. Erityisesti identiteetinhallinta, tietoturvan ja yksityisyyden hallinta, sekä oikeudelliset näkökulmat ovat saaneet paljon huomiota. Tämä heijastaa koulutuksen kykyä vastata monipuolisesti kyberturvallisuuden nykyisiin ja tuleviin haasteisiin.

Suomen kyberturvallisuuskoulutuksen keskeiset roolit ja osaamisalueet on tiivistetty Taulukkoon 4. Taulukoissa 5 ja 6 on nähtävillä 30 eniten kyberturvallisuus-koulutuksessa esiintyvää avainosaamista ja niihin kuhunkin liittyvät kyber-turvallisuusroolit. Taulukoiden 5 ja 6 Total-arvo kertoo, kuinka monta kertaa kyseistä avainosaamista käsitellään kaikkien kurssien aikana. Taulukoiden 5 ja 6 Total-arvoihin perustuen Suomen kyberturvallisuuskoulutuksen avainosaamiset ja niihin liittyvät kyberturvallisuusroolit ovat:

1. **CISO (Chief Information Security Officer) (3096 teoria + 1827 käytäntö = 4923)**:
   - Kyberturvallisuuden suositukset ja parhaat käytännöt (566 teoria, 242 käytäntö)
   - Kyberturvallisuuden standardit, metodologiat ja viitekehykset (542 teoria, 215 käytäntö)
   - Kyberturvallisuuspolitiikat (536 teoria, 233 käytäntö)
   - Kyberturvallisuuteen liittyvät lait, säädökset ja lainsäädännöt (533 teoria, 222 käytäntö)
   - Riskinhallinnan standardit, metodologiat ja viitekehykset (käytäntö 222)
   - Johtamiskäytännöt (385 teoria, 159 käytäntö)
   - Kyberturvallisuuden kypsyysmallit (272 teoria)
   - Kyberturvallisuuden proseduurit (262 teoria)

2. **Cyber Incident Responder (3465 teoria + 1246 käytäntö =4711)**:
    - Tietoverkkojen turvallisuus (925 teoria, 433 käytäntö)
    - Käyttöjärjestelmien turvallisuus (749 teoria, 335 käytäntö)
    - Secure Operation Center (SOC) -toiminta (388 teoria, 169 käytäntö)
    - CSIRT-toiminta (388 teoria, 169 käytäntö)
    - Tapahtumien käsittelystandardit, metodologiat ja viitekehykset (306 teoria, 140 käytäntö)
    - Tapahtumien käsittelyn suositukset ja parhaat käytännöt (281 teoria)
    - Tapahtumien käsittelyn kommunikointiproseduurit (217 teoria)
    - Tapahtumien käsittelyn työkalut (211 teoria)
3. **Cybersecurity Architect (1844 teoria + 513 käytäntö = 2357)**:
    - Kyberturvallisuuden suositukset ja parhaat käytännöt (1186 teoria, 513 käytäntö)
    - Kyberturvallisuuden standardit, metodologiat ja viitekehykset (243 teoria)
    - Turvallisen kehittämisen elinkaari (218 teoria)
    - Kyberturvallisuuteen liittyvä vaatimusanalyysi (197 teoria)
4. **Cyber Threat Intelligence Specialist (1648 teoria + 677 käytäntö =2325**):
    - Tietoverkkojen turvallisuus (818 teoria, 390 käytäntö)
    - Käyttöjärjestelmien turvallisuus (626 teoria, 287 käytäntö)
    - CTI:n standardien, metodologioiden ja viitekehysten jakaminen (204 teoria)

Taulukko 4. Suomen yliopistojen kyberturvallisuuskoulutuksen tarjoama teoria ja harjoitukset verrattuna ENISA:n kyberturvallisuusrooleihin

TEORIA		**HARJOITUKSET**	
Rooli	**# Roolin avainosaaminen top 50**	**Rooli**	**# Roolin avainosaaminen top 50**
Cyber Incident Responder	12	Cyber Incident Responder	10
CISO	10	CISO	9
Cybersecurity Architect	6	Cybersecurity Risk Manager	7
Cyber Legal, Policy and Compliance Officer	5	Cybersecurity Implementer	5
Cyber Threat Intelligence Specialist	5	Cybersecurity Architect	4
Cybersecurity Implementer	4	Cybersecurity Auditor	3
Cybersecurity Auditor	2	Cyber Legal, Policy and Compliance Officer	3
Cybersecurity Risk Manager	2	Cyber Threat Intelligence Speclist	3
Digital Forensics Investigator	2	Digital Forensics Investigator	3
Penetration Tester	2	Penetration Tester	3

Taulukko 5. Suomen yliopistojen kyberturvallisuuskoulutuksen avainosaaminen teorian osalta - TOP 30 ENISA:n kyberturvallisuusrooli ja avainosaaminen

Rooli	**Avainosaaminen**	**Käsitellään kursseilla (lkm)**
Cybersecurity Architect	Cybersecurity recommendations and best practices	1186
Cyber Incident Responder	Computer networks security	925
Cyber Threat Intelligence Specialist	Computer networks security	818
Cyber Incident Responder	Operating systems security	749
Cyber Threat Intelligence Specialist	Operating systems security	626
CISO	Cybersecurity recommendations and best practices	566
CISO	Cybersecurity standards, methodologies and frameworks	542
CISO	Cybersecurity policies	536

Rooli	Avainosaaminen	Käsitellään kursseilla (lkm)
CISO	Cybersecurity related laws, regulations and legislations	533
CISO	Risk management standards, methodologies and framework	525
Cyber Legal, Policy and Compliance Officer	Legal, regulatory and legislative compliance requirements, recommendations and best practices	502
Cyber Incident Responder	Secure Operation Centres (SOCs) operation	388
Cyber Incident Responder	Computer Security Incident Response Teams (CSIRTs) operation	388
CISO	Management practices	385
Cyber Legal, Policy and Compliance Officer	Cybersecurity related laws, regulations and legislations	365
Cyber Incident Responder	Incident handling standards, methodologies and frameworks	306
Cyber Legal, Policy and Compliance Officer	Cybersecurity policies	294
Cyber Incident Responder	Incident handling recommendations and best practices	281
CISO	Cybersecurity maturity models	272
CISO	Cybersecurity procedures	262
Cybersecurity Architect	Cybersecurity standards, methodologies and frameworks	243
Penetration Tester	Computer networks security	237
CISO	Resource management	236
Cybersecurity Architect	Secure development lifecycle	218
Cyber Incident Responder	Incident handling communication procedures	217
Digital Forensics Investigator	Computer networks security	217
Cyber Incident Responder	Incident handling tools	211
Cyber Threat Intelligence Specialist	Cyber Threat Intelligence (CTI) sharing standards, methodologies and frameworks	204
Cybersecurity Architect	Cybersecurity-related requirements analysis	197
CISO	Ethical cybersecurity organisation requirements	196

Taulukko 6. Suomen yliopistojen kyberturvallisuuskoulutuksen avainosaaminen harjoitusten osalta - TOP 30 ENISA:n kyberturvallisuusrooli ja avainosaaminen

Rooli	Avainosaaminen	Käsitellään kursseilla (lkm)
Cybersecurity Architect	Cybersecurity recommendations and best practices	513
Cyber Incident Responder	Computer networks security	433
Cyber Threat Intelligence Specialist	Computer networks security	390
Cyber Incident Responder	Operating systems security	335
Penetration Tester	Computer networks security	322
Digital Forensics Investigator	Computer networks security	292
Cyber Threat Intelligence Specialist	Operating systems security	287
Cybersecurity Implementer	Computer networks security	262
CISO	Cybersecurity recommendations and best practices	242
CISO	Cybersecurity policies	233
Penetration Tester	Operating systems security	229
CISO	Cybersecurity related laws, regulations and legislations	222
CISO	Risk management standards, methodologies and framework	222
Cyber Legal, Policy and Compliance Officer	Legal, regulatory and legislative compliance requirements, recommendations and best practices	216
CISO	Cybersecurity standards, methodologies and frameworks	215
Cybersecurity Auditor	Monitoring, testing and evaluating cybersecurity controls' effectiveness	209
Digital Forensics Investigator	Operating systems security	209
Cybersecurity Risk Manager	Monitoring, testing and evaluating cybersecurity controls' effectiveness	201
Cybersecurity Auditor	Legal, regulatory and legislative compliance requirements, recommendations and best practices	196
Cybersecurity Implementer	Cybersecurity recommendations and best practices	193
Cybersecurity Implementer	Operating systems security	181
Cyber Incident Responder	Secure Operation Centres (SOCs) operation	169

Rooli	Avainosaaminen	Käsitellään kursseilla (lkm)
Cyber Incident Responder	Computer Security Incident Response Teams (CSIRTs) operation	169
Cybersecurity Implementer	Cybersecurity controls and solutions	167
Cybersecurity Risk Manager	Cybersecurity controls and solutions	161
CISO	Management practices	159
Cybersecurity Implementer	Secure development lifecycle	149
Cyber Legal, Policy and Compliance Officer	Cybersecurity related laws, regulations and legislations	147
Cybersecurity Risk Manager	Cybersecurity risks	146
Cyber Incident Responder	Incident handling standards, methodologies and frameworks	140

3.1.2 Suomen yliopistojen kyberturvallisuuskurssien aiheet taksonomian mukaisesti tarkasteltuna

Seuraavat JRC:n taksonomian aiheet ovat saaneet laajaa käsittelyä Suomen opetusohjelmissa teorian ja harjoitusten osalta, mikä korostaa niiden merkitystä kyberturvallisuuden pohjaosaamisen ja ymmärryksen rakentamisessa osana kursseja (Taulukko 7 ja Taulukko 8):

1. **Assurance, Audit, and Certification**:

   - Assessment käsitelty 42 teoriakursseilla ja 27 käytännön harjoituksissa.
   - Audit käsitelty 35 teoriakursseilla ja 18 käytännön harjoituksissa.
   - Certification käsitelty 34 kertaa teoriakursseilla.

2. **Legal Aspects**:

   - Cybercrime prosecution and law enforcement käsitelty 41 teoriakursseilla ja 19 käytännön harjoituksissa.
   - Cybersecurity regulation analysis and design käsitelty 37 teoriakursseilla ja 17 käytännön harjoituksissa.

3. **Data Security and Privacy**:

   - Data integrity käsitelty 44 teoriakursseilla ja 18 käytännön harjoituksissa.

4. **Education and Training**:

   - Cybersecurity-aware culture käsitelty 33 teoriakursseilla ja 16 käytännön harjoituksissa.

5. **Network and Distributed Systems Security**:

   - Managerial, procedural and technical aspects of network security käsitelty 34 teoriakurssilla.

Suomen kyberturvallisuuskoulutuksessa vähiten käsiteltyjä JRC:n taksonomian aihealueita kurssisisällöissä teorian ja harjoitusten osalta ovat (Taulukko 9 ja Taulukko 10):

1. **Steganography, Steganalysis, and Watermarking**:

   - Steganalysis: käsitelty 7 teoriakursseilla ja 2 käytännön harjoituksissa.

2. **Software and Hardware Security Engineering**:

   - Security support in programming environments: käsitelty 7 teoriakursseilla ja 3 käytännön harjoituksissa.
   - Security testing and validation: käsitelty 5 teoriakursseilla ja 3 käytännön harjoituksissa.
   - Attack techniques: käsitelty 7 teoriakursseilla ja 3 käytännön harjoituksissa.

3. **Theoretical Foundations**:

   - Formal verification of security assurance: käsitelty 7 teoriakursseilla ja 3 käytännön harjoituksissa.

4. **Security Management and Governance**:

   - Processes and procedures to ensure device end-of-life security and privacy: käsitelty 3 teoriakursseilla.
   - Threats and vulnerabilities modelling: käsitelty 3 käytännön harjoituksissa.

Nämä aihealueet ovat saaneet vähemmän huomiota verrattuna muihin JRC:n taksonomian mukaisiin aihealueisiin, mikä voi tarjota mahdollisuuksia ja ideoita kehittää aiheiden käsittelyä kursseissa. Erityisesti Software and Hardware Security Engineering ja Security Management and Governance -aiheiden kehittäminen olisi hyödyllistä, kun tavoitteena on turvallinen ohjelmointi (secure programming) ja turvallinen ohjelmistokehitys (secure software development).

Taulukko 7. Suomen yliopistojen kurssien eniten käsittelemät aiheet teorian osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	**Taksonomian aihe**	**Kurssien lkm**
3.1.6 Identity Management	Privacy and identity management (e.g. privacy-preserving authentication)	47
3.1.3 Data Security and Privacy	Data integrity	44
3.1.1 Assurance, Audit, and Certification	Assessment	42
3.1.14 Theoretical Foundations	Formal specification of various aspects of security (e.g properties, threat models, etc.)	42
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Asymmetric cryptography	41
3.1.8 Legal Aspects	Cybercrime prosecution and law enforcement	41
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Symmetric cryptography	40
3.1.15 Trust Management and Accountability	Trust management architectures, mechanisms and policies	38
3.1.8 Legal Aspects	Cybersecurity regulation analysis and design	37
3.1.12 Software and Hardware Security Engineering	Vulnerability discovery and penetration testing	37
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Hash functions	36
3.1.5 Human Aspects	Usability	36
3.1.1 Assurance, Audit, and Certification	Audit	35
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Digital signatures	35
3.1.14 Theoretical Foundations	Formal specification and verification of the various aspects of security;	35

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.1 Assurance, Audit, and Certification	Assurance	34
3.1.6 Identity Management	Legal aspects of identity management	34
3.1.9 Network And Distributed Systems	Managerial, procedural and technical aspects of network security	34
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Message authentication	33
3.1.4 Education and Training	Cybersecurity-aware culture (e.g. including children education)	33
3.1.15 Trust Management and Accountability	Trusted computing	33
3.1.5 Human Aspects	Non-intrusive security	32
3.1.9 Network and Distributed Systems	Network layer attacks and mitigation techniques	32
3.1.12 Software and Hardware Security Engineering	Malware analysis including adversarial learning of malware	32
3.1.7 Incident Handling and Digital Forensics	Incident analysis, communication, documentation, forecasting (intelligence based), response, and reporting	31
3.1.11 Security Measurements	Security analytics and visualization	31
3.1.13 Steganography, Steganalysis and Watermarking	Digital watermarking	31
3.1.15 Trust Management and Accountability	Trust and privacy	31
3.1.5 Human Aspects	User acceptance of security policies and technologies	30
3.1.6 Identity Management	Identity management quality assurance	30
3.1.8 Legal Aspects	Legal and societal issues in information security (e.g. identity management, digital forensics, cybersecurity litigation)	30

Taulukko 8. Suomen yliopistojen kurssien eniten käsittelemät aiheet harjoitusten osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.1 Assurance, Audit, and Certification	Assessment	27
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Asymmetric cryptography	22
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Symmetric cryptography	22
3.1.6 Identity Management	Privacy and identity management (e.g. privacy-preserving authentication)	22
3.1.4 Education and Training	Cyber ranges, Capture the Flag, exercises, simulation platforms, educational/training tools, cybersecurity awareness	21
3.1.10 Security Management and Governance	Techniques to ensure business continuity/disaster recovery	20
3.1.8 Legal Aspects	Cybercrime prosecution and law enforcement	19
3.1.1 Assurance, Audit, and Certification	Audit	18
3.1.3 Data Security and Privacy	Data integrity	18
3.1.5 Human Aspects	Non-intrusive security	18
3.1.12 Software and Hardware Security Engineering	Vulnerability discovery and penetration testing	18
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Digital signatures	17
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Hash functions	17
3.1.8 Legal Aspects	Cybersecurity regulation analysis and design	17
3.1.4 Education and Training	Cybersecurity-aware culture (e.g. including children education)	16
3.1.5 Human Aspects	User acceptance of security policies and technologies	16
3.1.7 Incident Handling and Digital Forensics	Incident analysis, communication, documentation, forecasting (intelligence based), response, and reporting	16

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Message authentication	15
3.1.11 Security Measurements	Security analytics and visualization	15
3.1.14 Theoretical Foundations	Formal specification of various aspects of security (e.g properties, threat models, etc.)	15
3.1.15 Trust Management and Accountability	Trust management architectures, mechanisms and policies	15
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Mathematical foundations of cryptography	14
3.1.4 Education and Training	Higher Education	14
3.1.6 Identity Management	Legal aspects of identity management	14
3.1.1 Assurance, Audit, and Certification	Assurance	13
3.1.3 Data Security and Privacy	Privacy Enhancing Technologies (PET)	13
3.1.8 Legal Aspects	Legal and societal issues in information security (e.g. identity management, digital forensics, cybersecurity litigation)	13
3.1.9 Network and Distributed Systems	Protocols and frameworks for secure distributed computing	13
3.1.14 Theoretical Foundations	Formal specification, analysis, and verification of software and hardware	13

Taulukko 9. Suomessa kurssien vähiten käsittelemät aiheet teorian osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.11 Security Measurements	Validation and comparison frameworks for security metrics	7
3.1.12 Software and Hardware Security Engineering	Security support in programming environments	7
3.1.12 Software And Hardware Security Engineering	Attack techniques (e.g. side channel attacks, power attacks, stealth attacks, advanced persistent attacks, rowhammer attacks)	7
3.1.13 Steganography, Steganalysis and Watermarking	Steganalysis	7

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.14 Theoretical Foundations	Formal verification of security assurance	7
3.1.15 Trust Management and Accountability	Trust in securing digital as well as physical assets	7
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML Legislation	7
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML-related standards	7
3.1.5 Human Aspects	Enhancing risk perception	6
3.1.10 Security Management and Governance	Identification of the impact of hardware and software changes on the management of Information Security	6
3.1.12 Software and Hardware Security Engineering	Security and risk analysis of components compositions	6
3.1.12 Software and Hardware Security Engineering	Refinement and verification of security management policy models	6
3.1.12 Software and Hardware Security Engineering	Runtime security verification and enforcement	6
3.1.7 Incident Handling and Digital Forensics	Coordination and information sharing in the context of cross-border/organizational incidents	5
3.1.10 Security Management and Governance	Compliance with information security and privacy policies, procedures, and regulations	5
3.1.10 Security Management and Governance	Capability maturity models (e.g. assessment of capacities and capabilities)	5
3.1.12 Software and Hardware Security Engineering	Security testing and validation	5
3.1.4 Education and Training	Vocational training	4
3.1.10 Security Management and Governance	Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling)	3

Taulukko 10. Suomessa kurssien vähiten käsittelemät aiheet harjoitusten osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Homomorphic encryption	3
3.1.10 Security Management and Governance	Threats and vulnerabilities modelling	3
3.1.12 Software and Hardware Security Engineering	Secure software architectures and design (security by design)	3
3.1.12 Software and Hardware Security Engineering	Security support in programming environments	3
3.1.12 Software and Hardware Security Engineering	Security testing and validation	3
3.1.12 Software and Hardware Security Engineering	Model-driven security and domain-specific modelling languages	3
3.1.12 Software and Hardware Security Engineering	Attack techniques (e.g. side channel attacks, power attacks, stealth attacks, advanced persistent attacks, rowhammer attacks)	3
3.1.14 Theoretical Foundations	Formal verification of security assurance	3
3.1.15 Trust Management and Accountability	Trust in securing digital as well as physical assets	3
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML threat assessment (e.g. evasion, oracle, poisoning)	3
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML security management	3
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML-related standards	3
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Quantum cryptography	2
3.1.4 Education and Training	Vocational training	2
3.1.10 Security Management and Governance	Identification of the impact of hardware and software changes on the management of Information Security	2
3.1.10 Security 1Management and Governance	Compliance with information security and privacy policies, procedures, and regulations	2
3.1.10 Security Management and Governance	Capability maturity models (e.g. assessment of capacities and capabilities)	2
3.1.12 Software and Hardware Security Engineering	Security and risk analysis of components compositions	2

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.12 Software and Hardware Security Engineering	Refinement and verification of security management policy models	2
3.1.12 Software and Hardware Security Engineering	Privacy by design	2
3.1.13 Steganography, Steganalysis and Watermarking	Steganalysis	2
3.1.10 Security Management and Governance	Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling)	1
3.1.11 Security Measurements	Validation and comparison frameworks for security metrics	1
3.1.12 Software and Hardware Security Engineering	Runtime security verification and enforcement	1

3.2 Ylemmän kyberturvallisuustutkinnon tarjoavat yliopistot – yli 20 kurssia raportoineet

Seuraavassa tarkastellaan yli 20 kurssia raportoineet yliopistot, jotka tarjoavat myös kyberturvallisuuteen keskittyvän ylemmän tutkinnon. Yliopistot esitetään aakkosjärjestyksessä. Roolien/avainosaamisten ja taksonomian käsittelyyn liittyvissä taulukoissa on otettu mukaan kaikki samanarvoiset tiedot. Tämän takia taulukoiden koot voivat vaihdella eri yliopistoilla, koska taulukkoon on otettu esim. kaikki 0 arvon saaneet kurssit.

3.2.1 Jyväskylän yliopisto – 21 kurssia

Kybertuvallisuusroolien ja avainosaamisten pohjalta tarkasteltuna koulutuksella on seuraavia piirteitä:

- Roolikohtainen painotus: Koulutuksessa on korostuvat tietyt roolit, erityisesti CISO ja Cyber Incident Responder
- Monialaiset osaamiset: Kurssit kattavat laajasti eri osa-alueita, mukaan lukien hallinnolliset taidot (esim. turvallisuuspolitiikat ja riskienhallinta) sekä oikeudelliset ja sääntelyyn liittyvät taidot, ja tekniset taidot (esim. tietoverkkojen ja käyttöjärjestelmien turvallisuus).
- Laaja-alainen koulutus: Koulutuksessa on laaja-alainen lähestymistapa, joka kattaa sekä strategisen, teknisen että operatiivisen kyberturvallisuuden osa-alueet.

Kyberturvallisuuden koulutuksessa on vahva painotus strategisessa, hallinnollisessa ja operatiivisessa osaamisessa, mikä on välttämätöntä nykyisten ja tulevien kyberuhkien hallinnassa. Jyväskylän yliopiston kyberturvallisuus-koulutuksen keskeiset roolit ja osaamisalueet on esitetty Taulukossa 11. Taulukoissa 12 ja 13 on nähtävillä 20 kyberturvallisuuskoulutuksessa eniten esiintyvää avainosaamista ja kuhunkin niistä liittyvät kyberturvallisuusroolit. Taulukkojen 12 ja 13 Total-arvo kertoo, kuinka monta kertaa kyseinen avainosaaminen on tunnistettu eri kursseissa. Em. taulukoiden Total-arvoihin perustuen Jyväskylän yliopiston kyberturvallisuuskoulutuksen avainosaamiset ja niihin liittyvät kyberturvallisuusroolit ovat:

1. **CISO (Chief Information Security Officer) (942 teoria + 634 käytäntö = 1576)**:

    - Kyberturvallisuuden standardit, metodologiat ja viitekehykset (174 teoria, 110 käytäntö)
    - Kyberturvallisuuspolitiikat (171 teoria, 114 käytäntö)
    - Kyberturvallisuuden suositukset ja parhaat käytännöt (165 teoria, 116 käytäntö)
    - Kyberturvallisuuteen liittyvät lait ja säädökset (161 teoria, 107 käytäntö)
    - Riskienhallinnan standardit, metodologiat ja viitekehykset (154 teoria, 108 käytäntö)
    - Johtamiskäytännöt (117 teoria, 79 käytäntö)

2. **Cyber Incident Responder (556 teoria + 240 käytäntö = 796)**:

    - Tietoverkkojen turvallisuus (178 teoria, 146 käytäntö)
    - Käyttöjärjestelmien turvallisuus (144 teoria, 94 käytäntö)
    - Secure Operation Centre (SOC) -operointi (117 teoria)
    - CSIRT-operointi (117 teoria)

3. **Cybersecurity Auditor (314 teoria + 189 käytäntö = 503)**:

    - Kyberturvallisuuskontrollien tehokkuuden seuranta, testaus ja arviointi (160 teoria, 95 käytäntö)
    - Lakisääteisten vaatimusten ja suositusten noudattaminen (154 teoria, 94 käytäntö)

4. **Cyber Legal, Policy, and Compliance Officer (278 teoria + 100 käytäntö = 378)**:

    - Lakisääteiset ja lainsäädännölliset vaatimukset, suositukset ja parhaat käytännöt (158 teoria, 100 käytäntö)
    - Kyberturvallisuuteen liittyvät lait ja säädökset (120 teoria)

Taulukko 11. Jyväskylän yliopiston kyberturvallisuuskoulutuksen tarjoama teoria ja harjoitukset verrattuna ENISA:n kyberturvallisuusrooleihin

TEORIA		**HARJOITUKSET**	
Rooli	**# Roolin avainosaaminen top 50**	**Rooli**	**# Roolin avainosaaminen top 50**
CISO	9	CISO	10
Cyber Incident Responder	9	Cyber Incident Responder	10
Cybersecurity Risk Manager	7	Cybersecurity risk manager	7
Cybersecurity Implementer	5	Cybersecurity Implementer	5
Cyber Legal, Policy and Compliance Officer	4	Digital forensics investigator	4
Cyber Threat Intelligence Specialist	4	Cyber Legal, Policy and Compliance Officer	3
Cybersecurity Architect	4	Cyber Threat Intelligence Specialist	3
Digital Forensics Investigator	4	Cybersecurity Architect	3
Cybersecurity Auditor	2	Cybersecurity Auditor	3
Penetration Tester	2	Penetration tester	2

Taulukko 12. Jyväskylän yliopiston kyberturvallisuuskoulutuksen avainosaaminen teorian osalta - TOP 20 ENISA:n kyberturvallisuusrooli ja avainosaaminen

Rooli	Avainosaaminen	Käsitellään kursseilla (lkm)
Cybersecurity Architect	Cybersecurity recommendations and best practices	244
Cyber Incident Responder	Computer networks security	178
CISO	Cybersecurity standards, methodologies and frameworks	174
CISO	Cybersecurity policies	171
CISO	Cybersecurity recommendations and best practices	165
CISO	Cybersecurity related laws, regulations and legislations	161
Cybersecurity Auditor	Monitoring, testing and evaluating cybersecurity controls' effectiveness	160
Cyber Legal, Policy And Compliance Officer	Legal, regulatory and legislative compliance requirements, recommendations and best practices	158
Cyber Threat Intelligence Specialist	Computer networks security	155
CISO	Risk management standards, methodologies and framework	154
Cybersecurity Auditor	Legal, regulatory and legislative compliance requirements, recommendations and best practices	154
Cyber Incident Responder	Operating systems security	144
Cybersecurity Risk Manager	Monitoring, testing and evaluating cybersecurity controls' effectiveness	140
Cybersecurity Risk Manager	Cybersecurity controls and solutions	130
Cybersecurity Implementer	Cybersecurity recommendations and best practices	123
Penetration Tester	Computer networks security	122
Cyber Legal, Policy and Compliance Officer	Cybersecurity related laws, regulations and legislations	120
CISO	Management practices	117
Cyber Incident Responder	Secure Operation Centres (SOCs) operation	117
Cyber Incident Responder	Computer Security Incident Response Teams (CSIRTs) operation	117

Taulukko 13. Jyväskylän yliopiston kyberturvallisuuskoulutuksen avainosaaminen harjoitusten osalta - TOP 20 ENISA:n kyberturvallisuusrooli ja avainosaaminen

Rooli	Avainosaaminen	Käsitellään kursseilla (lkm)
Cybersecurity Architect	Cybersecurity recommendations and best practices	178
Cyber Incident Responder	Computer networks security	146
Cyber Threat Intelligence Specialist	Computer networks security	131
CISO	Cybersecurity recommendations and best practices	116
CISO	Cybersecurity policies	114
CISO	Cybersecurity standards, methodologies and frameworks	110
CISO	Risk management standards, methodologies and framework	108
CISO	Cybersecurity related laws, regulations and legislations	107
Penetration Tester	Computer networks security	103
Cyber Legal, Policy and Compliance Officer	Legal, regulatory and legislative compliance requirements, recommendations and best practices	100
Cybersecurity Auditor	Monitoring, testing and evaluating cybersecurity controls' effectiveness	95
Digital Forensics Investigator	Computer networks security	95
Cyber Incident Responder	Operating systems security	94
Cybersecurity Auditor	Legal, regulatory and legislative compliance requirements, recommendations and best practices	94
Cybersecurity Risk Manager	Monitoring, testing and evaluating cybersecurity controls' effectiveness	87
Cybersecurity Implementer	Cybersecurity recommendations and best practices	81
Cybersecurity Implementer	Computer networks security	80
CISO	Management practices	79
Cyber Threat Intelligence Specialist	Operating systems security	76
Cybersecurity Implementer	Cybersecurity controls and solutions	76

3.2.2 Jyväskylän yliopiston kyberturvallisuuskurssien aiheet taksonomian mukaisesti tarkasteltuna

Seuraavat JRC:n taksonomian aiheet ovat saaneet laajaa käsittelyä Jyväskylän opetusohjelmassa teorian ja harjoitusten osalta, mikä korostaa niiden merkitystä kyberturvallisuuden pohjaosaamisen ja ymmärryksen rakentamista osana kursseja (Taulukko 14 ja Taulukko 15):

Taksonomian aihealueet ja painotus:

- Assurance, Audit, and Certification: Nämä aiheet ovat hyvin edustettuina kursseilla, mikä heijastaa tarvetta arvioida ja sertifioida turvallisuusratkaisuja.
- Legal Aspects: Kurssit käsittelevät kyberrikollisuuden torjuntaa, oikeudellisia kysymyksiä ja sääntelyanalyysiä, mikä osoittaa oikeudellisten taitojen tärkeyden osana kyberturvallisuuskursseja.
- Software and Hardware Security Engineering: Korostetaan teknisten taitojen merkitystä.
- Education and Training: Kyberturvallisuuskoulutuksen työkalut ja tietoturvatietoisuuden lisääminen painottavat koulutuksen ja jatkuvan oppimisen tärkeyden.
- Human Aspects: Käyttäjäystävällisyyden ja kyberturvallisuusprofiilien huomioiminen korostaa ihmisten ja teknologian vuorovaikutuksen merkitystä.

Kurssien aiheiden sisältö heijastaa laajaa osaamisvaatimusta, joka kattaa strategiset, tekniset ja oikeudelliset osa-alueet. Kurssit pyrkivät varmistamaan, että valmistuvilla opiskelijoilla on laaja-alainen osaaminen ja kyky vastata nykyaikaisen kyberturvallisuusympäristön hallinnollisiin haasteisiin.

Kursseilla eniten käsiteltyjä aiheita taksonomian mukaisesti ovat (Taulukkojen 14 ja 15 perusteella):

Assurance, Audit, and Certification

- Assessment: Käsitelty yhteensä 69 kertaa (42 teoria + 27 käytäntö)
- Audit: Käsitelty yhteensä 53 kertaa (35 teoria + 18 käytäntö)
- Assurance: Käsitelty yhteensä 42 kertaa (32 teoria + 10 käytäntö)
- Certification: Käsitelty yhteensä 38 kertaa (28 teoria + 10 käytäntö)

Legal aspects

- Cybercrime prosecution and law enforcement: Käsitelty yhteensä 60 kertaa (41 teoria + 19 käytäntö)
- Legal and societal issues in information security: Käsitelty yhteensä 42 kertaa (31 teoria + 11 käytäntö)
- Cybersecurity regulation analysis and design: Käsitelty yhteensä 47 kertaa (30 teoria + 17 käytäntö)

Network and Distributed Systems

- Network layer attacks and mitigation techniques: Käsitelty yhteensä 41 kertaa (31 teoria + 10 käytäntö)
- Managerial, procedural and technical aspects of network security: Käsitelty yhteensä 41 kertaa (31 teoria + 10 käytäntö)
- Requirements for network security: Käsitelty yhteensä 41 kertaa (31 teoria + 10 käytäntö)

Software and Hardware Security Engineering

- Vulnerability discovery and penetration testing: Käsitelty yhteensä 54 kertaa (40 teoria + 14 käytäntö)

Education and Training

- Cyber ranges, Capture the Flag exercises, simulation platforms, educational/training tools, cybersecurity awareness: Käsitelty yhteensä 44 kertaa (33 teoria + 11 käytäntö)
- Cybersecurity-aware culture: Käsitelty yhteensä 43 kertaa (33 teoria + 10 käytäntö)

Human aspects

- User acceptance of security policies and technologies: Käsitelty yhteensä 50 kertaa (32 teoria + 18 käytäntö)
- Non-intrusive security: Käsitelty yhteensä 41 kertaa (31 teoria + 10 käytäntö)
- Cybersecurity profiling: Käsitelty yhteensä 41 kertaa (31 teoria + 10 käytäntö)

Jyväskylän kyberturvallisuuskoulutuksessa vähiten käsiteltyjä JRC:n taksonomian aihealueita kurssisisällöissä teorian ja harjoitusten osalta ovat (Taulukko 16 ja Taulukko 17):

Cryptology (Cryptography and Cryptanalysis)

- Functional encryption: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Mathematical foundations of cryptography: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Quantum cryptography: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Post-quantum cryptography: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Homomorphic encryption: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)

Security Management and Governance

- Identification of the impact of hardware and software changes on the management of Information Security: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Standards for Information Security: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Privacy impact assessment and risk management: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Processes and procedures to ensure device end-of-life security and privacy: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Capability maturity models (e.g. assessment of capacities and capabilities): Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)

Security Measurements

- Security metrics, key performance indicators, and benchmarks: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Validation and comparison frameworks for security metrics: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Measurement and assessment of security levels: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)

Software and Hardware Security Engineering

- Security requirements engineering with emphasis on identity, privacy, accountability, and trust: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Security and risk analysis of components compositions: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Secure software architectures and design (security by design): Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Security support in programming environments: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Refinement and verification of security management policy models: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Security testing and validation: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)

Steganography, Steganalysis, and Watermarking

- Steganalysis**:** Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)

Trust Management and Accountability

- Semantics and models for security, accountability, privacy, and trust: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Identity and trust management: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Trust in securing digital as well as physical assets: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Trust and reputation of social and mainstream media: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Social aspects of trust: Käsitelty yhteensä 1 kertaa (1 teoria + 0 käytäntö)

Artificial Intelligence (New area not included in JRC Taxonomy)

- AI/ML threat assessment (e.g. evasion, oracle poisoning): Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- AI/ML security management: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- AI/ML-related standards: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- Ethical and trustworthy AI/ML: Käsitelty yhteensä 2 kertaa (2 teoria + 0 käytäntö)
- AI/ML Legislation: Käsitelty yhteensä 1 kertaa (1 teoria + 0 käytäntö)

Taulukko 14. Jyväskylän yliopiston kurssien eniten käsittelemät aiheet teorian osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.1 Assurance, Audit, and Certification	Assessment	13
3.1.8 Legal Aspects	Cybercrime prosecution and law enforcement	12
3.1.12 Software and Hardware Security Engineering	Vulnerability discovery and penetration testing	12
3.1.1 Assurance, Audit, and Certification	Audit	11
3.1.4 Education and Training	Cyber ranges, Capture the Flag, exercises, simulation platforms, educational/training tools, cybersecurity awareness	11
3.1.5 Human Aspects	User acceptance of security policies and technologies	11
3.1.8 Legal Aspects	Legal and societal issues in information security (e.g. identity management, digital forensics, cybersecurity litigation)	11
3.1.9 Network and Distributed Systems	Network layer attacks and mitigation techniques	11
3.1.1 Assurance, Audit, and Certification	Assurance	10
3.1.1 Assurance, Audit, and Certification	Certification	10
3.1.4 Education and Training	Cybersecurity-aware culture (e.g. including children education)	10
3.1.5 Human Aspects	Non-intrusive security	10
3.1.5 Human Aspects	Cybersecurity profiling	10
3.1.5 Human Aspects	History of cybersecurity	10
3.1.8 Legal Aspects	Cybersecurity regulation analysis and design	10
3.1.9 Network and Distributed Systems	Managerial, procedural and technical aspects of network security	10
3.1.9 Network and Distributed Systems	Requirements for network security	10

Taulukko 15. Jyväskylän yliopiston kurssien eniten käsittelemät aiheet harjoitusten osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.1 Assurance, Audit, and Certification	Assessment	13
3.1.5 Human Aspects	User acceptance of security policies and technologies	9
3.1.1 Assurance, Audit, and Certification	Audit	8
3.1.4 Education and Training	Cybersecurity-aware culture (e.g. including children education)	8
3.1.5 Human Aspects	Non-intrusive security	8
3.1.8 Legal Aspects	Cybercrime prosecution and law enforcement	8
3.1.8 Legal Aspects	Legal and societal issues in information security (e.g. identity management, digital forensics, cybersecurity litigation)	8
3.1.12 Software and Hardware Security Engineering	Vulnerability discovery and penetration testing	8
3.1.4 Education and Training	Cyber ranges, Capture the Flag, exercises, simulation platforms, educational/training tools, cybersecurity awareness	7
3.1.8 Legal Aspects	Cybersecurity regulation analysis and design	7
3.1.9 Network and Distributed Systems	Requirements for network security	7
3.1.9 Network and Distributed Systems	Protocols and frameworks for secure distributed computing	7
3.1.14 Theoretical Foundations	Formal specification of various aspects of security (e.g properties, threat models, etc.)	7
3.1.14 Theoretical Foundations	Formal specification, analysis, and verification of software and hardware	7
3.1.15 Trust Management and Accountability	Trust management architectures, mechanisms and policies	7
3.1.15 Trust Management and Accountability	Trusted computing	7

Taulukko 16. Jyväskylän yliopiston kurssien vähiten käsittelemät aiheet teorian osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Functional encryption	2
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Mathematical foundations of cryptography	2
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Quantum cryptography	2
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Post-quantum cryptography	2
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Homomorphic encryption	2
3.1.4 Education and Training	Vocational training	2
3.1.10 Security Management and Governance	Identification of the impact of hardware and software changes on the management of Information Security	2
3.1.10 Security Management and Governance	Standards for Information Security	2
3.1.10 Security Management and Governance	Privacy impact assessment and risk management	2
3.1.10 Security Management and Governance	Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling)	2
3.1.10 Security Management and Governance	Capability maturity models (e.g. assessment of capacities and capabilities)	2
3.1.11 Security Measurements	Security metrics, key performance indicators, and benchmarks	2
3.1.11 Security Measurements	Validation and comparison frameworks for security metrics	2
3.1.11 Security Measurements	Measurement and assessment of security levels	2
3.1.12 Software and Hardware Security Engineering	Security requirements engineering with emphasis on identity, privacy, accountability, and trust	2
3.1.12 Software and Hardware Security Engineering	Security and risk analysis of components compositions	2
3.1.12 Software and Hardware Security Engineering	Secure software architectures and design (security by design)	2

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.12 Software and Hardware Security Engineering	Security support in programming environments	2
3.1.12 Software and Hardware Security Engineering	Refinement and verification of security management policy models	2
3.1.12 Software and Hardware Security Engineering	Security testing and validation	2
3.1.13 Steganography, Steganalysis and Watermarking	Steganalysis	2
3.1.14 Theoretical Foundations	Formal verification of security assurance	2
3.1.15 Trust Management and Accountability	Semantics and models for security, accountability, privacy, and trust	2
3.1.15 Trust Management and Accountability	Identity and trust management	2
3.1.15 Trust Management and Accountability	Trust in securing digital as well as physical assets	2
3.1.15 Trust Management and Accountability	Trust and reputation of social and mainstream media	2
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML threat assessment (e.g. evasion, oracle, poisoning)	2
16. Artificial Intelligence	AI/ML security management	2
16. Artificial Intelligence	AI/ML-related standards	2
16. Artificial Intelligence	Ethical and trustworthy AI/ML	2
3.1.15 Trust Management and Accountability	Social aspects of trust	1
16. Artificial Intelligence	AI/ML Legislation	1

Taulukko 17. Jyväskylän yliopiston kurssien vähiten käsittelemät aiheet harjoitusten osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Quantum cryptography	1
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Post-quantum cryptography	1
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Homomorphic encryption	1
3.1.9 Network and Distributed Systems	Network steganography	1
3.1.10 Security Management and Governance	Threats and vulnerabilities modelling	1
3.1.10 Security Management and Governance	Attack modelling, techniques, and countermeasures (e.g. adversary machine learning)	1
3.1.10 Security Management and Governance	Managerial aspects concerning information security	1
3.1.10 Security Management and Governance	Identification of the impact of hardware and software changes on the management of Information Security	1
3.1.10 Security Management and Governance	Standards for Information Security	1
3.1.10 Security Management and Governance	Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling)	1
3.1.10 Security Management and Governance	Capability maturity models (e.g. assessment of capacities and capabilities)	1
3.1.11 Security Measurements	Security metrics, key performance indicators, and benchmarks	1
3.1.11 Security Measurements	Validation and comparison frameworks for security metrics	1
3.1.11 Security Measurements	Measurement and assessment of security levels	1
3.1.12 Software and Hardware Security Engineering	Security requirements engineering with emphasis on identity, privacy, accountability, and trust	1

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.12 Software and Hardware Security Engineering	Security and risk analysis of components compositions	1
3.1.12 Software and Hardware Security Engineering	Secure software architectures and design (security by design)	1
3.1.12 Software and Hardware Security Engineering	Security support in programming environments	1
3.1.12 Software and Hardware Security Engineering	Refinement and verification of security management policy models	1
3.1.12 Software and Hardware Security Engineering	Runtime security verification and enforcement	1
3.1.12 Software and Hardware Security Engineering	Security testing and validation	1
3.1.13 Steganography, Steganalysis and Watermarking	Steganalysis	1
3.1.14 Theoretical Foundations	Formal verification of security assurance	1
3.1.15 Trust Management and Accountability	Social aspects of trust	1
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML security management	1
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML-related standards	1
16. Artificial Intelligence (New area not included in JRC Taxonomy)	Ethical and trustworthy AI/ML	1

3.2.3 Turun yliopisto – 27 kurssia

Kybertuvallisuusroolien ja avainosaamisten pohjalta tarkasteltuna koulutuksella on seuraavia piirteitä:

- Roolikohtainen painotus: Koulutusohjelmissa on painotettu erityisesti rooleja kuten Cyber Incident Responder ja CISO (Chief Information Security Officer)
- Monialaiset osaamiset: Koulutus kattaa laajasti eri osa-alueita, mukaan lukien tekniset taidot kuten tietoverkkojen ja käyttöjärjestelmien turvallisuus. Hallinnolliset taidot, kuten turvallisuuspolitiikat ja riskienhallinta, sekä oikeudelliset ja sääntelyyn liittyvät taidot (näihin liittyvät vaatimukset) ovat myös keskeisiä osia koulutuksessa.
- Laaja-alainen koulutus**:** Koulutus tarjoaa laaja-alaisen lähestymistavan, joka sisältää strategiset, tekniset ja operatiiviset kyberturvallisuuden osa-alueet.

Kurssit ovat laajasti suunnattuja kattamaan sekä teoreettista tietämystä että käytännön taitoja. Tämä korostaa näiden roolien kriittistä merkitystä organisaatioiden kyberturvallisuusstrategioissa.

Turun yliopiston kyberturvallisuuden koulutuksessa on vahva painotus teknisessä ja operatiivisessa osaamisessa, ja tämän lisäksi strategisessa ja hallinnollisessa osaamisessa, mikä on välttämätöntä nykyisten ja tulevien kyberuhkien hallinnassa. Kurssien sisältö heijastaa laajaa osaamisvaatimusta, joka kattaa strategiset, tekniset ja lakiin tai muihin vastaaviin rajoituksiin liittyvät osa-alueet. Kurssit pyrkivät varmistamaan, että valmistuvilla opiskelijoilla on laaja-alainen osaaminen ja kyky vastata nykyaikaisen kyberturvallisuusympäristön tarpeisiin painottaen teknisiä näkökulmia ja ratkaisuja huomioiden myös hallinnolliset haasteet.

Turun yliopiston kyberturvallisuuskoulutuksen keskeiset roolit ja osaamisalueet on kuvattu Taulukossa 18. Taulukoissa 19 ja 20 on nähtävillä 20 eniten kyberturvallisuuskoulutuksessa esiintyvää avainosaamista ja niihin kuhunkin liittyvät kyberturvallisuusroolit. Taulukkojen 19 ja 20 Total-arvo kertoo, kuinka monta kertaa kyseinen avainosaaminen on tunnistettu eri kursseissa. Em. taulukoiden Total-

arvoihin perustuen Turun yliopiston kyberturvallisuuskoulutuksen avainosaamiset ja niihin liittyvät kyberturvallisuusroolit ovat:

1. **CISO (Chief Information Security Officer) (757 teoria + 264 käytäntö = 1021)**:

    - Kyberturvallisuuden suositukset ja parhaat käytännöt (170 teoria, 65 käytäntö)
    - Kyberturvallisuuden standardit, metodologiat ja viitekehykset (155 teoria, 50 käytäntö)
    - Kyberturvallisuuspolitiikat (150 teoria, 54 käytäntö)
    - Riskienhallinnan standardit, metodologiat ja viitekehykset (148 teoria, 51 käytäntö)
    - Kyberturvallisuuteen liittyvät lait ja säädökset (134 teoria, 44 käytäntö)

2. **Cyber Incident Responder (583 teoria + 175 käytäntö = 758)**:

    - Tietoverkkojen turvallisuus (330 teoria, 102 käytäntö)
    - Käyttöjärjestelmien turvallisuus (253 teoria, 73 käytäntö)
    - Secure Operation Centre (SOC) -operointi (39 käytäntö)

3. **Cyber Threat Intelligence Specialist (506 teoria + 149 käytäntö = 655)**:

    - Tietoverkkojen turvallisuus (289 teoria, 89 käytäntö)
    - Käyttöjärjestelmien turvallisuus (208 teoria, 60 käytäntö)

4. **Cyber Security Implementer (489 teoria + 113 käytäntö = 602)**

    - Tietoverkkojen turvallisuus (192 teoria, 61 käytäntö)
    - Kyberturvallisuuden suositukset ja parhaat käytännöt (171 teoria, 52 käytäntö)
    - Käyttöjärjestelmien turvallisuus (126 teoria)

Taulukko 18. Turun yliopiston kyberturvallisuuskoulutuksen tarjoama teoria ja harjoitukset verrattuna ENISA:n kyberturvallisuusrooleihin

TEORIA		**HARJOITUKSET**	
Rooli	**# Roolin avainosaaminen top 50**	**Rooli**	**# Roolin avainosaaminen top 50**
CISO	10	Cyber Incident Responder	10
Cyber Incident Responder	10	CISO	9
Cybersecurity Risk Manager	7	Cybersecurity risk manager	7
Cybersecurity Implementer	5	Cybersecurity Implementer	5
Cybersecurity Architect	4	Cybersecurity Architect	4
Cyber Legal, Policy and Compliance Officer	3	Penetration tester	4
Cyber Threat Intelligence Specialist	3	Cyber Legal, Policy and Compliance Officer	3
Digital Forensics Investigator	3	Cyber Threat Intelligence Specialist	3
Penetration Tester	3	Digital forensics investigator	3
Cybersecurity Auditor	2	Cybersecurity Auditor	2

Taulukko 19. Turun yliopiston kyberturvallisuuskoulutuksen avainosaaminen teorian osalta - TOP 20 ENISA:n kyberturvallisuusrooli ja avainosaaminen

Rooli	Avainosaaminen	Käsitellään kursseilla (lkm)
Cybersecurity Architect	Cybersecurity recommendations and best practices	389
Cyber Incident Responder	Computer networks security	330
Cyber Threat Intelligence Specialist	Computer networks security	289
Cyber Incident Responder	Operating systems security	253
Penetration Tester	Computer networks security	237
Digital Forensics Investigator	Computer networks security	217
Cyber Threat Intelligence Specialist	Operating systems security	208
Cybersecurity Implementer	Computer networks security	192
Cybersecurity Implementer	Cybersecurity recommendations and best practices	171
CISO	Cybersecurity recommendations and best practices	170
Penetration Tester	Operating systems security	165
CISO	Cybersecurity standards, methodologies and frameworks	155
Digital Forensics Investigator	Operating systems security	152
CISO	Cybersecurity policies	150
CISO	Risk management standards, methodologies and framework	148
CISO	Cybersecurity related laws, regulations and legislations	134
Cybersecurity Auditor	Monitoring, testing and evaluating cybersecurity controls' effectiveness	130
Cybersecurity Risk Manager	Cybersecurity controls and solutions	128
Cybersecurity Implementer	Operating systems security	126
Cyber Legal, Policy and Compliance Officer	Legal, regulatory and legislative compliance requirements, recommendations and best practices	124

Taulukko 20. Turun yliopiston kyberturvallisuuskoulutuksen avainosaaminen harjoitusten osalta - TOP 20 ENISA:n kyberturvallisuusrooli ja avainosaaminen

Rooli	Avainosaaminen	Käsitellään kursseilla (lkm)
Cybersecurity Architect	Cybersecurity recommendations and best practices	114
Cyber Incident Responder	Computer networks security	102
Cyber Threat Intelligence Specialist	Computer networks security	89
Cyber Incident Responder	Operating systems security	73
Penetration Tester	Computer networks security	72
CISO	Cybersecurity recommendations and best practices	65
Digital Forensics Investigator	Computer networks security	65
Cybersecurity Implementer	Computer networks security	61
Cyber Threat Intelligence Specialist	Operating systems security	60
CISO	Cybersecurity policies	54
Cybersecurity Implementer	Cybersecurity recommendations and best practices	52
CISO	Risk management standards, methodologies and framework	51
CISO	Cybersecurity standards, methodologies and frameworks	50
Penetration Tester	Operating systems security	46
CISO	Cybersecurity related laws, regulations and legislations	44
Cybersecurity Risk Manager	Monitoring, testing and evaluating cybersecurity controls' effectiveness	43
Digital Forensics Investigator	Operating systems security	43
Cyber Legal, Policy And Compliance Officer	Legal, regulatory and legislative compliance requirements, recommendations and best practices	41
Cybersecurity Auditor	Legal, regulatory and legislative compliance requirements, recommendations and best practices	41
Cyber Incident Responder	Secure Operation Centres (SOCs) operation	39

3.2.4 Turun yliopiston kyberturvallisuuskurssien aiheet taksonomian mukaisesti tarkasteltuna

Seuraavat JRC:n taksonomian aiheet ovat saaneet laajaa käsittelyä Turun yliopiston opetusohjelmassa teorian ja harjoitusten osalta, mikä korostaa niiden merkitystä kyberturvallisuuden pohjaosaamisen ja ymmärryksen rakentamisessa osana kursseja (Taulukko 21 ja Taulukko 22):

Taksonomian aihealueet ja painotus:

- Software and Hardware Security Engineering: Teknisten taitojen korostaminen on olennainen osa koulutusta.
- Education and Training sekä Human Aspects: Tietoturvatietoisuuden lisääminen ja käyttäjäystävällisyyden huomioon ottaminen korostavat ihmisten ja teknologian vuorovaikutuksen merkitystä. Tämä on huomioitava osana teknisiä ratkaisuja.
- Assurance, Audit, and Certification: Nämä aiheet ovat hyvin edustettuina kursseilla, mikä heijastaa tarvetta ymmärtää ja hallinnoida turvallisuusratkaisuja.
- Legal Aspects: Koulutus sisältää aiheita, jotka käsittelevät järjestelmien vaatimuksiin liittyvää sääntelyanalyysiä, korostaen oikeudellisten näkökulmien ymmärtämisen tärkeyttä.

Kursseilla eniten käsiteltyjä aiheita taksonomian mukaisesti (Taulukko 21 ja Taulukko 22):

Identity Management

- Identity Management Quality Assurance: Käsitelty yhteensä 28 kertaa (20 teoria + 8 käytäntö)

Theoretical Foundations

- Formal Specification, Analysis, and Verification of Software and Hardware: Käsitelty yhteensä 16 kertaa (16 teoria + 0 käytäntö)

Cryptology (Cryptography and Cryptanalysis)

- Symmetric Cryptography: Käsitelty yhteensä 19 kertaa (14 teoria + 5 käytäntö)
- Cryptanalysis Methodologies, Techniques and Tools: Käsitelty yhteensä 19 kertaa (14 teoria + 5 käytäntö)

Data Security and Privacy

- Privacy Enhancing Technologies (PET): Käsitelty yhteensä 14 kertaa (14 teoria + 0 käytäntö)

Security Measurements

- Security Metrics, Key Performance Indicators, and Benchmarks: Käsitelty yhteensä 14 kertaa (14 teoria + 0 käytäntö)

Kursseilla vähiten käsiteltyjä aiheita taksonomian mukaisesti (Taulukko 23 ja Taulukko 24):

Assurance, Audit, and Certification

- **Assurance: Ei käsitelty lainkaan (0 teoria + 0 käytäntö)**

Cryptology (Cryptography and Cryptanalysis)

- Digital signatures: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Post-quantum cryptography: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Homomorphic encryption: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Data Security and Privacy

- Privacy requirements for data management systems: Ei käsitelty (1 teoria + 0 käytäntö)
- Risk analysis and attacks with respect to de-anonymization or data re-identification: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Human Aspects

- Accessibility: Ei käsitelty (1 teoria + 0 käytäntö)
- Enhancing risk perception: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Psychological models and cognitive processes: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Cybersecurity profiling: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Security visualization: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Gamification: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

- Human perception of cybersecurity: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- History of cybersecurity: Ei käsitelty (1 teoria + 0 käytäntö)

Identity Management

- Protocols and frameworks for authentication, authorization, and rights management: Ei käsitelty (1 teoria + 0 käytäntö)

Legal Aspects

- Cybercrime prosecution and law enforcement: Ei käsitelty (1 teoria + 0 käytäntö)
- Cybersecurity regulation analysis and design: Ei käsitelty (1 teoria + 0 käytäntö)

Security Management and Governance

- Assessment of information security effectiveness and degrees of control: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Economic aspects of the cybersecurity ecosystem: Ei käsitelty (1 teoria + 0 käytäntö)
- Capability maturity models: Ei käsitelty lainkaan (0 teoria + 0 käytäntö)

Security Measurements

- Security analytics and visualization: Ei käsitelty (1 teoria + 0 käytäntö)
- Validation and comparison frameworks for security metrics: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Measurement and assessment of security levels: Ei käsitelty lainkaan (0 teoria + 0 käytäntö)

Software and Hardware Security Engineering

- Runtime security verification and enforcement: Ei käsitelty (1 teoria + 0 käytäntö)
- Security testing and validation: Ei käsitelty lainkaan (0 teoria + 0 käytäntö)
- Privacy by design: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö).

Steganography, Steganalysis, and Watermarking

- Steganography: Ei käsitelty (1 teoria + 0 käytäntö)
- Digital watermarking: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Taulukko 21. Turun yliopiston kurssien eniten käsittelemät aiheet teorian osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.6 Identity Management	Identity management quality assurance	20
3.1.14 Theoretical Foundations	Formal specification, analysis, and verification of software and hardware	16
3.1.14 Theoretical Foundations	Formal specification of various aspects of security (e.g properties, threat models, etc.)	15
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Symmetric cryptography	14
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Cryptanalysis methodologies, techniques and tools	14
3.1.3 Data Security and Privacy	Privacy Enhancing Technologies (PET)	14
3.1.6 Identity Management	Optical and electronic document security	14
3.1.6 Identity Management	Biometric methods, technologies and tools	14
3.1.7 Incident Handling and Digital Forensics	Theories, techniques and tools for the identification, collection, attribution, acquisition, analysis and preservation of digital evidence (e.g. code authorship and attacker identification, provenance assurance, digital evidence correlation, digital evidence triage)	14
3.1.11 Security Measurements	Security metrics, key performance indicators, and benchmarks	14
3.1.14 Theoretical Foundations	Formal specification and verification of the various aspects of security;	14
3.1.1 Assurance, Audit, and Certification	Certification	13
3.1.15 Trust Management and Accountability	Trust and privacy	13
3.1.15 Trust Management and Accountability	Identity and trust management	13
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML security management	13
3.1.8 Legal Aspects	Intellectual property rights	12
3.1.12 Software and Hardware Security Engineering	Quantitative security for assurance	12
3.1.15 Trust Management and Accountability	Algorithmic auditability and accountability (e.g. explainable AI)	12

Taulukko 22. Turun yliopiston kurssien eniten käsittelemät aiheet harjoitusten osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.6 Identity Management	Identity management quality assurance	20
3.1.7 Incident Handling and Digital Forensics	Theories, techniques and tools for the identification, collection, attribution, acquisition, analysis and preservation of digital evidence (e.g. code authorship and attacker identification, provenance assurance, digital evidence correlation, digital evidence triage)	16
3.1.4 Education and Training	Cyber ranges, Capture the Flag, exercises, simulation platforms, educational/training tools, cybersecurity awareness	15
3.1.1 Assurance, Audit, and Certification	Certification	14
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Symmetric cryptography	14
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Cryptanalysis methodologies, techniques and tools	14
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Crypto material management (e.g. key management, PKI)	14
3.1.5 Human Aspects	Privacy concerns, behaviours, and practices	14
3.1.10 Security Management and Governance	Compliance with information security and privacy policies, procedures, and regulations	14
3.1.12 Software and Hardware Security Engineering	Quantitative security for assurance	14
3.1.15 Trust Management and Accountability	Trust in securing digital as well as physical assets	14

Taulukko 23. Turun yliopiston kurssien vähiten käsittelemät aiheet teorian osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.3 Data Security and Privacy	Privacy requirements for data management systems	1
3.1.5 Human Aspects	Accessibility	1
3.1.5 Human Aspects	History of cybersecurity	1
3.1.6 Identity Management	Protocols and frameworks for authentication, authorization, and rights management	1
3.1.8 Legal Aspects	Cybercrime prosecution and law enforcement	1
3.1.8 Legal Aspects	Cybersecurity regulation analysis and design	1
3.1.10 Security Management and Governance	Economic aspects of the cybersecurity ecosystem	1
3.1.11 Security Measurements	Security analytics and visualization	1
3.1.11 Security Measurements	Measurement and assessment of security levels	1
3.1.12 Software and Hardware Security Engineering	Security documentation	1
3.1.12 Software and Hardware Security Engineering	Runtime security verification and enforcement	1
3.1.12 Software and Hardware Security Engineering	Vulnerability discovery and penetration testing	1
3.1.13 Steganography, Steganalysis and Watermarking	Steganography	1
3.1.14 Theoretical Foundations	Cybersecurity uncertainty models	1
3.1.1 Assurance, Audit, and Certification	Assurance	0
3.1.10 Security Management and Governance	Capability maturity models (e.g. assessment of capacities and capabilities)	0
3.1.12 Software and Hardware Security Engineering	Security testing and validation	0
3.1.13 Steganography, Steganalysis and Watermarking	Digital watermarking	0

Taulukko 24. Turun yliopiston kurssien vähiten käsittelemät aiheet teorian osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.1 Assurance, Audit, and Certification	Assurance	0
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Digital signatures	0
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Post-quantum cryptography	0
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Homomorphic encryption	0
3.1.3 Data Security and Privacy	Privacy requirements for data management systems	0
3.1.3 Data Security and Privacy	Risk analysis and attacks with respect to de-anonymization or data re-identification (e.g. inference attack)	0
3.1.4 Education and Training	Higher Education	0
3.1.5 Human Aspects	Accessibility	0
3.1.5 Human Aspects	Enhancing risk perception	0
3.1.5 Human Aspects	Psychological models and cognitive processes	0
3.1.5 Human Aspects	Cybersecurity profiling	0
3.1.5 Human Aspects	Security visualization	0
3.1.5 Human Aspects	Gamification	0
3.1.5 Human Aspects	Human perception of cybersecurity	0
3.1.5 Human Aspects	History of cybersecurity	0
3.1.6 Identity Management	Protocols and frameworks for authentication, authorization, and rights management	0
3.1.8 Legal Aspects	Cybercrime prosecution and law enforcement	0
3.1.10 Security Management and Governance	Assessment of information security effectiveness and degrees of control	0
3.1.10 Security Management and Governance	Economic aspects of the cybersecurity ecosystem	0
3.1.10 Security Management and Governance	Capability maturity models (e.g. assessment of capacities and capabilities)	0

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.11 Security Measurements	Security analytics and visualization	0
3.1.11 Security Measurements	Validation and comparison frameworks for security metrics	0
3.1.11 Security Measurements	Measurement and assessment of security levels	0
3.1.12 Software and Hardware Security Engineering	Runtime security verification and enforcement	0
3.1.12 Software and Hardware Security Engineering	Security testing and validation	0
3.1.12 Software and Hardware Security Engineering	Privacy by design	0
3.1.13 Steganography, Steganalysis and Watermarking	Steganography	0
3.1.13 Steganography, Steganalysis and Watermarking	Digital watermarking	0

3.3 Kyberturvallisuussuuntautumisen tarjoavat yliopistot – yli 8 kurssia raportoineet

Seuraavassa tarkastellaan vähintään 9 kurssia raportoineet yliopistot, jotka tarjoavat myös kyberturvallisuuteen keskittyviä opintoja. Yliopistot esitetään aakkosjärjestyksessä. Roolien/avainosaamisten ja taksonomian käsittelyyn liittyvissä taulukoissa on otettu mukaan kaikki samanarvoiset tiedot. Tämän takia taulukoiden koot voivat vaihdella eri yliopistoilla, koska taulukkoon on otettu esim. kaikki 0 arvon saaneet kurssit.

3.3.1 Oulun yliopisto – 9 kurssia

Kyberturvallisuusalan kurssit keskittyvät tärkeimpiin kyberturvallisuuden rooleihin ja osaamisalueisiin sekä teoriassa että käytännön harjoituksissa. joille annetaan erityistä huomiota niin teoreettisen tiedon kuin käytännön taitojen osalta. Kybertuvallisuusroolien ja avainosaamisten pohjalta tarkasteltuna koulutuksella on seuraavia piirteitä:

- Roolikohtainen painotus: Keskeisiä rooleja ovat muun muassa Cyber Incident Responder ja CISO.
- Keskeiset osaamisalueet: Kurssit korostavat kyberturvallisuuden suosituksia ja parhaita käytäntöjä, tietoverkkojen turvallisuutta, ja käyttöjärjestelmien turvallisuutta. Kurssit tarjoavat aiheita, jotka kattavat tekniset taidot, hallinnolliset kyvykkyydet ja oikeudelliset vaatimukset.
- Lainsäädäntö ja politiikat: Erityisesti CISO-rooliin liittyen kursseilla käsitellään kyberturvallisuuteen liittyviä lakeja ja säädöksiä, mikä korostaa hallinnollista ulottuvuutta.

Oulun yliopiston kyberturvallisuuskoulutuksen keskeiset roolit ja osaamisalueet on esitetty Taulukossa 25. Taulukoissa 26 ja 27 on nähtävillä 20 kyberturvallisuuskoulutuksessa eniten esiintyvää avainosaamista ja niistä kuhunkin liittyvät kyberturvallisuusroolit. Taulukoiden 26 ja 27 Total arvo kertoo, kuinka monta kertaa kyseinen avainosaaminen on tunnistettu eri kursseissa. Em. taulukoiden Total-arvoihin perustuen Oulun yliopiston kyberturvallisuuskoulutuksen avainosaamiset ja niihin liittyvät kyberturvallisuusroolit ovat:

1. **CISO (Chief Information Security Officer) (313 teoria + 634 käytäntö = 947)**:

    - Kyberturvallisuuden suositukset ja parhaat käytännöt (56 teoria, 116 käytäntö)
    - Kyberturvallisuuden standardit, metodologiat ja viitekehykset (56 teoria, 110 käytäntö)
    - Kyberturvallisuuspolitiikat (64 teoria, 114 käytäntö)
    - Riskienhallinnan standardit, metodologiat ja viitekehykset (66 teoria, 108 käytäntö)
    - Kyberturvallisuuteen liittyvät lait ja säädökset (71 teoria, 107 käytäntö)
    - Johtamiskäytännöt (79 käytäntö)

2. **Cyber Incident Responder (teoria 209 + käytäntö 240 = 449)**:

    - Tietoverkkojen turvallisuus (106 teoria, 146 käytäntö)
    - Käyttöjärjestelmien turvallisuus (103 teoria, 94 käytäntö)

3. **Cyber Threat Intelligence Specialist (188 teoria + 207 käytäntö = 395)**:

    - Tietoverkkojen turvallisuus (97 teoria, 131 käytäntö)
    - Käyttöjärjestelmien turvallisuus (91 teoria, 76 käytäntö)

4. **Cybersecurity Architect (teoria 169 + käytäntö 178 = 347)**:

    - Kyberturvallisuuden suositukset ja parhaat käytännöt (169 teoria, 178 käytäntö)

Taulukko 25. Oulun yliopiston kyberturvallisuuskoulutuksen tarjoama teoria ja harjoitukset verrattuna ENISA:n kyberturvallisuusrooleihin

TEORIA		**HARJOITUKSET**	
Rooli	**# Roolin avainosaaminen top 50**	**Rooli**	**# Roolin avainosaaminen top 50**
CISO	10	CISO	9
Cyber Incident Responder	8	Cyber Incident Responder	8
Cybersecurity Risk Manager	7	Cybersecurity Implementer	8
Cybersecurity Architect	5	Cybersecurity Risk Manager	7
Cybersecurity Implementer	5	Cybersecurity Architect	4
Cyber Legal, Policy and Compliance Officer	3	Cyber Legal, Policy and Compliance Officer	3
Cyber Threat Intelligence Specialist	3	Cybersecurity Auditor	3
Cybersecurity Auditor	3	Digital Forensics Investigator	3
Digital Forensics Investigator	3	Penetration Tester	3
Penetration Tester	2	Cyber Threat Intelligence Specialist	2

Taulukko 26. Oulun yliopiston kyberturvallisuuskoulutuksen avainosaaminen teorian osalta - TOP 20 ENISA:n kyberturvallisuusrooli ja avainosaaminen

Rooli	Avainosaaminen	Käsitellään kursseilla (lkm)
Cybersecurity Architect	Cybersecurity recommendations and best practices	169
Cyber Incident Responder	Computer networks security	106
Cyber Incident Responder	Operating systems security	103
Cyber Threat Intelligence Specialist	Computer networks security	97
Cyber Threat Intelligence Specialist	Operating systems security	91
Penetration Tester	Computer networks security	81
Cybersecurity Implementer	Cybersecurity recommendations and best practices	73
Digital Forensics Investigator	Computer networks security	73
CISO	Cybersecurity related laws, regulations and legislations	71
Cybersecurity Risk Manager	Monitoring, testing and evaluating cybersecurity controls' effectiveness	69
Cybersecurity Auditor	Monitoring, testing and evaluating cybersecurity controls' effectiveness	67
CISO	Risk management standards, methodologies and framework	66
CISO	Cybersecurity policies	64
Cybersecurity Implementer	Computer networks security	64
Cyber Legal, Policy and Compliance Officer	Legal, regulatory and legislative compliance requirements, recommendations and best practices	62
Penetration Tester	Operating systems security	61
Cybersecurity Risk Manager	Cybersecurity controls and solutions	59
Cybersecurity Auditor	Legal, regulatory and legislative compliance requirements, recommendations and best practices	58
CISO	Cybersecurity standards, methodologies and frameworks	56
CISO	Cybersecurity recommendations and best practices	56

Taulukko 27. Oulun yliopiston kyberturvallisuuskoulutuksen avainosaaminen harjoitusten osalta - TOP 20 ENISA:n kyberturvallisuusrooli ja avainosaaminen

Rooli	Avainosaaminen	Käsitellään kursseilla (lkm)
Cybersecurity Architect	Cybersecurity recommendations and best practices	178
Cyber Incident Responder	Computer networks security	146
Cyber Threat Intelligence Specialist	Computer networks security	131
CISO	Cybersecurity recommendations and best practices	116
CISO	Cybersecurity policies	114
CISO	Cybersecurity standards, methodologies and frameworks	110
CISO	Risk management standards, methodologies and framework	108
CISO	Cybersecurity related laws, regulations and legislations	107
Penetration Tester	Computer networks security	103
Cyber Legal, Policy and Compliance Officer	Legal, regulatory and legislative compliance requirements, recommendations and best practices	100
Cybersecurity Auditor	Monitoring, testing and evaluating cybersecurity controls' effectiveness	95
Digital Forensics Investigator	Computer networks security	95
Cyber Incident Responder	Operating systems security	94
Cybersecurity Auditor	Legal, regulatory and legislative compliance requirements, recommendations and best practices	94
Cybersecurity Risk Manager	Monitoring, testing and evaluating cybersecurity controls' effectiveness	87
Cybersecurity Implementer	Cybersecurity recommendations and best practices	81
Cybersecurity Implementer	Computer networks security	80
CISO	Management practices	79
Cyber Threat Intelligence Specialist	Operating systems security	76
Cybersecurity Implementer	Cybersecurity controls and solutions	76

3.3.2 Oulun yliopiston kyberturvallisuuskurssien aiheet taksonomian mukaisesti tarkasteltuna

Seuraavat JRC:n taksonomian aiheet ovat saaneet laajaa käsittelyä Oulun yliopiston opetusohjelmassa teorian ja harjoitusten osalta, mikä korostaa niiden merkitystä kyberturvallisuuden pohjaosaamisen ja ymmärryksen rakentamista osana kursseja (Taulukko 28 ja Taulukko 29):

Kursseilla eniten käsitellyt aiheet taksonomian mukaisesti:

Data Security and Privacy

- Data integrity: Käsitelty yhteensä 14 kertaa (8 teoria + 6 käytäntö)

Assurance, Audit, and Certification

- Assurance: Käsitelty yhteensä 14 kertaa (7 teoria + 7 käytäntö)
- Audit: Käsitelty yhteensä 12 kertaa (7 teoria + 5 käytäntö)
- Assessment: Käsitelty yhteensä 12 kertaa (7 teoria + 5 käytäntö)

Education and Training

- Higher Education: Käsitelty yhteensä 14 kertaa (7 teoria + 7 käytäntö)
- Professional training: Käsitelty yhteensä 12 kertaa (6 teoria + 6 käytäntö)
- Cyber ranges, Capture the Flag exercises, simulation platforms, educational/training tools, cybersecurity awareness: Käsitelty yhteensä 12 kertaa (6 teoria + 6 käytäntö)

Cryptology (Cryptography and Cryptanalysis)

- Message authentication: Käsitelty yhteensä 11 kertaa (6 teoria + 5 käytäntö)

Legal Aspects

- Cybersecurity regulation analysis and design: Käsitelty yhteensä 11 kertaa (6 teoria + 5 käytäntö)

Security Management and Governance

- Modelling of cross-sectoral interdependencies and cascading effects: Käsitelty yhteensä 12 kertaa (6 teoria + 6 käytäntö)
- Governance aspects of incident management, disaster recovery, business continuity: Käsitelty yhteensä 11 kertaa (6 teoria + 5 käytäntö)

Theoretical Foundations

- Formal specification of various aspects of security (e.g., properties, threat models, etc.): Käsitelty yhteensä 12 kertaa (6 teoria + 6 käytäntö)

Trust Management and Accountability

- Social aspects of trust: Käsitelty yhteensä 12 kertaa (6 teoria + 6 käytäntö)

Kursseilla vähiten käsiteltyjä aiheita taksonomian mukaisesti (Taulukko 30 ja Taulukko 31):

Incident Handling and Digital Forensics

- Resilience aspects: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö).
- Coordination and information sharing in the context of cross-border/organizational incidents: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö).

Network and Distributed Systems

- Fault tolerant models: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö).

Security Management and Governance

- Compliance with information security and privacy policies, procedures and regulations: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö).
- Capability maturity models (e.g., assessment of capacities and capabilities): Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö).

Software and Hardware Security Engineering

- Security requirements engineering with emphasis on identity, privacy, accountability, and trust: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö).
- Runtime security verification and enforcement: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö).

Artificial Intelligence (New area not included in JRC Taxonomy)

- AI/ML Legislation: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö).
- Fundamentals of AI/ML (Algorithms, methods, assets, procedures, etc.): Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö).

- AI/ML threat assessment (e.g., evasion, oracle poisoning): Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö).
- AI/ML security management: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö).
- AI/ML-related standards: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö).

Taulukko 28. Oulun yliopiston kurssien eniten käsittelemät aiheet teorian osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	**Taksonomian aihe**	**Kurssien lkm**
3.1.3 Data Security and Privacy	Data integrity	8
3.1.1 Assurance, Audit, and Certification	Assurance	7
3.1.1 Assurance, Audit, and Certification	Audit	7
3.1.1 Assurance, Audit, and Certification	Assessment	7
3.1.4 Education and Training	Higher Education	7
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Message authentication	6
3.1.4 Education and Training	Professional training	6
3.1.4 Education and Training	Cyber ranges, Capture the Flag, exercises, simulation platforms, educational/training tools, cybersecurity awareness	6
3.1.8 Legal Aspects	Cybersecurity regulation analysis and design	6
3.1.10 Security Management and Governance	Modelling of cross-sectoral interdependencies and cascading effects	6
3.1.10 Security Management and Governance	Governance aspects of incident management, disaster recovery, business continuity	6
3.1.14 Theoretical Foundations	Formal specification of various aspects of security (e.g properties, threat models, etc.)	6
3.1.15 Trust Management and Accountability	Social aspects of trust	6

Taulukko 29. Oulun yliopiston kurssien eniten käsittelemät aiheet harjoitusten osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.3 Data Security and Privacy	Data integrity	6
3.1.4 Education and Training	Cyber ranges, Capture the Flag, exercises, simulation platforms, educational/training tools, cybersecurity awareness	6
3.1.6 Identity Management	Privacy and identity management (e.g. privacy-preserving authentication)	6
3.1.1 Assurance, Audit, and Certification	Audit	5
3.1.1 Assurance, Audit, and Certification	Assessment	5
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Message authentication	5
3.1.8 Legal Aspects	Cybersecurity regulation analysis and design	5
3.1.10 Security Management and Governance	Governance aspects of incident management, disaster recovery, business continuity	5

Taulukko 30. Oulun yliopiston kurssien vähiten käsittelemät aiheet teorian osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.5 Human Aspects	Enhancing risk perception	1
3.1.5 Human Aspects	Privacy concerns, behaviours, and practices	1
3.1.5 Human Aspects	Transparent security	1
3.1.5 Human Aspects	Cybersecurity profiling	1
3.1.5 Human Aspects	Security visualization	1
3.1.6 Identity Management	Identity management quality assurance	1
3.1.6 Identity Management	Biometric methods, technologies and tools	1

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.7 Incident Handling and Digital Forensics	Vulnerability analysis and response	1
3.1.7 Incident Handling and Digital Forensics	Digital forensic processes and workflow models	1
3.1.7 Incident Handling and Digital Forensics	Digital forensic case studies	1
3.1.7 Incident Handling and Digital Forensics	Policy issues related to digital forensics	1
3.1.7 Incident Handling and Digital Forensics	Anti-forensics and malware analytics	1
3.1.8 Legal Aspects	Intellectual property rights	1
3.1.9 Network and Distributed Systems	Network security (principles, methods, protocols, algorithms and technologies)	1
3.1.9 Network and Distributed Systems	Protocols and frameworks for secure distributed computing	1
3.1.9 Network and Distributed Systems	Network interoperability	1
3.1.10 Security Management and Governance	Identification of the impact of hardware and software changes on the management of Information Security	1
3.1.10 Security Management and Governance	Privacy impact assessment and risk management	1
3.1.10 Security Management and Governance	Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling)	1
3.1.11 Security Measurements	Validation and comparison frameworks for security metrics	1
3.1.12 Software and Hardware Security Engineering	Security and risk analysis of components compositions	1
3.1.12 Software and Hardware Security Engineering	Secure software architectures and design (security by design)	1
3.1.12 Software and Hardware Security Engineering	Security support in programming environments	1
3.1.12 Software and Hardware Security Engineering	Security documentation	1
3.1.12 Software and Hardware Security Engineering	Security testing and validation	1
3.1.12 Software and Hardware Security Engineering	Attack techniques (e.g. side channel attacks, power attacks, stealth attacks,	1

Taksonomian alue	Taksonomian aihe	Kurssien lkm
	advanced persistent attacks, rowhammer attacks)	
3.1.12 Software and Hardware Security Engineering	Privacy by design	1
3.1.13 Steganography, Steganalysis And Watermarking	Steganalysis	1
3.1.15 Trust Management and Accountability	Trust in securing digital as well as physical assets	1
16. Artificial Intelligence (New area not included in JRC Taxonomy)	Application of AI/ML in cybersecurity	1
16. Artificial Intelligence (New area not included in JRC Taxonomy)	Ethical and trustworthy AI/ML	1
16. Artificial Intelligence (New area not included in JRC Taxonomy)	Human related threats for AI/ML in cybersecurity	1
3.1.4 Education and Training	Vocational training	0
3.1.7 Incident Handling and Digital Forensics	Resilience aspects	0
3.1.7 Incident Handling and Digital Forensics	Coordination and information sharing in the context of cross-border/organizational incidents	0
3.1.9 Network and Distributed Systems	Fault tolerant models	0
3.1.10 Security Management and Governance	Compliance with information security and privacy policies, procedures, and regulations	0
3.1.10 Security Management and Governance	Capability maturity models (e.g. assessment of capacities and capabilities)	0
3.1.12 Software and Hardware Security Engineering	Security requirements engineering with emphasis on identity, privacy, accountability, and trust	0
3.1.12 Software and Hardware Security Engineering	Runtime security verification and enforcement	0
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML Legislation	0
16. Artificial Intelligence (New area not included in JRC Taxonomy)	Fundamentals of AI/ML (Algorithms, methods, assets, procedures, etc.)	0
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML threat assessment (e.g. evasion, oracle, poisoning)	0
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML security management	0

Taksonomian alue	Taksonomian aihe	Kurssien lkm
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML-related standards	0

Taulukko 31. Oulun yliopiston kurssien vähiten käsittelemät aiheet harjoitusten osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.3 Data Security and Privacy	Design, implementation, and operation of data management systems that include security and privacy functions	0
3.1.4 Education and Training	Cybersecurity-aware culture (e.g. including children education)	0
3.1.4 Education and Training	Education methodology	0
3.1.4 Education and Training	Vocational training	0
3.1.5 Human Aspects	Socio-technical security	0
3.1.5 Human Aspects	Enhancing risk perception	0
3.1.5 Human Aspects	Psychological models and cognitive processes	0
3.1.5 Human Aspects	Forensic cyberpsychology	0
3.1.5 Human Aspects	Privacy concerns, behaviours, and practices	0
3.1.5 Human Aspects	Transparent security	0
3.1.5 Human Aspects	Cybersecurity profiling	0
3.1.5 Human Aspects	Security visualization	0
3.1.5 Human Aspects	Human aspects of trust	0
3.1.7 Incident Handling and Digital Forensics	Digital forensic processes and workflow models	0
3.1.7 Incident Handling and Digital Forensics	Digital forensic case studies	0
3.1.7 Incident Handling and Digital Forensics	Policy issues related to digital forensics	0
3.1.7 Incident Handling and Digital Forensics	Resilience aspects	0
3.1.7 Incident Handling and Digital Forensics	Coordination and information sharing in the context of cross-border/organizational incidents	0

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.9 Network and Distributed Systems	Requirements for network security	0
3.1.9 Network and Distributed Systems	Protocols and frameworks for secure distributed computing	0
3.1.9 Network and Distributed Systems	Fault tolerant models	0
3.1.10 Security Management and Governance	Identification of the impact of hardware and software changes on the management of Information Security	0
3.1.10 Security Management and Governance	Compliance with information security and privacy policies, procedures, and regulations	0
3.1.10 Security Management and Governance	Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling)	0
3.1.10 Security Management and Governance	Capability maturity models (e.g. assessment of capacities and capabilities)	0
3.1.11 Security Measurements	Validation and comparison frameworks for security metrics	0
3.1.12 Software and Hardware Security Engineering	Security requirements engineering with emphasis on identity, privacy, accountability, and trust	0
3.1.12 Software and Hardware Security Engineering	Security and risk analysis of components compositions	0
3.1.12 Software and Hardware Security Engineering	Security design patterns	0
3.1.12 Software and Hardware Security Engineering	Secure programming principles and best practices	0
3.1.12 Software and Hardware Security Engineering	Security support in programming environments	0
3.1.12 Software and Hardware Security Engineering	Runtime security verification and enforcement	0
3.1.12 Software and Hardware Security Engineering	Model-driven security and domain-specific modelling languages	0
3.1.12 Software and Hardware Security Engineering	Attack techniques (e.g. side channel attacks, power attacks, stealth attacks, advanced persistent attacks, rowhammer attacks)	0
3.1.12 Software and Hardware Security Engineering	Privacy by design	0

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.13 Steganography, Steganalysis and Watermarking	Steganalysis	0
3.1.14 Theoretical Foundations	Cybersecurity concepts, definitions, ontologies, taxonomies, foundational aspects	0
3.1.15 Trust Management and Accountability	Semantics and models for security, accountability, privacy, and trust	0
3.1.15 Trust Management and Accountability	Trust in securing digital as well as physical assets	0
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML Legislation	0
16. Artificial Intelligence (New area not included in JRC Taxonomy)	Fundamentals of AI/ML (Algorithms, methods, assets, procedures, etc.)	0
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML threat assessment (e.g. evasion, oracle, poisoning)	0
16. Artificial Intelligence (New area not included in JRC Taxonomy)	Application of AI/ML in cybersecurity	0
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML security management	0
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML-related standards	0
16. Artificial Intelligence (New area not included in JRC Taxonomy)	Ethical and trustworthy AI/ML	0
16. Artificial Intelligence (New area not included in JRC Taxonomy)	Human related threats for AI/ML in cybersecurity	0

3.3.3 Tampereen yliopisto – 13 kurssia

Kybertuvallisuusroolien ja avainosaamisten pohjalta tarkasteltuna koulutuksella on seuraavia piirteitä:

- Roolikohtainen painotus: Keskeisiä rooleja ovat CISO ja Cyber Incident Responder.
- Keskeiset osaamisalueet: Kurssit korostavat kyberturvallisuuden suosituksia ja parhaita käytäntöjä, tietoverkkojen turvallisuutta, ja käyttöjärjestelmien turvallisuutta. Kyberturvallisuuden suositukset ja parhaat käytännöt ovat keskeisessä roolissa.
- Tietoverkkojen turvallisuus ja käyttöjärjestelmien turvallisuus: Näitä aiheita käsitellään laajasti eri rooleissa, mikä heijastaa niiden tärkeyttä kyberturvallisuuden alalla.

Tampereen yliopiston kyberturvallisuuskoulutuksen keskeiset roolit ja osaamisalueet on esitetty Taulukossa 32. Taulukoissa 33 ja 34 on nähtävillä 20 kyberturvallisuuskoulutuksessa eniten esiintyvää avainosaamista ja niistä kuhunkin liittyvät kyberturvallisuusroolit. Taulukoiden 33 ja 34 Total-arvo kertoo, kuinka monta kertaa kyseinen avainosaaminen on tunnistettu eri kursseissa. Em. taulukoiden Total-arvoihin perustuen Tampereen yliopiston kyberturvallisuuskoulutuksen avainosaamiset ja niihin liittyvät kyberturvallisuusroolit ovat:

1. **CISO (Chief Information Security Officer) (567 teoria + 135 käytäntö = 702)**:

    - Kyberturvallisuuden suositukset ja parhaat käytännöt (121 teoria, 26 käytäntö)
    - Kyberturvallisuuteen liittyvät lait ja säädökset (117 teoria, 31 käytäntö)
    - Kyberturvallisuuden politiikat (112 teoria, 28 käytäntö)
    - Riskienhallinnan standardit (112 teoria, 25 käytäntö)
    - Kyberturvallisuuden standardit, metodologiat ja viitekehykset (105 teoria, 25 käytäntö)
    - Johtamiskäytännöt (23 käytäntö)

2. **Cyber Incident Responder (351 teoria + 129 käytäntö = 480)**:

    - Tietoverkkojen turvallisuus (187 teoria, 63 käytäntö)
    - Käyttöjärjestelmien turvallisuus (164 teoria, 66 käytäntö)

3. **Cyber Threat Intelligence Specialist (315 teoria + 118 käytäntö = 433)**:

    - Tietoverkkojen turvallisuus (171 teoria, 58 käytäntö)
    - Käyttöjärjestelmien turvallisuus (144 teoria, 60 käytäntö)

4. **Penetration tester (252 teoria + 101 käytäntö = 353):**

    - Tietoverkkojen turvallisuus (140 teoria, 52 käytäntö)
    - Käyttöjärjestelmien turvallisuus (112 teoria, 49 käytäntö)

Taulukko 32. Tampereen yliopiston kyberturvallisuuskoulutuksen tarjoama teoria ja harjoitukset verrattuna ENISA:n kyberturvallisuusrooleihin

TEORIA		**HARJOITUKSET**	
Rooli	**# Roolin avainosaaminen top 50**	**Rooli**	**# Roolin avainosaaminen top 50**
CISO	10	CISO	10
Cyber Incident Responder	10	Cyber Incident Responder	10
Cybersecurity Risk Manager	7	Cybersecurity Risk Manager	7
Cybersecurity Implementer	5	Cybersecurity Implementer	5
Cyber Legal, Policy and Compliance Officer	4	Digital Forensics Investigator	4
Digital Forensics Investigator	4	Cyber Legal, Policy and Compliance Officer	3
Cyber Threat Intelligence Specialist	3	Cyber Threat Intelligence Specialist	3
Cybersecurity Architect	3	Cybersecurity Architect	3
Cybersecurity Auditor	2	Cybersecurity Auditor	3
Penetration Tester	2	Penetration Tester	2

Taulukko 33. Tampereen yliopiston kyberturvallisuuskoulutuksen avainosaaminen teorian osalta - TOP 20 ENISA:n kyberturvallisuusrooli ja avainosaaminen

Rooli	Avainosaaminen	Käsitellään kursseilla (lkm)
Cybersecurity Architect	Cybersecurity recommendations and best practices	247
Cyber Incident Responder	Computer networks security	187
Cyber Threat Intelligence Specialist	Computer networks security	171
Cyber Incident Responder	Operating systems security	164
Cyber Threat Intelligence Specialist	Operating systems security	144
Penetration Tester	Computer networks security	140
Digital Forensics Investigator	Computer networks security	127
CISO	Cybersecurity recommendations and best practices	121
CISO	Cybersecurity related laws, regulations and legislations	117
Cybersecurity Implementer	Computer networks security	115
Cyber Legal, Policy and Compliance Officer	Legal, regulatory and legislative compliance requirements, recommendations and best practices	113
CISO	Cybersecurity policies	112
CISO	Risk management standards, methodologies and framework	112
Penetration Tester	Operating systems security	112
Digital Forensics Investigator	Operating systems security	107
CISO	Cybersecurity standards, methodologies and frameworks	105
Cybersecurity Implementer	Cybersecurity recommendations and best practices	105
Cybersecurity Auditor	Monitoring, testing and evaluating cybersecurity controls' effectiveness	104
Cybersecurity Risk Manager	Cybersecurity controls and solutions	98
Cybersecurity Risk Manager	Monitoring, testing and evaluating cybersecurity controls' effectiveness	96

Taulukko 34. Tampereen yliopiston kyberturvallisuuskoulutuksen avainosaaminen harjoitusten osalta - TOP 20 ENISA:n kyberturvallisuusrooli ja avainosaaminen

Rooli	Avainosaaminen	Käsitellään kursseilla (lkm)
Cybersecurity Architect	Cybersecurity recommendations and best practices	74
Cyber Incident Responder	Operating systems security	66
Cyber Incident Responder	Computer networks security	63
Cyber Threat Intelligence Specialist	Operating systems security	60
Cyber Threat Intelligence Specialist	Computer networks security	58
Penetration Tester	Computer networks security	52
Penetration Tester	Operating systems security	49
Digital Forensics Investigator	Computer networks security	45
Cybersecurity Implementer	Computer networks security	43
Digital Forensics Investigator	Operating systems security	43
Cybersecurity Implementer	Operating systems security	40
CISO	Cybersecurity related laws, regulations and legislations	31
Cyber Legal, Policy And Compliance Officer	Legal, regulatory and legislative compliance requirements, recommendations and best practices	30
CISO	Cybersecurity policies	28
CISO	Cybersecurity recommendations and best practices	26
CISO	Cybersecurity standards, methodologies and frameworks	25
CISO	Risk management standards, methodologies and framework	25
Cybersecurity Auditor	Monitoring, testing and evaluating cybersecurity controls' effectiveness	24
CISO	Management practices	23
Cybersecurity Auditor	Legal, regulatory and legislative compliance requirements, recommendations and best practices	22

3.3.4 Tampereen yliopiston kyberturvallisuuskurssien aiheet taksonomian mukaisesti tarkasteltuna

Seuraavat JRC:n taksonomian aiheet ovat saaneet laajaa käsittelyä Tampereen yliopiston opetusohjelmassa teorian ja harjoitusten osalta, mikä korostaa niiden merkitystä kyberturvallisuuden pohjaosaamisen ja ymmärryksen rakentamisessa osana kursseja (Taulukko 35 ja Taulukko 36):

Kursseilla eniten käsitellyt aiheet JRC:n taksonomian mukaisesti:

Cryptology (Cryptography and Cryptanalysis)

- Asymmetric cryptography: Käsitelty yhteensä 10 kertaa (10 teoria + 0 käytäntö)
- Symmetric cryptography: Käsitelty yhteensä 9 kertaa (9 teoria + 6 käytäntö)
- Hash functions: Käsitelty yhteensä 9 kertaa (9 teoria + 6 käytäntö)
- Crypto material management (e.g. key management, PKI): Käsitelty yhteensä 8 kertaa (8 teoria + 4 käytäntö)
- Digital signatures: Käsitelty yhteensä 8 kertaa (8 teoria + 5 käytäntö)
- Message authentication: Käsitelty yhteensä 8 kertaa (8 teoria + 0 käytäntö)

Software and Hardware Security Engineering

- Vulnerability discovery and penetration testing: Käsitelty yhteensä 9 kertaa (9 teoria + 0 käytäntö)
- Malware analysis including adversarial learning of malware: Käsitelty yhteensä 8 kertaa (8 teoria + 0 käytäntö)

Education and Training

- Cybersecurity-aware culture (e.g. including children education): Käsitelty yhteensä 8 kertaa (8 teoria + 0 käytäntö)
- Cyber ranges, Capture the Flag exercises, simulation platforms, educational/training tools, cybersecurity awareness: Käsitelty yhteensä 5 kertaa (5 teoria + 5 käytäntö)

Network and Distributed Systems

- Managerial, procedural, and technical aspects of network security: Käsitelty yhteensä 8 kertaa (8 teoria + 0 käytäntö)
- Network layer attacks and mitigation techniques: Käsitelty yhteensä 8 kertaa (8 teoria + 0 käytäntö)
- Protocols and frameworks for secure distributed computing: Käsitelty yhteensä 4 kertaa (0 teoria + 4 käytäntö)

Theoretical Foundations

- Formal specification of various aspects of security (e.g. properties, threat models, etc.): Käsitelty yhteensä 8 kertaa (8 teoria + 0 käytäntö)

Trust Management and Accountability

- Trust management architectures, mechanisms, and policies: Käsitelty yhteensä 8 kertaa (8 teoria + 0 käytäntö)

Security Management and Governance

- Techniques to ensure business continuity/disaster recovery: Käsitelty yhteensä 6 kertaa (0 teoria + 6 käytäntö)

Kursseilla vähiten käsiteltyjä aiheita taksonomian mukaisesti (Taulukko 37 ja Taulukko 38):

Assurance, Audit, and Certification

- Assurance: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Certification: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Cryptology (Cryptography and Cryptanalysis)

- Quantum cryptography: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Data Security and Privacy

- Data usage control: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Human Aspects

- Forensic cyberpsychology: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Automating security functionality: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Privacy concerns behaviours and practices: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Transparent security: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Cybersecurity profiling: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Security visualization: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Gamification: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Human perception of cybersecurity: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Identity Management

- Privacy and identity management (e.g. privacy-preserving authentication): Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Identity management quality assurance: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Biometric methods, technologies and tools: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Incident Handling and Digital Forensics

- Incident analysis, communication, documentation, forecasting (intelligence based), response and reporting: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Theories, techniques, and tools for the identification, collection, attribution, acquisition, analysis, and preservation of digital evidence: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Digital forensic processes and workflow models: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Policy issues related to digital forensics: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

- Resilience aspects: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Anti-forensics and malware analytics: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Coordination and information sharing in the context of cross-border/organizational incidents: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Legal Aspects

- Intellectual property rights: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Network and Distributed Systems

- Network security (principles, methods, protocols, algorithms, and technologies): Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Distributed systems security: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Network attack propagation analysis: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Distributed systems security analysis and simulation: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Fault tolerant models: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Secure distributed computations: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Network interoperability: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Secure system interconnection: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Security Management and Governance

- Threats and vulnerabilities modelling: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Identification of the impact of hardware and software changes on the management of Information Security: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

- Compliance with information security and privacy policies, procedures and regulations: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Privacy impact assessment and risk management: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Processes and procedures to ensure device end-of-life security and privacy: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Security Measurements

- Validation and comparison frameworks for security metrics: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Software and Hardware Security Engineering

- Security and risk analysis of components compositions: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Secure software architectures and design (security by design): Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Security design patterns: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Secure programming principles and best practices: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Refinement and verification of security management policy models: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Runtime security verification and enforcement: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Security testing and validation: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Quantitative security for assurance: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Intrusion detection and honeypots: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Model-driven security and domain-specific modelling languages: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Self- including self-healing, self-protecting, self-configuration systems: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

- Attack techniques (e.g. side channel attacks, power attacks, stealth attacks, advanced persistent attacks, rowhammer attacks): Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Cybersecurity and cyber-safety co-engineering: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Privacy by design: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Steganography, Steganalysis, and Watermarking

- Digital watermarking: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Trust Management and Accountability

- Semantics and models for security, accountability, privacy, and trust: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Identity and trust management: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Trust in securing digital as well as physical assets: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Trust in decision making algorithms: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Trust and reputation of social and mainstream media: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)
- Reputation models: Ei käsitelty lainkaan käytännössä (0 teoria + 0 käytäntö)

Taulukko 35. Tampereen yliopiston kurssien eniten käsittelemät aiheet teorian osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Asymmetric cryptography	10
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Symmetric cryptography	9
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Hash functions	9
3.1.12 Software and Hardware Security Engineering	Vulnerability discovery and penetration testing	9
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Crypto material management (e.g. key management, PKI)	8
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Digital signatures	8
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Message authentication	8
3.1.4 Education and Training	Cybersecurity-aware culture (e.g. including children education)	8
3.1.9 Network and Distributed Systems	Managerial, procedural and technical aspects of network security	8
3.1.9 Network and Distributed Systems	Network layer attacks and mitigation techniques	8
3.1.12 Software and Hardware Security Engineering	Malware analysis including adversarial learning of malware	8
3.1.14 Theoretical Foundations	Formal specification of various aspects of security (e.g properties, threat models, etc.)	8
3.1.15 Trust Management and Accountability	Trust management architectures, mechanisms and policies	8

Taulukko 36. Tampereen yliopiston kurssien eniten käsittelemät aiheet harjoitusten osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Symmetric cryptography	6
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Hash functions	6
3.1.10 Security Management and Governance	Techniques to ensure business continuity/disaster recovery	6
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Asymmetric cryptography	5
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Digital signatures	5
3.1.4 Education and Training	Cyber ranges, Capture the Flag, exercises, simulation platforms, educational/training tools, cybersecurity awareness	5
3.1.1 Assurance, Audit, and Certification	Assessment	4
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Crypto material management (e.g. key management, PKI)	4
3.1.9 Network and Distributed Systems	Protocols and frameworks for secure distributed computing	4

Taulukko 37. Tampereen yliopiston kurssien vähiten käsittelemät aiheet teorian osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.9 Network and Distributed Systems	Fault tolerant models	1
3.1.10 Security Management and Governance	Identification of the impact of hardware and software changes on the management of Information Security	1
3.1.10 Security Management and Governance	Compliance with information security and privacy policies, procedures, and regulations	1
3.1.12 Software and Hardware Security Engineering	Security and risk analysis of components compositions	1
3.1.12 Software and Hardware Security Engineering	Intrusion detection and honeypots	1
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Quantum cryptography	0
3.1.4 Education and Training	Education methodology	0
3.1.4 Education and Training	Vocational training	0
3.1.5 Human Aspects	Enhancing risk perception	0
3.1.7 Incident Handling and Digital Forensics	Coordination and information sharing in the context of cross-border/organizational incidents	0
3.1.9 Network and Distributed Systems	Secure system interconnection	0
3.1.10 Security Management and Governance	Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling)	0
3.1.12 Software and Hardware Security Engineering	Refinement and verification of security management policy models	0
3.1.12 Software and Hardware Security Engineering	Security testing and validation	0
3.1.12 Software and Hardware Security Engineering	Attack techniques (e.g. side channel attacks, power attacks, stealth attacks, advanced persistent attacks, rowhammer attacks)	0
3.1.14 Theoretical Foundations	Formal verification of security assurance	0
3.1.15 Trust Management and Accountability	Trust in securing digital as well as physical assets	0
3.1.15 Trust Management and Accountability	Trust in decision making algorithms	0

Taulukko 38. Tampereen yliopiston kurssien vähiten käsittelemät aiheet teorian osalta taksonomian mukaisesti tarkasteltuna

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.1 Assurance, Audit, and Certification	Assurance	0
3.1.1 Assurance, Audit, and Certification	Certification	0
3.1.2 Cryptology (Cryptography and Cryptanalysis)	Quantum cryptography	0
3.1.3 Data Security and Privacy	Data usage control.	0
3.1.5 Human Aspects	Forensic cyberpsychology	0
3.1.5 Human Aspects	Automating security functionality	0
3.1.5 Human Aspects	Privacy concerns, behaviours, and practices	0
3.1.5 Human Aspects	Transparent security	0
3.1.5 Human Aspects	Cybersecurity profiling	0
3.1.5 Human Aspects	Security visualization	0
3.1.5 Human Aspects	Gamification	0
3.1.5 Human Aspects	Human perception of cybersecurity	0
3.1.6 Identity Management	Privacy and identity management (e.g. privacy-preserving authentication)	0
3.1.6 Identity Management	Identity management quality assurance	0
3.1.6 Identity Management	Biometric methods, technologies and tools	0
3.1.7 Incident Handling and Digital Forensics	Incident analysis, communication, documentation, forecasting (intelligence based), response, and reporting	0
3.1.7 Incident Handling and Digital Forensics	Theories, techniques and tools for the identification, collection, attribution, acquisition, analysis and preservation of digital evidence (e.g. code authorship and attacker identification, provenance assurance, digital evidence correlation, digital evidence triage)	0
3.1.7 Incident Handling and Digital Forensics	Digital forensic processes and workflow models	0
3.1.7 Incident Handling and Digital Forensics	Policy issues related to digital forensics	0
3.1.7 Incident Handling and Digital Forensics	Resilience aspects	0
3.1.7 Incident Handling and Digital Forensics	Anti-forensics and malware analytics	0

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.7 Incident Handling and Digital Forensics	Coordination and information sharing in the context of cross-border/organizational incidents	0
3.1.8 Legal Aspects	Intellectual property rights	0
3.1.9 Network and Distributed Systems	Network security (principles, methods, protocols, algorithms and technologies)	0
3.1.9 Network and Distributed Systems	Distributed systems security	0
3.1.9 Network and Distributed Systems	Network attack propagation analysis	0
3.1.9 Network and Distributed Systems	Distributed systems security analysis and simulation	0
3.1.9 Network and Distributed Systems	Fault tolerant models	0
3.1.9 Network and Distributed Systems	Secure distributed computations	0
3.1.9 Network and Distributed Systems	Network interoperability	0
3.1.9 Network and Distributed Systems	Secure system interconnection	0
3.1.10 Security Management and Governance	Threats and vulnerabilities modelling	0
3.1.10 Security Management and Governance	Identification of the impact of hardware and software changes on the management of Information Security	0
3.1.10 Security Management and Governance	Compliance with information security and privacy policies, procedures, and regulations	0
3.1.10 Security Management and Governance	Privacy impact assessment and risk management	0
3.1.10 Security Management and Governance	Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling)	0
3.1.11 Security Measurements	Validation and comparison frameworks for security metrics	0
3.1.12 Software and Hardware Security Engineering	Security and risk analysis of components compositions	0
3.1.12 Software and Hardware Security Engineering	Secure software architectures and design (security by design)	0
3.1.12 Software and Hardware Security Engineering	Security design patterns	0

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.12 Software and Hardware Security Engineering	Secure programming principles and best practices	0
3.1.12 Software and Hardware Security Engineering	Refinement and verification of security management policy models	0
3.1.12 Software and Hardware Security Engineering	Runtime security verification and enforcement	0
3.1.12 Software and Hardware Security Engineering	Security testing and validation	0
3.1.12 Software and Hardware Security Engineering	Quantitative security for assurance	0
3.1.12 Software and Hardware Security Engineering	Intrusion detection and honeypots	0
3.1.12 Software and Hardware Security Engineering	Model-driven security and domain-specific modelling languages	0
3.1.12 Software and Hardware Security Engineering	Self-* including self-healing, self-protecting, self-configuration systems	0
3.1.12 Software and Hardware Security Engineering	Attack techniques (e.g. side channel attacks, power attacks, stealth attacks, advanced persistent attacks, rowhammer attacks)	0
3.1.12 Software and Hardware Security Engineering	Cybersecurity and cyber-safety co-engineering	0
3.1.12 Software and Hardware Security Engineering	Privacy by design	0
3.1.13 Steganography, Steganalysis and Watermarking	Digital watermarking	0
3.1.14 Theoretical Foundations	New theoretically-based techniques for the formal analysis and design of cryptographic protocols and their applications	0
3.1.14 Theoretical Foundations	Formal verification of security assurance	0
3.1.14 Theoretical Foundations	Cybersecurity concepts, definitions, ontologies, taxonomies, foundational aspects	0
3.1.15 Trust Management and Accountability	Semantics and models for security, accountability, privacy, and trust	0
3.1.15 Trust Management and Accountability	Identity and trust management	0
3.1.15 Trust Management and Accountability	Trust in securing digital as well as physical assets	0
3.1.15 Trust Management and Accountability	Trust in decision making algorithms	0

Taksonomian alue	Taksonomian aihe	Kurssien lkm
3.1.15 Trust Management and Accountability	Trust and reputation of social and mainstream media	0
3.1.15 Trust Management and Accountability	Reputation models	0
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML threat assessment (e.g. evasion, oracle, poisoning)	0
16. Artificial Intelligence (New area not included in JRC Taxonomy)	AI/ML security management	0
16. Artificial Intelligence (New area not included in JRC Taxonomy)	Human related threats for AI/ML in cybersecurity	0

4 Yhteenveto

Tässä raportissa kuvattiin Kansallisen kyberturvallisuuskoulutuksen yhteistyöverkoston rakentaminen -hankkeen työvaihe 2:ssa toteutettua selvitystä hankkeeseen osallistuvien yliopistojen kyberturvallisuusalan koulutuksien sisällöistä. Raportissa esitettiin kattava ajantasainen kuva siitä, miltä Suomen kyberturvallisuuskoulutus näyttää kokonaisuutena suhteutettuna eurooppalaiseen kyberturvallisuusroolitukseen ja avainosaamisiin sekä mitä aiheita kyberturvallisuuskoulutuksessa katetaan. Tarkastelu pohjautuu Turun yliopistossa aiemmin toteutettuun tutkimukseen ja työvaihe 2:n aikana Turun yliopistossa jatkokehitettyyn koulutuksen sisältöjen kehittämisen arviointityökaluun. Arviointityökalussa linkitettiin eurooppalainen kyberturvallisuusroolien avainosaaminen (ENISA) ja eurooppalainen kyberturvallisuustaksonomia (JRC) kursseilla käsiteltäviin aiheisiin. Arviointityökalun linkityksen mukaisesti työvaihe 2:ssa toteutettiin tietokanta ja websivusto yliopistojen kurssien tietojen syöttöä varten. Kurssien arviot ja niissä käsiteltäviksi ilmoitetut aiheet pohjautuvat kurssien vastuuopettajien syöttämään tietoon yliopistojen kyberturvallisuusalan kurssien toteutuksesta sekä teoriasisältöjen että käytännön harjoitusten näkökulmasta.

Työvaihe 2:n aikana kerättiin 82 kurssin tiedot, joista perusopintotasoisia kursseja 8, aineopintotasoisia kursseja 13 ja syventävän tasoisia kursseja 64. Suomessa eniten kyberturvallisuusalan kursseja tarjoaa kaksi yliopistoa: Turun yliopisto 27 kurssia ja Jyväskylän yliopisto 21 kurssia. Tampereen yliopisto ja Oulun yliopisto tarjoavat noin 10 kurssia. Näiden lisäksi muut yliopistot (Vaasan yliopisto, Helsingin yliopisto, Aalto-yliopisto, Lappeenrannan-Lahden teknillinen yliopisto ja Åbo Akademi tarjoavat yksittäisiä kyberturvallisuusalan kursseja. Raportoitujen

kurssien pohjalta voidaan todeta, että Suomessa kyberturvallisuuskursseja tarjotaan useissa yliopistoissa, mutta tarjonnan määrä vaihtelee yliopistokohtaisesti merkittävästi. Kurssien aikana harjoituksissa käsiteltävien aiheiden määrä on vähäisempi verrattuna teoria-aiheiden käsittelyyn. Yksi työvaihe 2:n löydös ja jatkokehityksen mahdollisuus hankkeen seuraaville vaiheille on kehittää lisää kursseihin liittyviä harjoituksia ja lisätä käytännön harjoitusten määrää kursseilla kattamaan enemmän aiheita, ja täten mahdollistaa syvällisempi käytännön harjoittelu jo opintojen aikana.

Suomen kyberturvallisuuskoulutus painottuu vahvasti kyberturvallisuusrooleja tarkasteltaessa CISO (kyberturvallisuuden suositukset ja parhaat käytännöt, kyberturvallisuuden standardit, metodologiat ja viitekehykset, kyberturvallisuus-politiikat, ja kyberturvallisuuteen liittyvät lait, säädökset ja lainsäädännöt -avainosaamisessa) ja Cyber Incident Reponder -rooleihin (erityisesti tietoverkkojen turvallisuus ja käyttöjärjestelmien turvallisuus -avainosaamisessa). Suomen kyberturvallisuuskoulutus kattaa hyvin laajan kirjon kyberturvallisuusosaamista, jonka painotus on teknisissä taidoissa. Teknistä osaamista täydennetään operatiivisilla, strategisilla ja hallinnollisilla taidoilla. Suomen kyberturvallisuus-opetuksen kyberturvallisuusroolien avainosaamisia ovat Kyberturvallisuus-suositukset ja parhaat käytännöt, Tietokoneverkkojen turvallisuus, Käyttö-järjestelmien turvallisuus, Kyberturvallisuussuositukset ja parhaat käytännöt, Kyberturvallisuusstandardit, -menetelmät ja -viitekehykset, Kyberturvallisuus-politiikat, Kyberturvallisuuteen liittyvät lait, asetukset ja säädökset, Riskienhallinnan standardit, menetelmät ja viitekehys sekä Lakisääteiset vaatimukset, suositukset ja parhaat käytännöt sekä säädösten ja lainsäädännön noudattaminen. Kaikkia näitä avainosaamisia käsitellään 500–1100 kertaa eri yliopistojen kurssien osina.

Taksonomian osalta eniten käsiteltyjä aiheita Suomen yliopistojen kyberturvallisuusopetuksessa ovat Tietosuojan ja identiteetin hallinta (esim. tietosuojaa säilyttävä tunnistautuminen), Tietojen eheys, Arviointi, Erilaisten tietoturvan osa-alueiden (esim. ominaisuudet, uhkamallit jne.) formaali määrittely, Epäsymmetrinen salaus, Kyberrikollisuuden syytteeseenpano ja lainvalvonta, Symmetrinen salaus, Luottamuksenhallinnan arkkitehtuurit, mekanismit ja politiikat, Kyberturvallisuuslainsäädännön analysointi ja suunnittelu, Haavoittuvuuksien löytäminen ja tunkeutumistestaus, Hajautusfunktiot, Käytettävyys, Auditointi, Digitaaliset allekirjoitukset ja Erilaisten tietoturvan osa-alueiden formaali määrittely ja vahvistus.

Selkeästi jokaisessa yliopistossa toistuvat tietyt samat aiheet ja kurssien käsiteltävät sisällöt. Tämä myös osoittaa, että Suomessa on hyvä yhteisymmärrys yliopistojen osalta niistä aiheista, joita kursseilla tulee käsitellä, jotta varmistetaan kyberturvallisuusalan perustaitojen rakentaminen opiskelijoille tutkinto-opintojen aikana. Suomessa yliopistojen tarjoamissa kyberturvallisuusalan kursseissa ja

niissä käsiteltävissä aiheissa on kurssitason päällekkäisyyttä, minkä osalta olisi mahdollista harkita yliopistojen välisen koulutusyhteistyön lisäämistä. Tällaisen yhteistyön haasteeksi ja esteeksi voi kuitenkin muodostua kurssien osallistujamäärien lisäksi se, että yliopistojen tutkintorakenteet ja niissä vaadittavat aiheet tulee olla tarjolla tiettynä ajankohtana tutkintorakenteen mukaisesti, ja käsiteltävien aiheiden tulee tukea opintojen edistymistä tietyssä muodossa. Tästä syystä jokaisen yliopiston on jatkossakin varmistettava kyberturvallisuustaitoihin liittyvän perusopetuksen tarjonta mahdollisen yliopistoyhteistyön lisäksi.

Suomessa on kaksi yliopistoa, jotka tarjoavat yli 20 kyberturvallisuusalan kurssia: Jyväskylän yliopisto ja Turun yliopisto. Näille yliopistoille oli mahdollista tehdä tarkempi tarkastelu kurssisisältöjen ja painopisteiden osalta. Jyväskylän yliopiston kyberturvallisuusroolien painopiste on CISO- ja Cyber Incident Responder -rooleissa. Jyväskylän yliopiston tarjoamat kurssit kattavat laajasti eri osa-alueita ja avainosaamisia, ja opetuksessa on vahva painotus strategisessa, hallinnollisessa ja operatiivisessa osaamisessa, mikä on välttämätöntä nykyisten ja tulevien kyberuhkien hallinnassa. Jyväskylän yliopisto tarjoaa 19 syventävää kurssia, 1 aineopintotasoisen ja 1 perusopintotasoisen kurssin. Turun yliopiston kyberturvallisuusroolien painopiste on myös CISO- ja Cyber Incident Responder -rooleissa. Turun yliopiston kyberturvallisuuden koulutuksessa on vahva painotus teknisessä ja operatiivisessa osaamisessa, ja tämän lisäksi strategisessa ja hallinnollisessa osaamisessa. Turun yliopisto tarjoaa 18 syventävää kurssia, 4 aineopintotasoista ja 5 perusopintotasoista kurssia. Näiden kahden yliopiston aiheiden käsittelyssä ja painopisteissä on hieman eroja; Jyväskylän yliopiston koulutus on enemmän hallinnollisiin näkökulmiin painottuva, kun taas Turun yliopisto painottaa enemmän teknisiä näkökulmia. Lisäksi Turun yliopisto tarjoaa muutamia kursseja jo alemmassa tutkinnossa mahdollistaen kyberturvallisuusaiheiden käsittelyn jo opintojen alkuvaiheessa. Suomen kyberturvallisuusopetuksessa nämä kaksi yliopistoa täydentävät kybertuvallisuuden opetuksen osaamiskenttää tuomalla opetukseen sekä teknisen että hallinnollisen painotuksen ja tämä mahdollistaa koulutussuuntausten painopisteiden rakentamisen sekä erityiskurssien tarjoamisen.

Kaksi yliopistoa, Oulun yliopisto ja Tampereen yliopisto, tarjoavat noin 10 kyberturvallisuusalan kurssia. Näiden yliopistojen osalta oli mahdollista tehdä alustavaa tarkastelua kurssisisällöistä ja painopisteistä. Oulun yliopiston painopisteet kyberturvallisuusroolien osalta ovat CISO ja Cyber Incident Responder. Samalla tavalla Tampereen yliopisto painottuu CISO- ja Cyber Incident Responder -rooleihin. Näissä yliopistoissa on vahva tekninen ja operatiivinen painotus avainosaamisen osalta. Oulun yliopisto tarjoaa 7 syventävää kurssia ja kaksi aineopintotasoista kurssia, ja Tampereen yliopisto tarjoaa 5 syventävää kurssia, 4 aineopintotasoista ja 4 perusopintotason kurssia. Kummankin yliopiston painotus on

tekninen, mutta Tampereen yliopisto tarjoaa opiskelijoille jo alemmassa tutkinnossa kyberturvallisuusalan kursseja.

Raportissa tuodaan esille myös niitä taksonomian aiheita, jotka ovat vähiten käsiteltyjä Suomen yliopistoissa. Vastausten pohjalta on nähtävissä, että useat tärkeät osa-alueet jäävät vähemmälle huomiolle kurssien aiheiden ja harjoitusten osalta. Näitä ovat esimerkiksi 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, rajat ylittävien ja organisaatioiden välisten tapausten koordinointi ja tiedonjakaminen. Lisäksi erityisesti tekoälyyn liittyvät näkökulmat, lainsäädäntö ja standardit uutena digitalisaatiota muuttavana aihealueena tulisi entistä vahvemmin rakentaa osaksi kyberturvallisuuskoulutuksen opetussuunnitelmia, koska tekoäly on yhä merkittävämpi osa kyberturvallisuutta. Koulutuksen kehitysehdotuksena suositellaan, että yliopistot lisäävät jatkossa tekoälyyn ja sen hyödyntämiseen kyberturvallisuudessa liittyvää koulutusta. Lisäksi jatkokehitysehdotuksena on lisätä 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.

Hankkeen jatkon osalta erityistä huomiota tulisi kiinnittää käytännön harjoituksiin, kuten kybertuvallisuustestaukseen ja erilaisiin hyökkäystekniikoihin, jotta opiskelijat saavat konkreettisia taitoja. Myös mahdollisia lyhytkursseja ja täydennyskoulutusta (esimerkiksi FITechin ja avointen yliopistojen kautta tarjottuna) tulisi kehittää erityisesti työelämän tarpeita vastaaviksi rakentamalla kursseille vahvaa työelämärelevanssia. Lisäksi mahdollisten ajasta ja paikasta riippumattomien kyberturvallisuusalan kurssien toteutusta kannattaa tarkastella, jotta koulutuksen tarjoaminen myös työelämässä oleville opiskelijoille mahdollistuu. Kyberturvallisuusalan kursseilla tärkeässä roolissa on yritysyhteistyö ja yrityksien kautta saatava relevanssi. Kehitysehdotuksena on kyberturvallisuusalan kurssien rakentaminen yhteistyössä alan toimijoiden ja yritysten kanssa, mm. vierailuluentojen muodossa tai erikoiskurssien järjestämisenä erilaisten teemojen kautta. Erikoiskurssien järjestämisessä on myös hyvät yhteistyömahdollisuudet yliopistojen välillä. Yhteistyö yliopistojen ja yritysten välillä voisi tehostaa koulutusta ja varmistaa, että opetuksen sisältö vastaa ajankohtaisia ja tulevaisuuden tarpeita. Yliopistoilla on myös mahdollisuus profiloitua tarkemmin tiettyjen kyberturvallisuusroolien

suuntaisesti ja tätä kautta mahdollistaa lähestymistapojen ja erikoistumiskurssien toteuttaminen.

Kansallisella tasolla kyberturvallisuusalan korkeakoulutuksen kehittämisen tueksi ja lisätarpeiden tunnistamiseksi on tässä raportissa esitetyn tutkimuksen lisäksi suoritettu yritysten osaamistarvekartoitus, josta on julkaistu oma raporttinsa (Majanoja et al., 2024). Lisäksi ohjelmistoturvallisuuden koulutuksen kehittämisestä on parhaillaan meneillään Turun yliopiston toteuttamana korkeakouluopettajien kehitystarvenäkemyksiin perustuva tutkimus, josta raportoidaan erikseen.

Lähteet

ENISA (2021). Securing Machine Learning Algorithms — ENISA. https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms (2024-10-08)

ENISA (2022). European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework (2024-10-08)

ENISA (2023). Multilayer Framework for Good Cybersecurity Practices for AI — ENISA. https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practices-for-ai (2024-10-08)

European Committee for Standardization (2019). SFS-EN 16234-1:2019. e-Competence Framework (e-CF). A common European Framework for ICT Professionals in all sectors – Part 1: Framework.

European Union Agency for Cybersecurity ECSF (2022). European cybersecurity skills framework. European Union Agency for Cybersecurity. https://data.europa.eu/doi/10.2824/859537 (2024-10-08)

Hakkala, A., Majanoja, A.-M., Leppänen, V., & Virtanen, S. (2023). Framework for the Evaluation of Cybersecurity Curriculum Educational Content. The 19th International CDIO Conference, Trondheim, Norway, June 26—29, 2023., pp. 543–554.

Majanoja, A.-M., Ekqvist, J., Hakkala A., & Virtanen, S. (2024). Kyberturvallisuuskoulutuksen 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)

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.