UNIVERSITY OF TURKU
Faculty of Technology

# Kyberturvallisuuskoulutuksen kehittäminen Suomessa: yritysten osaamistarvekartoitus

Anne-Maarit Majanoja, Jani Ekqvist, Antti Hakkala, Seppo Virtanen

**Reports from the Faculty of Technology No. 2**

**University of Turku, Finland, 2024**

UNIVERSITY
OF TURKU
Faculty of Technology

Reports from the Faculty of Technology No. 2
University of Turku, Finland, 2024

Teknillisen tiedekunnan raportteja nro 2
Turun yliopisto, 2024



ISBN 978-951-29-9920-0 (PDF)
ISSN 2984-360X (Online)

TIIVISTELMÄ

**Tekijät:** Anne-Maarit Majanoja[1,*], Jani Ekqvist[2], Antti Hakkala[1], Seppo Virtanen[1]

**Otsikko:** Kyberturvallisuuskoulutuksen kehittäminen Suomessa: yritysten osaamistarvekartoitus

**Julkaisun tiedot:** Reports from the Faculty of Technology No. 2, University of Turku, Finland, 2024, 35 pages

Tässä raportissa kuvataan Kansallisen kyberturvallisuuskoulutuksen yhteistyöverkoston rakentaminen -hankkeen aikana toteutettu yritysten osaamistarvekartoitus kyberturvallisuuskoulutuksen kehittämisestä. Hankkeeseen osallistuu yhdeksän suomalaista yliopistoa ja 14 ammattikorkeakoulua, jotka tarjoavat kyberturvallisuusalan koulutusta. Yliopistojen ja ammattikorkeakoulujen yhteisenä toteutuksena toteutettiin sidosryhmäkysely, jonka tarkoituksena oli kartoittaa yritysten ja organisaatioiden kyberturvallisuustaitoja ja -tarpeita. Kartoitus toteutettiin 28.1.2024 - 31.3.2024, ja kyselyyn vastasi 61 yrityksen tai julkishallinnon organisaation edustajaa. Kyselyä täydennettiin myös haastatteluilla, joilla saatiin syvällisempää tietoa vastaajien näkemyksistä ja tarpeista.

Kyselyn perusteella yritykset ja organisaatiot tarvitsevat monipuolista osaamista kyberturvallisuuden eri osa-alueilla. Tärkeimmät osa-alueet tällä hetkellä ovat tietoturva ja yksityisyyden suoja, koulutus ja jatkuva oppiminen, identiteetin hallinta sekä turvallisuuden hallinta ja hallintotavat. Näitä osa-alueita pidetään kriittisinä yritysten toiminnan kannalta. Lisäksi oikeudelliset näkökohdat, ohjelmisto- ja laitteistoturvallisuus sekä ihmistekijät ovat keskeisiä nykyhetken tarpeita, kun taas vähemmän tärkeinä pidettiin steganografiaa, teoreettisia perusteita ja kryptologiaa. Tulevaisuudessa tärkeimmiksi osa-alueiksi arvioidaan tietoturva ja yksityisyyden suoja, turvallisuuden hallinta ja hallintotavat, ohjelmisto- ja laitteistoturvallisuus, identiteetin hallinta sekä oikeudelliset näkökohdat. Myös tekoäly ja koneoppiminen nähdään merkittävinä osa-alueina tulevaisuudessa.

Yritykset odottavat uusilta työntekijöiltä vahvaa teoreettista perustaa sekä kykyä jatkuvaan oppimiseen ja opittujen taitojen soveltamiseen käytännössä. Pehmeät taidot, kuten ymmärrys laajasta kybertoimintaympäristöstä, resilienssiajattelu ja lainsäädännön perusteet, ovat tärkeitä. Teknisiin taitoihin kuuluvat kiristyshaitta-ohjelmien tuntemus, digitaalinen forensiikka, koodaus- ja skriptaustaidot sekä verkko-

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

osaaminen. Uusien työntekijöiden perehdytys yrityksissä vaatii laaja-alaista ja monipuolista koulutusta. Tämä sisältää ohjelmistotuotannon tuottavuuden ja käytäntöjen parantamisen, ohjelmistokehityksen tuottavuuden parantamisen, erilaiset direktiivit ja sertifioinnit, biometrisen tunnistuksen ja turvaratkaisujen haastamisen sekä toimialakohtaisten vaatimusten ymmärtämisen ja soveltamisen. Perehdytysprosessin parantamiseksi olisi hyödyllistä tarjota systemaattista sisääntuloperehdytystä, mentoreita ja säännöllisiä tarkistuspisteitä.

Korkeakoulujen roolina on tarjota sekä teoreettista että käytännön asiantuntemusta kyberturvallisuudessa. Tämä sisältää vahvan perustan hallinnollisesta tietoturva-osaamisesta, joka kattaa lait, asetukset, säädökset, direktiivit ja standardit, sekä käytännön taidot riskienhallinnassa ja teknologioiden toimintaperiaatteissa. Korkeakoulujen tulisi tarjota opiskelijoille yleiskuva kyberturvallisuusalasta, mukaan lukien teknologiat, niiden toimintaperiaatteet ja keskeiset käsitteet. Yritykset arvostavat käytännön osaamista teknologiasta tai ratkaisusta, jota voidaan soveltaa työssä heti valmistumisen jälkeen. Erityisen tärkeää on kyky ymmärtää ja käyttää verkkotekniikoita, hankkia kokemusta palomuureista, sekä verkon valvonnan ja hallinnollisen puolen tuntemusta, kuten standardien ja riskienhallinnan vaatimusten täyttämisen.

AVAINSANAT: Kyberturvallisuuskoulutus, Koulutuksen kehittäminen, Yrityskysely, Yritysten kyberturvallisuustarpeet

# Sisällys

# 1 Johdanto

Kansallisen kyberturvallisuuskoulutuksen yhteistyöverkoston rakentamisen hankkeeseen osallistuu yhdeksän suomalaista yliopistoa ja 14 ammattikorkeakoulua, joissa järjestetään kyberturvallisuusalan koulutusta. Hankkeen tehtävänä on vahvistaa korkeakoulujen kyberturvallisuusalan opetusyhteistyötä sekä vuorovaikutusta teollisuuden ja julkisen sektorin kanssa, jotta alan tutkinto-opetuksen ja jo työelämässä olevien kyberturvallisuusosaamisen kehittäminen mahdollistuu. Hankkeen rahoittajana toimii Suomen opetus- ja kulttuuriministeriö. Hankeaika on 1.1.2023-31.12.2025. Hanke toteutetaan kahtena erillisenä osahankkeena, joista toisessa ovat mukana yliopistot ja toisessa ammattikorkeakoulut.

Hankkeeseen osallistuvat yliopistot ovat:

- Jyväskylän yliopisto
- Turun yliopisto
- Tampereen yliopisto
- Vaasan yliopisto
- Lappeenrannan-Lahden teknillinen yliopisto
- Helsingin yliopisto
- Aalto-yliopisto
- Oulun yliopisto
- Åbo Akademi

Hankkeeseen osallistuvat ammattikorkeakoulut ovat:

- Jyväskylän Ammattikorkeakoulu
- Centria-ammattikorkeakoulu
- Kajaanin Ammattikorkeakoulu

- Karelia Ammattikorkeakoulu
- Lapin ammattikorkeakoulu
- Laurea-ammattikorkeakoulu
- Metropolia Ammattikorkeakoulu
- Oulun Ammattikorkeakoulu
- Poliisiammattikorkeakoulu
- Savonia-ammattikorkeakoulu
- Tampereen ammattikorkeakoulu
- Turun ammattikorkeakoulu
- Vaasan ammattikorkeakoulu
- Kaakkois-Suomen Ammattikorkeakoulu

Kummallakin osahankkeella on oma hankesuunnitelmansa. Tässä raportissa esitettävä selvitys yritysten ja organisaatioiden kyberturvallisuuden osaamistarpeista on tehty yliopisto- ja ammattikorkeakouluosahankkeiden yhteistyönä Turun yliopiston ja Turun ammattikorkeakoulun johdolla. Selvitys perustuu yrityksille ja organisaatioille tehtyyn kyselytutkimukseen, jossa vastaajia pyydettiin arvioimaan Euroopan komission yhteisen tutkimuskeskuksen (European Commission Joint Research Centre, JRC) määrittämän kyberturvallisuustaksonomian (JRC Cybersecurity Taxonomy) (Fovino et al., 2019) kautta kyberturvallisuuden eri alojen osaamistarpeitaan. Lisäksi selvitettiin erilaisten yleisten työelämätaitojen tärkeyttä kyberturvallisuusalan tehtävissä. Kysely oli avoinna 28.1.2024 - 31.3.2024, ja siihen saatiin 61 vastausta. Vastaajilla oli myös mahdollisuus ilmoittautua henkilökohtaisesti haastateltavaksi syventämään kyselyyn annettuja vastauksia. Haastatteluihin ilmoittautui 19 yritysten ja organisaatioiden edustajaa, ja 14 heistä haastateltiin touko-kesäkuun 2024 aikana.

Yliopistojen osahankkeen osalta tämä raportti on yksi työvaihe 2:een määritetyistä hankkeen tuotoksista. Ammattikorkeakoulujen osalta raportti on 2. työpaketin 1. osion määritelty tuotos. Kummassakin osahankkeessa tehdään erikseen nykyisten koulutussisältöjen kartoitukset, ja tässä raportissa esitettyjen tulosten ja kyseisten kartoitusten perusteella saadaan selville nykyisten koulutussisältöjen relevanssi yritysten ja organisaatioiden nykyiseen ja tulevaan osaamistarpeeseen, ja pystytään tunnistamaan korkeakoulujen koulutussisältöjen kehittämissuuntia työelämän osaamistarpeiden näkökulmasta.

# 2 Yrityskyselyn ja haastatteluiden toteutus, tavoitteet ja vastaajat

Yrityskysely toteutettiin Turun yliopiston hallinnoimalla Webropol-kyselyllä. Kyselyn rakenne, kysymykset ja tavoitteet määriteltiin yhteistyössä yliopistojen ja ammattikorkeakoulujen edustajien muodostamassa työryhmässä. Kyselyn rakenne määriteltiin loka-marraskuussa 2023 ja kysely työstettiin valmiiksi Webropoliin joulukuussa 2023. Kysely oli avoinna 28.1.2024-31.3.2024.

Kyselyn tavoitteena oli tarkastella kyberturvallisuuskoulutusta, siihen liittyviä tarpeita sekä erilaisten kyberturvallisuustaitojen kehittämistä suomalaisissa yrityksissä ja organisaatioissa. Tutkimuksessa keskityttiin kolmeen pääaiheeseen:

1. Kyberturvallisuusteemat ja aiheet, joissa taitoja ja koulutusta tarvitaan nyt ja tulevaisuudessa.
2. Kuinka paljon aikaa käytetään uusien kyberturvallisuusalan työntekijöiden kouluttamiseen organisaatiossa.
3. Mitä pehmeitä taitoja (eli henkilökohtaisia kykyjä, taitoja tai toimintamalleja) työntekijöiltä tarvitaan.

Lisäksi kyselyssä kerättiin yleisiä taustatietoja vastaajien edustamista organisaatioista. Kyselyn avulla kartoitetaan kyberturvallisuustaitojen nykytilanne ja tulevaisuuden tarpeet yrityksissä ja organisaatioissa. Tuloksia käytetään korkeakoulujen kyberturvallisuuskoulutuksen kehittämiseen ja parantamiseen.

Kysymyksiä oli yhteensä 17. Jos vastaaja halusi osallistua lisäksi haastatteluun, kyselyn lopussa pyydettiin yhteystiedot tulevaa yhteydenottoa varten. Kaikki tiedot käsiteltiin nimettöminä, eikä mitään tietoja luovuteta sellaisenaan kolmansille osapuolille. Osittaisia tiivistelmiä ja anonymisoituja lainauksia saatetaan julkaista osana akateemisia julkaisuja tai muita raportteja, mutta kaikki viittaukset

tunnistetietoihin poistetaan. Julkaistut tulokset sisältävät koottuja tilastollisia havaintoja, joista on mahdotonta tunnistaa yksittäisiä vastauksia.

Kyselyä jaettiin useiden erilaisten kyberalan verkostojen kautta, mm Kyberala ry, teknologiateollisuus, TurkuSec ry, Business Tampere, salausasiantuntijaverkosto, Yrityssalo, Women4Cyber Finland, NexGenHack, YritysSalo, useat kauppakamarit, muut alueelliset business-verkostot, Sote-alueiden tietohallintopäälliköt. Näiden lisäksi kysely lähetettiin suoraan yrityksille henkilökohtaisten kontaktien kautta. Kyselyn vastaajaksi toivottiin kyberalan tehtävissä toimivaa henkilöä ja vastausten määräksi yksi per yritys. Tällä pyrittiin rajaamaan pois yksittäisen yrityksen sisältä tulevien useampien vastausten mahdollinen vääristävä vaikutus tuloksiin ja niistä tehtäviin johtopäätöksiin.

Kyselyyn vastasi 61 yritystä tai organisaatiota eri puolilta Suomea. 19 vastaajaa jätti yhteystietonsa ja ilmoittautuivat halukkaiksi haastattelua varten. Näistä 14 haastattelua toteutui 10.6.2024 mennessä.

## 2.1 Kyselyn ja haastatteluiden kysymysten määrittäminen

Kyselyn (Liite 1) kahdessa ensimmäisessä kysymyksessä (kysymykset 1–4, joista 1 ja 3 varsinaiset kysymykset ja 2 sekä 4 mahdollisia tarkennuksia varten) kartoitetaan yrityksen osaamistarpeita kyberturvallisuuden eri osa-alueilla sekä nyt että tulevaisuudessa. Kyberturvallisuuden osa-alueiden määrittelyssä käytetään Euroopan Unionin komission alaisen Joint Research Centren (JRC) tekemää kyberturvallisuustaksonomiaa (Fovino et al., 2019). Taksonomian päätavoitteena on selkeyttää Euroopan Unionin tasolla kyberturvallisuuden sanastoa, määritelmiä ja sovellusalueita sekä koota nämä yhtenäiseksi kokonaisuudeksi, jota voidaan hyödyntää Unionin kyberturvallisuuskyvykkyyden arvioinnissa ja kartoittamisessa.

Taksonomia jakautuu viiteentoista päätason aihealueeseen (domain), jotka vuorostaan jakautuvat useampiin alakohtiin (Fovino et al., 2019). Näiden tarkoituksena on tarjota yksityiskohtaisempi kuvaus päätason aihealueiden sisällöstä. Taksonomiassa esitettyjen aihealueiden lisäksi kyselyyn lisättiin uusi päätaso Artificial intelligence and machine learning, jonka jälkeen kyselyssä käytetty taksonomia muodostui seuraavanlaiseksi:

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

Artificial intelligence and machine learning -aihealue ja sen alakohdat 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.

Kyselyn vastaamisen käytettävyyden parantamiseksi alakohtien määrää rajattiin yhdistämällä aihealueissa käsiteltäviä aihealueita. Tämän seurauksena kyselyssä maksimimäärä alakohtia on 4 jokaista aihealuetta kohden. Aihealueen päätason vastaaminen määriteltiin pakolliseksi, ja halutessaan kyselyn vastaaja pääsi vastaamaan tarkemmalle tasolle alakohtaisiin aiheisiin valitsemalla “Haluan vastata yksityiskohtaisempiin alateemoihin”. Kysymykset 1 ja 3 esitettiin monivalinta-kysymyksinä, jossa vastaajaa pyydettiin pohtimaan kyseisen aiheen osaamisen tarvetta ja merkitystä heidän yrityksessään sekä nyt että tulevaisuudessa (Kuva 1).

| | 1 Not needed | 2 Not important currently | 3 Important/ needed currently | 4 Not important in future | 5 Important/ needed in future | 6 I want more detailed sub-topics |
|---|---|---|---|---|---|---|
| 1 Assurance, Audit, and Certification | ☐ | ☐ | ☑ | ☐ | ☑ | ☑ |
| 1.1 Assurance | ☐ | ☐ | ☑ | ☐ | ☑ | ☐ |
| 1.2 Audit | ☐ | ☑ | ☐ | ☐ | ☑ | ☐ |
| 1.3 Assessment | ☐ | ☐ | ☑ | ☐ | ☑ | ☐ |
| 1.4 Certification | ☐ | ☑ | ☐ | ☑ | ☐ | ☐ |
| 2. Cryptology (Cryptography and Cryptanalysis) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 3 Data Security and Privacy | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 4 Education and Training | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5 Human aspects | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 6 Identity Management | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 7 Incident Handling and Digital Forensics | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 8 Legal aspects | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

**Kuva 1.** Tarpeiden kartoitus taksonomian mukaisesti – Aihe tarpeellinen nyt/tulevaisuudessa

Kysymyksessä 5 kysyttiin työntekijöiltä tarvittavia pehmeitä taitoja (soft skills), joita yritykset pitävät tärkeinä palkatessaan uusia työntekijöitä. Tämä kysymys määriteltiin Soft Skills -projektin [2] määrittämien taitojen pohjalta.

Seuraavista pehmeistä taidoista pyydettiin valitsemaan viisi tärkeintä ja asettamaan ne tärkeysjär-jestykseen:

1. Adaptability - Sopeutumiskyky
2. Accepting professional remarks - Ammattimaisten huomautusten hyväksyminen
3. Autonomy - Itsenäisyys
4. Learning to learn - Oppimaan oppiminen
5. Presentation - Esittäminen
6. Emotional Intelligence - Tunneäly
7. Self-confidence - Itsevarmuus
8. Self-reflection - Itsearviointi
9. Sense of organisation - Organisointikyky
10. Sense of responsibility - Vastuuntunto
11. Taking initiative - Aloitteellisuus
12. Ability to anticipate - Ennakoimiskyky
13. Respect of rules - Sääntöjen kunnioittaminen

14. Efficiency - Tehokkuus
15. Sense of ethics - Eettinen ajattelu
16. Conscientiousness at work - Tunnollisuus työssä
17. Communication - Viestintä
18. Leadership - Johtajuus
19. Assertiveness - Jämäkkyys
20. Team work - Tiimityöskentely

Kysymyksessä 6 kartoitettiin organisaatioon juuri palkatun kyberturvallisuuden juniorityöntekijän keskimääräistä taitotasoa. Kysymyksellä pyritään hahmottamaan mahdollista osaamiskuilua vastavalmistuneiden ja tuottavien juniorityöntekijöiden välillä. Kysymyksessä 7 kysyttiin keskimääräistä koulutuspanosta (tunteina), joka tarvitaan juuri palkatun juniorityöntekijän osaamis- ja kyvykkyystason saattamiseksi organisaation standardien ja vaatimusten mukaiseksi. Tähän käytettävistä keinoista mainittiin esimerkiksi itseopiskelu, ohjattu oppiminen ja/tai ulkoiset kurssit/sertifiointikoulutus. Kysymyksessä 8 kartoitettiin, onko organisaatiolla mahdollisuutta palkata kansainvälisiä opiskelijoita tai kansainvälisen tutkinnon suorittaneita henkilöitä. Kysymykset 9–13 kartoittivat vastaajan edustaman organisaation toimialaa, henkilöstömäärää, kyberturvallisuuden asiantuntijoiden osuutta henkilöstöstä sekä kyberturvallisuuden asiantuntijoiden rekrytointitarvetta. Kysymykset 14–17 kartoittivat vastaajan roolia organisaatiossa, halukkuutta jatkohaastatteluun sekä yleistä palautetta kyselystä.

Haastatteluiden (Liite 2) tavoitteena oli syventää sidosryhmäkyselyn kautta kerättyä aineistoa. Kysymykset määriteltiin yhteistyössä yliopistojen ja ammattikorkeakoulujen edustajien muodostamassa työryhmässä. Haastatteluiden painopiste oli kyselyn tarkentavissa kysymyksissä. Erityisesti keskityttiin tärkeimpien kyberturvallisuustaitojen valintoihin, osaamistarpeiden kysymyksiin annettuihin vastauksiin sekä siihen, miten nykyiset ja tulevaisuuden tarpeet on määritelty vastauksissa. Lisäksi haastatteluissa pyrittiin selvittämään valmistuneiden opiskelijoiden todellista osaamistasoa ja valmiuksia sekä yritysten panostuksia ja minkälaista koulutusta niissä joudutaan toteuttamaan uusien työntekijöiden tuottavuuden parantamiseksi ja yritysten tarpeita vastaaviksi. Haastattelut kartoittivat myös yritysten ja organisaatioiden edustajien käsityksiä korkeakouluista valmistuneiden tutkintojen sisällöllisistä odotuksista ja mahdollisista havaituista puutteista. Koulutuksen arvostusta tarkasteltiin muun muassa tutkintotodistusten, täydennyskoulutuksen ja sertifiointikoulutuksen arvostuksen osalta.

## 2.2 Kyselyyn vastanneet organisaatiot

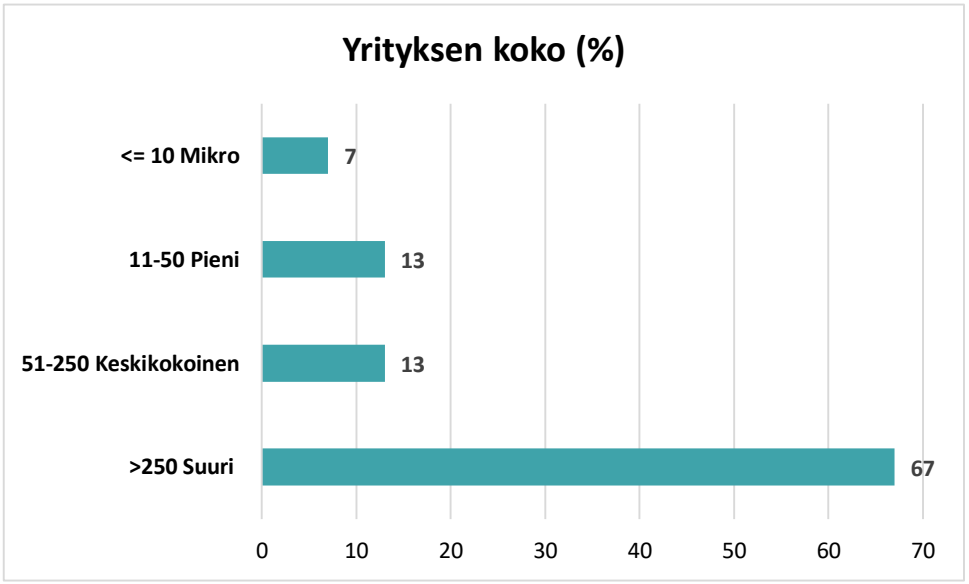
Kyselyyn vastanneet henkilöt edustivat sekä yksityisiä yrityksiä että julkishallinnon organisaatioita. Kyselyyn vastanneista n. 50 % toimi alalla Telekommunikaatio, tietokoneohjelmointi, konsultointi, laskentainfrastruktuuri ja muut tietopalvelut (Taulukko 1). Tämä osoittaa, että kyselyyn vastanneet olivat vahvasti IT-alalla toimivia yrityksiä tai isoja konsulttitaloja.

**Taulukko 1.** Kyselyyn vastanneiden toimialaluokitus

| Toimialaluokitus | Lkm | Prosenttiosuus |
|---|---|---|
| Telekommunikaatio, tietokoneohjelmointi, konsultointi, laskentainfrastruktuuri ja muut tietopalvelut | 31 | 50,80 % |
| Koulutus | 10 | 16,40 % |
| Ammatillinen, tieteellinen ja tekninen | 9 | 14,80 % |
| Julkishallinto ja maanpuolustus; pakollinen sosiaaliturva | 9 | 14,80 % |
| Muut palvelut | 8 | 13,10 % |
| Hallinto- ja tukipalvelut | 6 | 9,80 % |
| Teollisuus | 6 | 9,80 % |
| Tukkukauppa ja vähittäiskauppa | 3 | 4,90 % |
| Rahoitus ja vakuutus | 3 | 4,90 % |
| Sähkön, kaasun, höyryn ja ilmastoinnin jakelu | 3 | 4,90 % |
| Terveys- ja sosiaalipalvelut | 2 | 3,30 % |
| Kiinteistöala | 1 | 1,60 % |
| Kuljetus ja varastointi | 1 | 1,60 % |
| Rakentaminen | 1 | 1,60 % |
| Kaivostoiminta ja louhinta | 1 | 1,60 % |
| Taide, urheilu ja virkistys | 1 | 1,60 % |
| Vesihuolto; viemäröinti, jätehuolto ja kunnostus | 1 | 1,60 % |

Kyselyn pohjalta on mahdollista tulkita, että puolet vastaajien edustamista organisaatioista toimii myös konsultointitehtävissä: n. 52 % vastanneista yrityksistä tarjosi kyberturvallisuuspalveluita muille yrityksille. Kolme toimialaluokkaa jäi kokonaan ilman vastaajia: Maatalous, metsätalous ja kalastus, Majoitus- ja ravitsemistoiminta, sekä Kustannus-, lähetys- ja sisällöntuotanto ja jakelu. Kysely

tavoitti vastausten osalta erityisesti isot yritykset ja organisaatiot (Kuva 2). Kyselyyn vastanneista n. 67 % edusti yli 250 henkilöä työllistäviä yrityksiä tai organisaatioita. Hyvin pieniä tai yhden hengen yrityksiä oli vain muutama, n. 6 % vastanneista. Pienten ja keskikokoisten yritysten edustajien osuus oli yhteensä 26 % vastanneista.




**Kuva 2.** Kyselyyn vastanneiden yrityskoko

Kyselyyn vastanneiden henkilöiden roolit yrityksissä tai organisaatioissa on koottu Taulukkoon 2. Vastauksista voidaan havaita se, että kaikki vastaajat olivat vahvasti kyberturvallisuusalan tehtävissä toimivia ja täten omaavat näkemystä, kokemusta ja tarpeita liittyen kyberturvallisuusalan tarpeisiin ja opetuksen kehittämiseen.

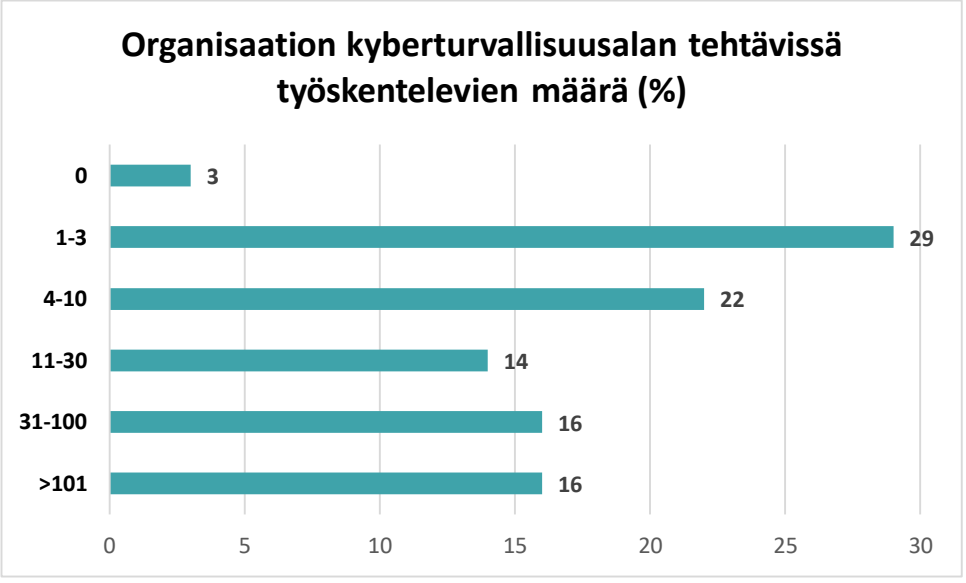
Suuri osa vastaajista on ilmoittamansa roolin perusteella myös mukana vaikuttamassa organisaationsa päätöksiin kyberturvallisuuteen liittyvissä asioissa. Omaa roolia organisaatiossa kuvailtaessa (Kuva 3) oli mahdollista vastata useampaan kuin yhteen vaihtoehtoon. Yli puolet vastaajista (51 %) ilmoitti työskentelevänsä organisaation sisäisen kyberturvallisuuden parissa ja lähes puolet (41 %) kertoi työskentelevänsä asiakkaille tarjottavien tuotteiden turvallisuuden parissa. Suoraan palveluita asiakkaille tarjosi 32 % vastaajista, ja muiden vastausten osuudesta (17 %) löytyvät mm. toimitusjohtajan tai yrittäjän roolit.

**Taulukko 2.** Kyselyyn vastanneiden rooli yrityksessä

| Vastaajan rooli yrityksessä | Lukumäärä |
|---|---|
| Asiantuntija/Specialist/Consultant/Project Manager | 12 |
| Director/ICT-päällikkö/IT Manager/Team Manager/Service Manager | 11 |
| CISO (Chief Information Security Officer) / CTO (Chief Technology Officer) | 11 |
| Head of IT/Cyber Security/Information Security Manager/Chief Information Officer | 7 |
| CEO (Chief Executive Officer) | 6 |
| Security and Cryptography Architect/Cyber Security Analyst | 3 |
| Researcher | 3 |
| Principal/Lead Engineer in Cybersecurity | 2 |
| Associate, Board Member | 2 |
| COO (Chief Operations Officer) | 1 |
| CDO (Chief Development Officer) | 1 |


**Kuva 3.** Vastaajien luonnehdinta omasta roolistaan organisaation sisällä. Vastaajan oli mahdollista vastata useampaan vaihtoehtoon.

Kysyttäessä montako kyberturvallisuuden ammattilaista yrityksessä/ organisaatiossa parhaillaan työskentelee, tulee esille enemmän hajaantumista (Kuva 4). Vaikka yrityksen/organisaation koon mukaan isoja yli 250 hengen toimijoita on 67 %, erityisesti kyberturvallisuusalan tehtävissä olevien määrä on huomattavasti alhaisempi.




**Kuva 4.** Yrityksen/organisaation kyberturvallisuusalan tehtävissä työskentelevien määrä

# 3 Tulokset

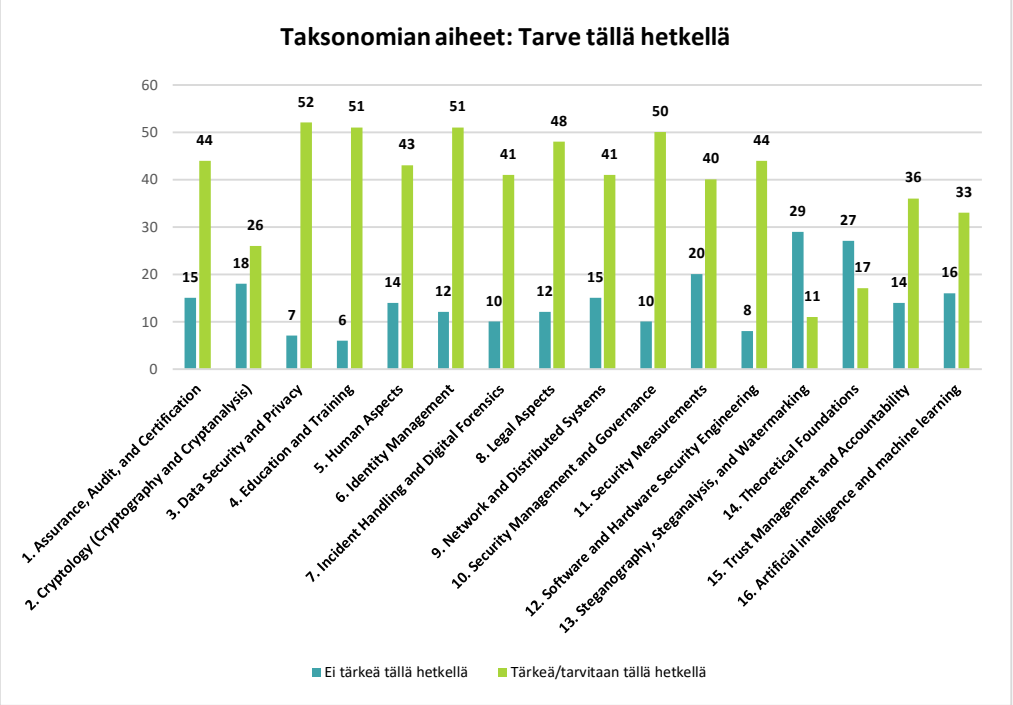
Tässä luvussa käsitellään kyselyn (61 yrityksen vastaukset) ja haastatteluiden (14 haastattelua) tuloksia, sekä näiden analyyseja. Kyselyn ja haastatteluiden tulosten pohjalta tunnistetaan yritysten tarvitsemia kyberturvallisuustaitoja ja -osaamisia.

## 3.1 Yritysten ja organisaatioiden osaamistarpeet

Kyselyn päätavoitteena oli kartoittaa yritysten osaamistarpeita kyberturvallisuuden eri osa-alueilla. Tarvekartoitus toteutettiin eurooppalaisen JRC:n kyberturvallisuustaksonomian mukaisesti. Kyseessä oli monivalintakysely, jossa vastaaja voi valita useamman kohdan arvoilla: Ei tarvetta (nyt eikä tulevaisuudessa), ei tärkeä tällä hetkellä, tärkeä tällä hetkellä, ei tärkeä tulevaisuudessa, tärkeä tulevaisuudessa. Tästä syystä eräät vastaajista ovat saattaneet valita vain esimerkiksi vaihtoehdon Ei tarvetta tai jos ei ole osannut arvioida tulevaisuuden tarvetta, on vastannut vain tämänhetkisen tarvenäkymän pohjalta. Haastatteluiden perusteella taksonomian mukainen jaottelu ja aiheet on koettu relevanteiksi työnantajan tarpeiden kannalta.

### 3.1.1 Tärkeät ja tarvittavat osa-alueet tällä hetkellä

Nykyhetken tarpeissa korostuvat Data Security and Privacy, Education and Training (tässä osiossa erityisesti kyberturvallisuustaitojen perusosaamisen tarve), Identity Management, Security management ja Governance (Kuva 5).




**Kuva 5.** Tämänhetkiset kyberturvallisuuden osaamistarpeet yritysten näkökulmasta

1. Data Security and Privacy: 52 vastaajaa piti tätä tärkeänä. Tämä osoittaa, että tietoturva ja yksityisyyden suoja ovat ensisijaisia huolenaiheita nykyhetkellä.
2. Education and Training: 51 vastaajaa piti tätä tärkeänä, mikä korostaa koulutuksen ja jatkuvan oppimisen merkitystä tietoturvassa.
3. Identity Management: 51 vastaajaa piti tätä tärkeänä, mikä viittaa identiteetin hallinnan keskeiseen rooliin nykyisessä digitaalisessa ympäristössä.
4. Security Management and Governance: 50 vastaajaa arvioi tämän tärkeäksi, mikä osoittaa, että turvallisuuden hallinta ja hallintotavat ovat keskeisiä vaatimuksia nykyhetkellä.

5. Legal Aspects: 48 vastaajaa piti tätä tärkeänä, mikä korostaa oikeudellisten näkökohtien merkitystä tietoturvassa.
6. Assurance, Audit, and Certification: 44 vastaajaa piti tätä tärkeänä, mikä korostaa vahvasti luotettavuuden ja laadun varmistamisen tarvetta.
7. Software and Hardware Security Engineering: 44 vastaajaa piti tätä tärkeänä, mikä viittaa tarpeeseen varmistaa ohjelmisto- ja laitteistoturvallisuus.
8. Human Aspects: 43 vastaajaa piti tätä tärkeänä, mikä viittaa ihmistekijöiden merkitykseen tietoturvassa.
9. Incident Handling and Digital Forensics: 41 vastaajaa arvioi tämän tärkeäksi, mikä osoittaa tarpeen kyvylle käsitellä tietoturvaloukkauksia ja suorittaa digitaalista forensiikkaa.
10. Network and Distributed Systems: 41 vastaajaa arvioi tämän tärkeäksi, mikä osoittaa verkko- ja hajautettujen järjestelmien tärkeyden.

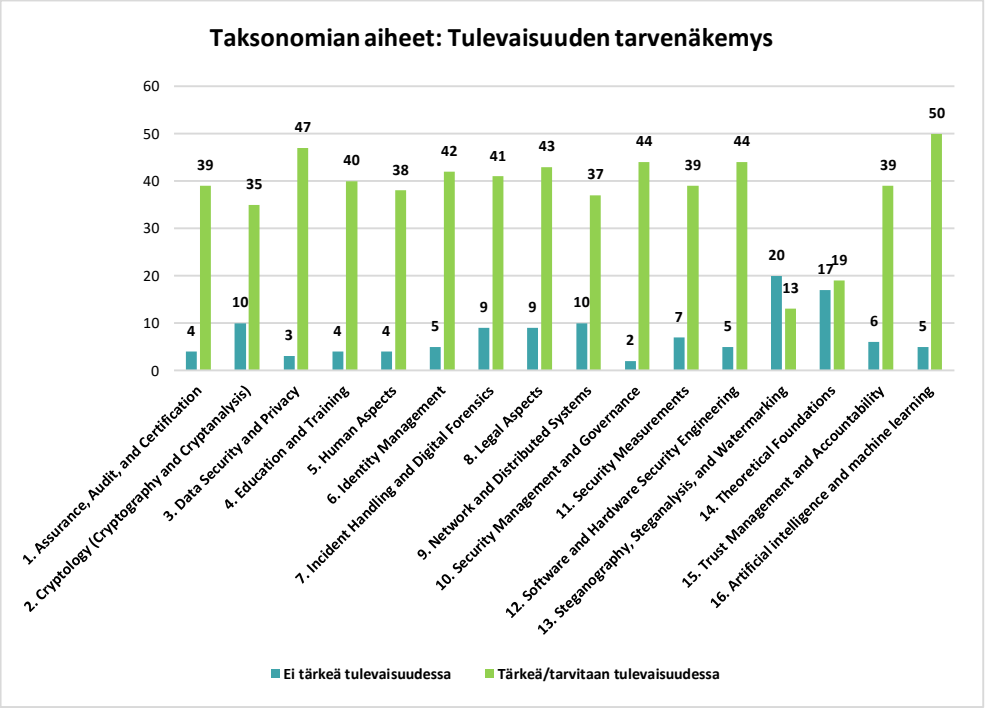
**Vähemmän tärkeät osa-alueet tällä hetkellä:**

1. Steganography, Steganalysis, and Watermarking: 29 vastaajaa ei pitänyt tätä tärkeänä, mikä viittaa siihen, että tämä osa-alue ei ole yhtä kriittinen nykyhetkellä. Kyseessä on erikoistumisaihealue, ja tästä syystä se ei ole kaikille yrityksille fokusalue.
2. Theoretical Foundations: 27 vastaajaa ei pitänyt tätä tärkeänä, mikä viittaa siihen, että teoreettiset perustat eivät ole ensisijainen huolenaihe. Kuitenkin samanaikaisesti haastatteluissa nostettiin esille, että kyberturvallisuuden perusasioiden hallinta on kriittistä, joten tässä vastaus on tulkittava siten, että teoreettiset perustat eivät ole kriittistä yrityksen toiminnan mahdollistamiseksi, mutta työntekijöille ja kyberturvallisuuden parissa työskenteleville kyberturvallisuuden perustan ymmärtäminen on kriittistä onnistumisen kannalta. Tämän kaltainen kyberturvallisuuden perusta hankintaan joko tutkintokoulutuksessa tai jatkuvan oppimisen koulutuksen kautta.
3. Cryptology (Cryptography and Cryptanalysis): 18 vastaajaa ei pitänyt tätä tärkeänä, mikä voi viitata siihen, että kryptologian tärkeys voi olla vähentynyt muiden prioriteettien rinnalla. Kryptologia on erikoistumisaihealue, ja tästä syystä sen edistyneet tutkimis- ja kehittämistaidot eivät ole monenkaan yrityksen fokusalue.

4. Artificial Intelligence and Machine Learning: 16 vastaajaa ei pitänyt tätä tärkeänä, mikä saattaa viitata siihen, että tällä hetkellä AI ja koneoppiminen eivät ole vielä yhtä keskeisiä kuin muut tietoturva-alueet.
5. Network and Distributed Systems: 15 vastaajaa ei pitänyt tätä tärkeänä, mikä osoittaa, että verkko- ja hajautettujen järjestelmien tärkeys voi olla vähentynyt.
6. Assurance, Audit, and Certification: 15 vastaajaa ei pitänyt tätä tärkeänä, mikä saattaa viitata siihen, että tämä osa-alue ei ole yhtä kriittinen kuin muut osa-alueet.

### 3.1.2 Tärkeät ja tarvittavat osa-alueet tulevaisuudessa

Tulevaisuuden tarpeita kartoitettaessa havaittiin, että suurin osa taksonomian osa-alueista nähtiin tasaisen tärkeinä. Tekoäly ja koneoppiminen nähtiin tärkeimpänä ja steganografia sekä teoreettiset perustat vähiten tärkeinä (Kuva 6).




**Kuva 6.** Tämänhetkiset kyberturvallisuuden osaamistarpeet yritysten näkökulmasta

1. Assurance, Audit, and Certification: 39 vastaajaa piti aihetta tärkeänä tulevaisuudessa. Tämä korostaa vahvasti tarvetta luotettavuuden ja laadun varmistamiselle.
2. Data Security and Privacy: Tämä osa-alue sai toiseksi korkeimman arvion tärkeänä pidettyjen osalta (47 vastaajaa). Se osoittaa, että tietoturva ja yksityisyyden suoja ovat ensisijaisia huolenaiheita tulevaisuudessa.
3. Security Management and Governance: 44 vastaajaa arvioi tämän tärkeäksi, mikä osoittaa, että turvallisuuden hallinta ja hallintotavat ovat keskeisiä tulevaisuuden vaatimuksia.
4. Software and Hardware Security Engineering: 44 vastaajaa pitää tätä tärkeänä, mikä viittaa tarpeeseen varmistaa ohjelmisto- ja laitteistoturvallisuus.
5. Identity Management: 42 vastaajaa korostaa identiteetin hallinnan tärkeyttä digitaalimaailmassa.
6. Legal Aspects: 43 vastaajaa pitää tätä tärkeänä, mikä korostaa oikeudellisten näkökohtien merkitystä ja niiden ymmärtämistä tietoturvassa.
7. Incident Handling and Digital Forensics: 41 vastaajaa arvioi tämän tärkeäksi, mikä osoittaa tarpeen kyvylle käsitellä tietoturvaloukkauksia ja suorittaa digitaalista forensiikkaa.
8. Education and Training: 40 vastaajaa piti tätä tärkeänä, mikä korostaa koulutuksen ja jatkuvan oppimisen merkitystä tietoturvassa.
9. Human Aspects: 38 vastaajaa piti tätä tärkeänä, mikä viittaa siihen, että ihmistekijät ovat merkittävä osa tietoturvaa.
10. Artificial Intelligence and Machine Learning: Tämä sai korkeimman arvion tärkeänä pidettyjen osalta (50 vastaajaa), mikä korostaa AI:n ja koneoppimisen kasvavaa roolia tietoturvassa. Tällä osaamisalueella oli merkittävä nousu verrattuna nykyhetken tarpeeseen.

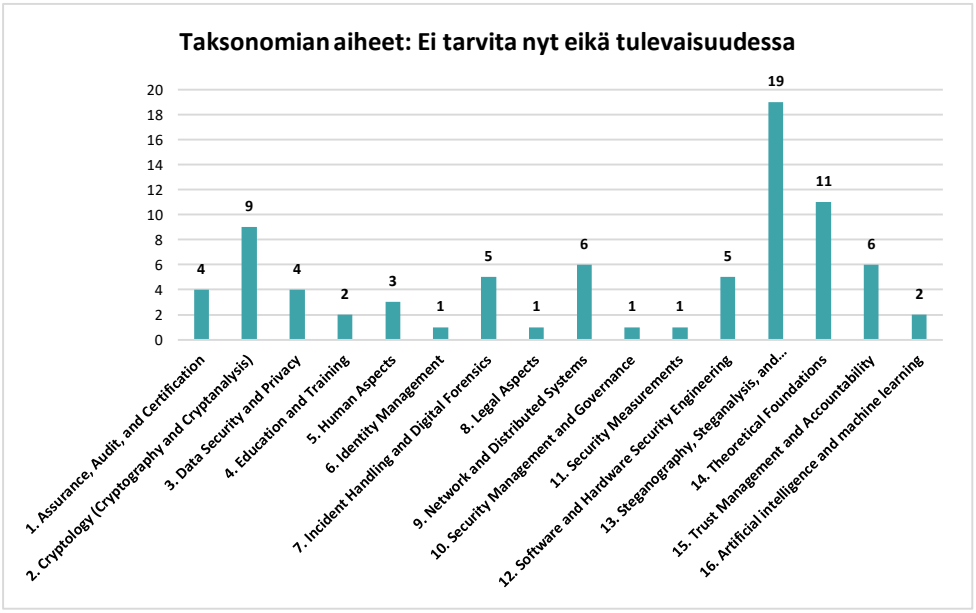
**Vähemmän tärkeät osa-alueet tulevaisuudessa:**

1. Steganography, Steganalysis, and Watermarking: 20 vastaajaa piti ei pitänyt tätä tärkeänä, mikä viittaa siihen, että tämä osa-alue ei ole yhtä kriittinen tulevaisuudessa. Kyseessä on erikoistumisaihealue, ja tästä syystä se ei ole kaikille yrityksille fokusalue.

2. Theoretical Foundations: 17 vastaajaa ei pitänyt tätä erityisen tärkeänä yrityksen toiminnan kannalta. Työntekijöiltä kuitenkin vaaditaan kyberturvallisuuden ymmärtämystä ja perustaitojen osaamista.
3. Cryptology (Cryptography and Cryptanalysis): 10 vastaajaa ei pitänyt tätä tärkeänä, mikä voi viitata siihen, että kryptologian tärkeys voi vähentyä muiden prioriteettien rinnalla. Kryptologia on erikoistumisaihealue, ja tästä syystä sen edistyneet tutkimis- ja kehittämistaidot eivät ole monenkaan yrityksen fokusalue.
4. Network and Distributed Systems: 10 vastaajaa ei pitänyt tätä tärkeänä, mikä viittaa siihen, että verkko- ja hajautettujen järjestelmien tärkeys voi vähentyä.

### 3.1.3 Osa-alueita, joita ei koettu tarpeellisiksi

Muutama vastaaja valitsi myös kohdan ei tarvita nyt eikä tulevaisuudessa. Myös nämä vastaukset vahvistavat aiempia löydöksiä nykytilanteesta ja tulevaisuuden tarpeista (Kuva 7). Näissä vastauksissa korostuvat myös tiettyjen erityisalojen fokusoitumisaiheet, jotka eivät ole kaikille yrityksille tarpeellisia. Lisäksi kyberturvallisuuden teoreettinen osaaminen ei ole yrityksen toiminnan kannalta tärkeää, mutta tärkeys tulee esille yksilön (työntekijöiden osaamisen) kautta.




**Kuva 7.** Osa-alueet, joita ei nähty tärkeinä nyt tai tulevaisuudessa

- Steganography, Steganalysis, and Watermarking: 19
    - Tämä osa-alue on selkeästi vähiten tärkeä suurimmalle osasta vastaajia, koska suurin osa vastaajista (19) pitää sitä tarpeettomana nyt ja tulevaisuudessa.
- Theoretical Foundations: 11
    - Teoreettiset perustat eivät ole ensisijainen huolenaihe, sillä merkittävä määrä vastaajia (11) pitää niitä vähemmän tärkeänä.
- Cryptology (Cryptography and Cryptanalysis): 9
    - Kryptologian erityisosaamista pidetään yleisesti ottaen vähemmän tärkeänä (9 vastaajaa).
- Network and Distributed Systems: 6
    - Verkko- ja hajautettujen järjestelmien merkitys on vähentynyt, koska 6 vastaajaa ei pidä niitä tarpeellisina.
- Trust Management and Accountability: 6
    - Luottamuksen hallintaa ja vastuullisuutta ei pidetty keskeisenä 6 vastaajan osalta.

Näiden lisäksi muutama vastasi, että seuraavia ei tarvita nyt eikä tulevaisuudessa:

Incident Handling and Digital Forensics: 5 vastaajaa, Software and Hardware Security Engineering: 5 vastaajaa, Assurance, Audit, and Certification: 4 vastaajaa, Data Security and Privacy: 4 vastaajaa, Human Aspects: 3 vastaajaa, Artificial Intelligence and Machine Learning: 2 vastaajaa, Education and Training: 2 vastaajaa, Identity Management: 1 vastaaja, Legal Aspects: 1 vastaaja, Security Management and Governance: 1 vastaaja ja Security Measurements: 1 vastaaja.

### 3.1.4 Yhteenveto kyselyssä tunnistetuista tarpeista

Analyysi osoittaa, että merkittävä osa vastaajista pitää steganografiaa, teoreettisia perusteita ja kryptologiaa vähiten tarpeellisina työntekijöidensä taitoina nyt ja tulevaisuudessa. Osa-alueet, kuten verkko- ja hajautetut järjestelmät sekä luottamuksen hallinta ja vastuullisuus, nähdään myös vähemmän tärkeinä. Tietoturva ja yksityisyyden suoja, koulutus ja jatkuva oppiminen, identiteetin hallinta, turvallisuuden hallinta ja hallintotavat sekä ohjelmisto- ja laitteistoturvallisuus sekä oikeudelliset näkökulmat ovat kriittisiä osa-alueita, jotka ovat keskeisiä tarvittavia osaamisia sekä nyt että tulevaisuudessa. Tulevaisuudessa tietoturvaan ja yksityisyyden suojaan liittyvät osa-alueet ovat tärkeitä sisältäen myös turvallisuuden

hallinnan, ohjelmisto- ja laitteistoturvallisuuden, identiteetin hallinnan sekä oikeudelliset näkökohdat. Erityisesti AI/ML:n kautta tuleva vaikutus on koettu merkittäväksi tarpeeksi tulevaisuudessa ja se tulee vaikuttamaan merkittävällä tavalla kyberturvallisuuden ratkaisuihin. Vähemmän tärkeinä pidetyt osa-alueet ovat erikoistumisaihealueita, jotka ovat tärkeitä niiden parissa toimiville yrityksille, mutta ei laajemmalle yrityskentälle.

Avoimen kentän vastauksissa vastaajat näkevät, että vaikka monet osa-alueet ovat jo nyt tärkeitä, niiden merkitys tulee kasvamaan entisestään tulevaisuudessa. Erityisesti tekoälyn ja kryptologian alalla odotetaan suuria muutoksia ja nopeaa kehitystä, mitkä vaikuttavat organisaatioiden osaamistarpeisiin ja koulutukseen. Kyselyn avoimen kentän vastausten pohjalta on havaittavissa, että vastaajat nostivat tärkeimmiksi osaamistarpeiksi ja kehityskohteiksi seuraavia:

- Kryptologia ja sen osaaminen: Vaikka moni vastaaja ilmaisi monivalinnoissa, että kryptologia ei ole organisaation osaamistarpeissa tärkeä, on vastaajissa myös organisaatioita, joille kryptologian erikoisosaaminen on kriittistä. Tämä ilmaistiin sanallisissa vastauksissa erityisesti salauksen ja salauksenpurun osalta. Kvanttisalaus nähdään tärkeänä tulevaisuudessa, ja osaamistarpeet jakautuvat neljään rooliin: arkkitehdit, kryptototeuttajat, salauskirjastoja käyttävät insinöörit sekä salauslaitteita käyttävät henkilöt.
- Inhimilliset ja lainopilliset näkökulmat: Tietoturvaan liittyvien inhimillisten tekijöiden ymmärtäminen ja kyberpsykologian huomiointi koulutuksessa ovat tärkeitä. Myös kyberlainsäädännön asiantuntijoille on kasvava tarve.
- Tietoturvan hallinta ja auditointi: Auditoinnin ja käytännön tarkastusten merkitystä korostetaan. Uudet säädökset, kuten NIS2 ja DORA, tuovat lisävaatimuksia organisaatioille, jotka tarvitsevat varmistusta ja sertifiointeja tietoturvastandardien noudattamisesta.
- Tekninen osaaminen ja käytännön taidot: Käytännön teknisten taitojen merkitys on suuri, erityisesti operatiivisessa tietoturvassa. Tämä kattaa verkkojen ja palvelimien suojauksen, laitteiden suunnittelun turvallisiksi ja erilaisten teknologisten ratkaisujen käytön ja opastuksen.
- Tietosuojan ja yksityisyyden hallinta: Tietosuoja ja yksityisyyden suojelu ovat tärkeitä erityisesti GDPR ja mobiililaitteiden lisääntyneen käytön myötä. Identiteetinhallinta ja sensitiivisen tiedon suojaaminen ovat myös korostettuja osa-alueita.
- AI ja sen tulevaisuus: Vaikka tekoäly ei ole vielä laajalti käytössä kyberturvallisuudessa, sen merkitys kasvaa tulevaisuudessa. Generatiivisten tekoälytuotteiden kysyntä on kasvussa, ja tekoälyn sääntöjen ymmärtäminen tulee olemaan tärkeä taito.

### 3.1.5 Avoimen kentän vastauksissa haasteiksi ja kehitystarpeiksi nostettuja aiheita

- Monialaisuus ja koulutus: Monialaisen koulutuksen merkitystä korostettiin, erityisesti teknisen tietämyksen yhdistämistä käyttäytymispsykologiaan ja inhimillisiin tekijöihin. Koulutustarpeiden monipuolisuus nähdään tärkeänä.
- Lainsäädäntö ja sääntely: Kyberlainsäädännön jatkuva kehittyminen vaatii organisaatioilta jatkuvaa päivitystä ja asiantuntemusta. Kommentit uusien säädösten vaikutukset tuotteisiin ja prosesseihin korostuvat.
- Osaamisen ulkoistaminen: Monet organisaatiot ulkoistavat tietoturvaan liittyviä palveluita ja koulutuksia. Tämä asettaa vaatimuksia palveluntarjoajien valmiuksille ja kyvykkyydelle tarjota tarvittavaa osaamista.
- Ekosysteemin ja yhteistyön merkitys: Organisaatioiden välinen yhteistyö ja ekosysteemit ovat tärkeitä osaamisen kehittämisessä. Tämä koskee erityisesti teknologiatoimittajia ja liikekumppaneita.
- Sosiaalipsykologian ja humanististen aineiden integrointi: Turvallisuuden huomioiminen laajemmasta näkökulmasta, mukaan lukien sosiaalipsykologia ja humanistiset tieteet, nähdään puutteellisena. Tämän integrointi koulutukseen voisi parantaa tietoturvan kokonaisvaltaista ymmärrystä, esimerkkinä kyberpsykologia.

Avoimen kentän vastauksissa nousi esille, että kyberturvallisuusalan tarpeet ovat moninaiset ja kattavat laajasti teknisiä, lainsäädännöllisiä ja inhimillisiä näkökulmia. Sertifiointi, auditointi ja kryptografia nousevat esiin kriittisinä osa-alueina, joilla on kasvava tarve erityisosaajille. GDPR ja muun lainsäädännön vaikutukset korostavat datan käsittelyn ja yksityisyyden suojan merkitystä. Lisäksi inhimilliset aspektit ja monialainen koulutus ovat tärkeitä, jotta voidaan ymmärtää ja hallita tietoturvariskejä tehokkaasti. Näiden tarpeiden täyttäminen vaatii jatkuvaa koulutusta ja päivitystä sekä teknisen että lainsäädännöllisen osaamisen osalta. Seuraavat asiat ja aiheet nousivat esille haastatteluissa erityisinä nostoina tai tarpeina:

1. Sertifiointi, auditointi ja varmennus:
    - NIS2-direktiivin myötä sertifiointien ja auditointitulosten merkitys korostuu.
    - Tarvitaan henkilöitä, jotka osaavat tulkita sertifiointi- ja tarkastuskriteerejä sekä soveltaa niitä yrityksen toimintaan.
    - Tekniset henkilöt, jotka voivat kerätä todisteita organisaation vaatimustenmukaisuudesta, ovat tärkeitä.

2. Kryptografia:
    - Kvanttiturvallinen (post-quantum) kryptografia nousee merkittäväksi vuoteen 2030 mennessä, ja algoritmimuutokset alkavat vuonna 2025.
    - Tarvitaan asiantuntijoita, jotka ymmärtävät uudet algoritmit ja voivat päivittää vanhat järjestelmät käyttämään uusia algoritmeja.
    - Aihealueen eri roolit huomioitava: uusien algoritmien oikeellisesta toteutuksesta vastaavat ja varmistavat henkilöt, sekä sähköisten allekirjoitusten asiantuntijat.
3. Tietoturva ja yksityisyys:
    - GDPR:n vaikutukset näkyvät erityisesti datan käsittelyssä ja suostumusten hallinnassa.
    - Tarvitaan osaajia, jotka ymmärtävät lainsäädännön toimintamallit ja voivat soveltaa niitä käytäntöön.
    - Kaksi korostuvaa roolia:
        - Datan käsittelyn toteuttajat (esim. liiketoiminnallinen etu, asiakkuuden hoito).
        - Konsultit/auditoijat, jotka löytävät riskikohdat ja ohjaavat soveltamisessa.
4. Koulutus ja kouluttaminen:
    - Kyberturvallisuutta lisäävien tuotteiden ja toimintatapojen tunnistaminen ja todellisen turvallisuuden parantaminen ovat keskeisiä.
5. Inhimilliset aspektit:
    - Ihmisten käyttäytyminen ja psykologia tietoturvassa ovat kriittisiä tekijöitä.
    - Tarvitaan parempaa ja kattavampaa ymmärrystä siitä, miten ihmiset vaikuttavat tietoturvaan ja rikosten onnistumiseen.
6. Lainsäädäntö ja sääntely:
    - Kyberturvallisuuslainsäädännön uudistukset ja tulevien päivitys-tarpeiden arviointi korostuvat.
    - Lainsäädäntöön perehtyneitä asiantuntijoita tarvitaan yhä enemmän.
7. Monialainen koulutus:
    - Koulutuksen monialaisuus, joka yhdistää teknistä ja inhimillistä näkökulmaa, on tärkeää.
    - Erityisesti digitaalisen forensiikan osaajia tarvitaan kyberrikos-torjunnassa.

## 3.2 Rekrytointiodotukset ja -tarpeet

Avointen vastausten perusteella uusien työntekijöiden osaamistaso kyberturvallisuusalan tehtävissä vaihtelee, mutta heiltä odotetaan vahvaa teoreettista perustaa, valmiutta jatkuvaan oppimiseen ja kykyä soveltaa opittuja taitoja käytännössä. Pehmeät taidot ja tekninen osaaminen ovat yhtä tärkeitä, ja organisaatioiden tuki ja koulutus ovat keskeisiä heidän kehitykselleen.

**Teoreettinen perusta ja käytännön kokemus**: Uusilla työntekijöillä on yleensä hyvä teoreettinen perusta kyberturvallisuuden peruskäsitteissä, mutta heiltä puuttuu käytännön kokemus näiden käsitteiden soveltamisesta. Heidän kykyään oppia ja soveltaa uusia taitoja arvioidaan usein tärkeämmäksi kuin valmiiksi korkeaa osaamistasoa.

**Pehmeät taidot**: Pehmeät taidot, kuten ymmärrys laajasta kybertoimintaympäristöstä, resilienssiajattelu, kyberympäristön lainsäädännön perusteet ja viranomaiskentän tunnistaminen, ovat erittäin tärkeitä. Uusien työntekijöiden tulee pystyä ymmärtämään monimutkaisia uhkakenttiä ja strategisia asiakirjoja.

**Tekniset taidot**: Teknisiin taitoihin ja näiden taitojen osaamisodotuksiin kuuluvat kiristyshaittaohjelmien tuntemus, digitaalinen forensiikka (esim. haittaohjelma-analyysi, tietoliikenneanalyysi) ja digitaalisen forensiikan työkalujen hallinta. Koodaus- ja skriptaustaidot, verkko-osaaminen sekä kiinnostus järjestelmien toimintaan ovat myös tärkeitä.

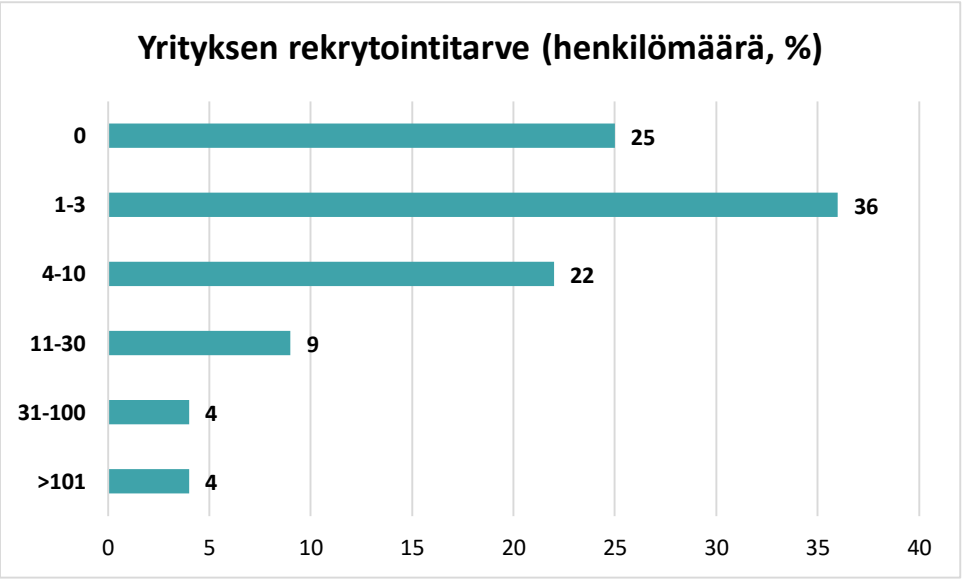
**Koulutus ja työympäristö**: Yliopisto- tai ammattikorkeakoulututkinto on usein lähtövaatimus, ja käytännön kokemus tietoturvan osa-alueilta katsotaan eduksi. Yritykset kouluttavat usein uusia työntekijöitä perusasioista alkaen, mikä voi kestää jopa kaksi vuotta. Alkuvaiheessa työntekijät sijoittuvat usein SOC (Security Operations Center) -tehtäviin, joissa he voivat oppia tarvittavat työkalut ja teknologiat.

**Haasteet ja kehitystarpeet**: Junioreilla on usein kapea perspektiivi ja korkea itsetunto, mikä voi vaikeuttaa juurisyiden löytämistä ja monimutkaisten ongelmien käsittelyä. Organisaatioiden tulee tukea heidän oppimistaan ja kehitystään. Monet yritykset eivät tällä hetkellä palkkaa junioritason kyberturvallisuusasiantuntijoita, koska heiltä puuttuu vaadittu kokemus, ja he keskittyvät rekrytoinneissaan senioritason tehtäviin.

**Kielitaito**: Englannin kielen osaaminen on vaadittua, mutta suomalaisissa yrityksissä suomen kielen taito on usein tärkeämpää, koska monet asiakkaat vaativat sitä.

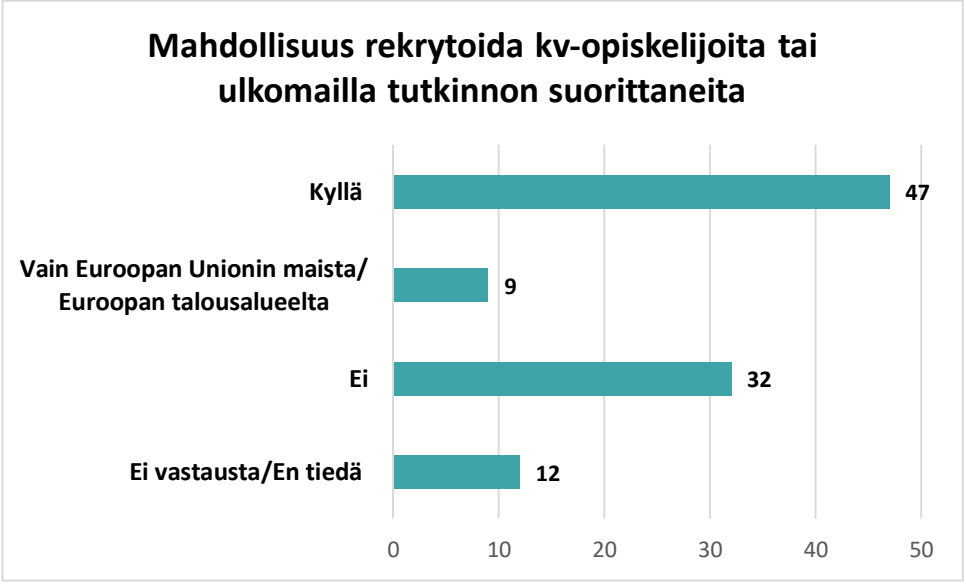
**Jatkuva oppiminen**: Uusilla työntekijöillä tulisi olla motivaatio ja halu oppia jatkuvasti. Kyberturvallisuusala kehittyy nopeasti, ja uusien taitojen hankkiminen on tärkeää. Yritykset panostavat työntekijöiden kouluttamiseen ja kehittämiseen, jotta he voivat nopeasti kehittyä junioritasolta senioritasolle.

Yrityksen rekrytointitarpeita kartoitettaessa (Kuva 8) voidaan havaita, että neljäsosa yrityksistä (25 %) ei näe tarpeelliseksi rekrytoida ainoatakaan kyberturvallisuuden asiantuntijaa kuluvan vuoden aikana. Tyypillisin rekrytoitavien määrä (36 % vastanneista) kuluvalle vuodelle on 1–3 henkilöä ja yhteensä 58 % vastanneista arvioi tämän vuoden rekrytointitarpeekseen 1–10 kyberturvallisuuden asiantuntijaa. Tätä suuremmat rekrytointitarpeet ovat harvinaisia, mutta 4 % ilmoittaa tarpeen olevan yli sadalle rekrytoitavalle asiantuntijalle vuoden 2024 aikana.




**Kuva 8.** Yrityksen/organisaation rekrytointitarve kyberturvallisuuden asiantuntijoille vuonna 2024

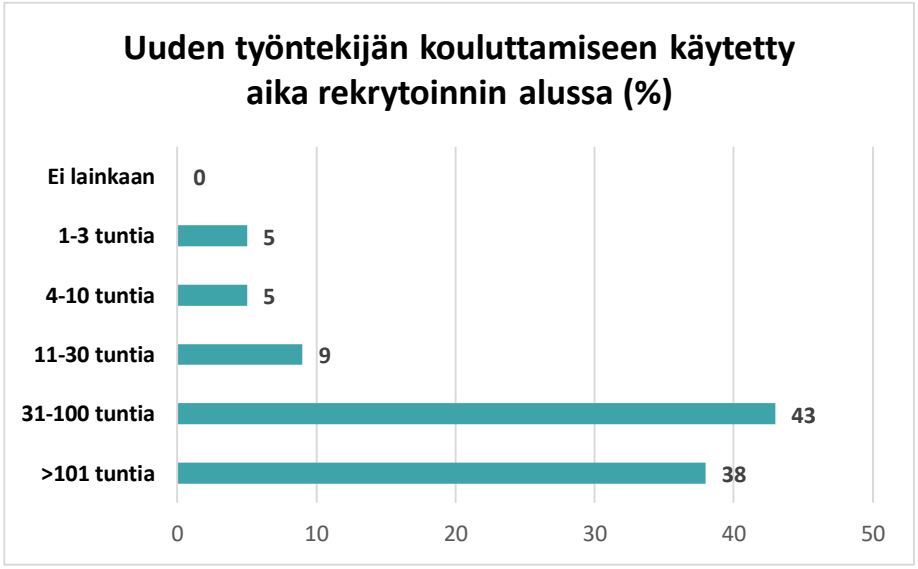
Ulkomailla tutkinnon suorittaneiden tai Suomessa tutkintoa suorittavien kansainvälisten opiskelijoiden rekrytoinnin suhteen vajaa puolet vastanneista (47 %) kertoi suoraan rekrytoinnin olevan mahdollista (Kuva 9). Vastaajista 9 % rajasi kansainvälisten hakijoiden taustan EU/ETA alueelle ja 32 % vastaajista vastasi kieltävästi kansainvälisille rekrytoinneille. Kieltävän vastauksen perusteluissa korostuvat kansainvälisten hakijoiden vaikeudet läpäistä vaadittu turvallisuusselvitys, vaatimus Suomen kansalaisuudesta, sekä kielitaitovaatimukset.




**Kuva 9.** Mahdollisuudet rekrytoida kv-opiskelijoita tai ulkomailla tutkinnon suorittaneita

Avoimen kentän (miksi ei voi rekrytoida kv-opiskelijoita tai ulkomaisen tutkinnon suorittaneita) vastausten analyysi osoitti, että rekrytointi kansainvälisistä opiskelijoista tai ulkomailla tutkinnon suorittaneista henkilöistä on haastavaa ja monissa tapauksissa mahdotonta. Yleisin este on Suomen kansalaisuusvaatimus, joka liittyy usein turvallisuusselvityksiin ja työn luonteeseen. Useat yritykset tarvitsevat työntekijöiltään suomen kielen taitoa sekä suomalaista taustaa, jotta lakisääteiset turvallisuusselvitykset voidaan suorittaa asianmukaisesti. Kansainvälinen turvallisuusselvitys on monimutkainen ja epävarma prosessi, minkä lisäksi asiakkaiden vaatimukset ja luottamuksellisuusasiat korostavat tarvetta suomalaisten työntekijöiden palkkaamiselle. Myös työn perusasioiden oppiminen vie aikaa, ja IPR-suojaus sekä asiakkaiden käyttämä kieli asettavat lisävaatimuksia. Useat pienet ja keskisuuret yritykset eivät ole halukkaita käyttämään englantia työskentelykielenä yksittäisen työntekijän vuoksi.

Kyselyssä kysyttiin myös miten paljon yrityksen/organisaation täytyy käyttää aikaa (tunneissa) uuden työntekijän kouluttamiseen, jotta hän on yrityksen näkökulmasta tuottava (Kuva 10). Tuloksissa on nähtävissä, että koulutukseen kuluu yrityksiltä huomattava määrä aikaa ja muita resursseja. Haastatteluiden kautta oli mahdollista avata koulutustarvetta lisää ja sen kautta esille nousi, että uusille työntekijöille tarvitaan laaja-alaista ja monipuolista perehdytystä ja koulutusta, jotta heistä tulee tuottavia työntekijöitä. Yrityksissä annettavan koulutuksen keskeisiä osa-alueita ovat ohjelmistotuotannon tuottavuuden parantaminen, erilaiset prosessit ja direktiivit, sertifioinnit ja arvioinnit, biometrisen tunnistuksen ja turvaratkaisujen haastaminen, sekä toimialakohtaisten vaatimusten ymmärtäminen ja soveltaminen. Lisäksi uusien työntekijöiden on ymmärrettävä yrityksen tuotteiden tekniset resurssit, käyttö ja toiminta, sekä miten ratkaisut toimivat käytännössä.

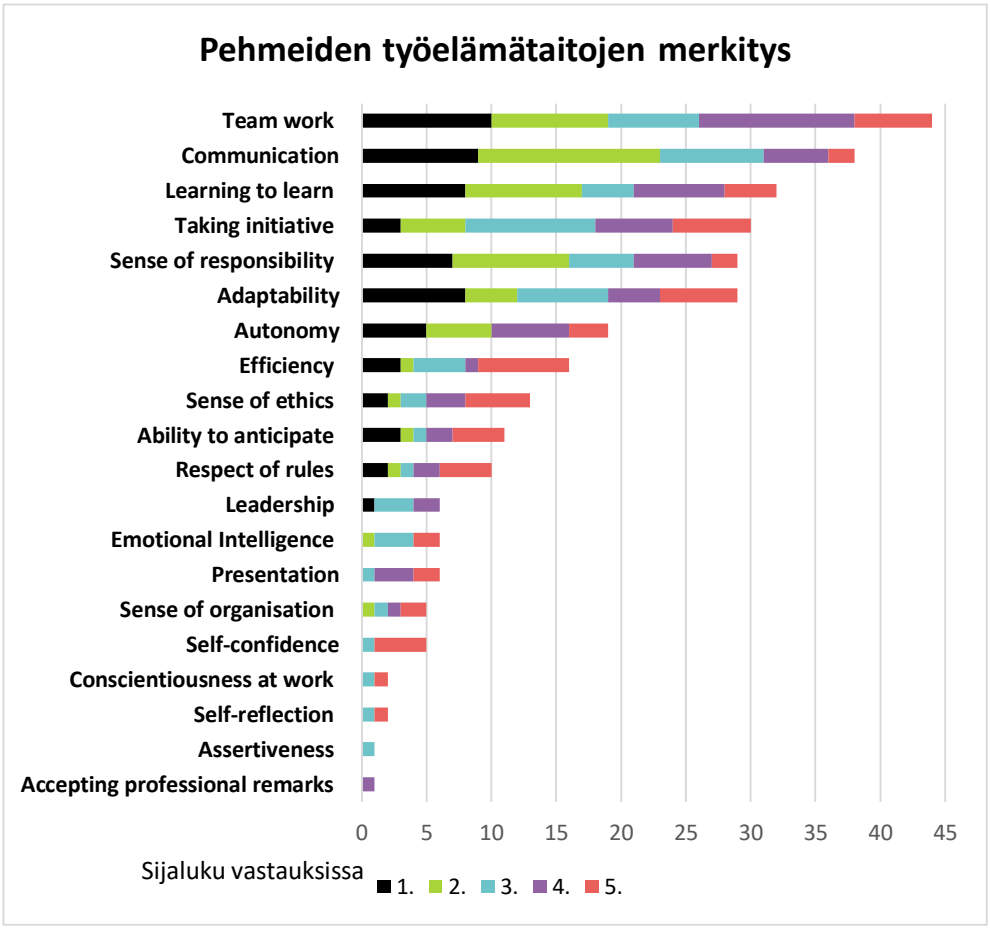



**Kuva 10.** Yrityksien käyttämä aika uuden työntekijän kouluttamiseen rekrytoinnin alussa

Haasteita tuottavat kontekstin ymmärtäminen ja soveltaminen, erityisesti toimialoilla kuten laivanrakennus ja teollisuusautomaatio. Lisäksi työnantajat arvostavat jatkuvaa oppimiskykyä, sanavalmista ja avointa asennetta sekä ymmärrystä verkkotekniikasta ja laajoista kokonaisuuksista. Perehdytysprosessin parantamiseksi olisi hyödyllistä tarjota systemaattista sisääntuloperehdytystä, mentoreita ja säännöllisiä tarkistuspisteitä. Lisäksi korkeakoulujen ja yritysten välistä yhteistyötä tulisi lisätä, jotta koulutus vastaa paremmin työelämän tarpeita ja valmistuneet työntekijät voivat siirtyä sujuvasti työelämään. Haastatteluissa nousi esille myös nostoja yritysten tekemistä vierailijaluennoista, jolloin työelämärelevanssia pystytään tuomaan jo opintojen aikana osaksi kursseja.

## 3.3 Tarvittavat pehmeät työelämätaidot (Soft Skills)

Vastausten perusteella voidaan päätellä, että kyberturvallisuusalalla tarvitaan laajaa valikoimaa pehmeitä taitoja. Kuusi tärkeintä taitoa, eli tiimityöskentely, viestintä, oppimaan oppiminen, aloitteellisuus, vastuuntunto ja sopeutumiskyky erottuvat selkeästi tuloksissa (Kuva 11). Nämä taidot kuvaavat työntekijää, joka pystyy työskentelemään tehokkaasti muuttuvissa tilanteissa jatkuvasti kehittyvällä alalla osana itseohjautuvaa tiimiä, ja joka pystyy kommunikoimaan selkeästi sidosryhmiensä kanssa. Korkeakoulujen rooli on keskeinen näiden taitojen opettamisessa ja kehittämisessä osana kyberturvallisuuskoulutusta.




**Kuva 11.** Työelämätaitojen tärkeysjärjestys

**Tiimityöskentely (Team work)**: Hyvä tiimityöskentely varmistaa sujuvan yhteistyön ja tehokkaan tehtävien jaon. Kyky tiimityöskentelyyn nähtiin selkeästi tärkeimpänä taitona. Vastaajat valitsivat sen sekä useimmin tärkeimpien taitojen listalleen että useimmin tärkeimmäksi taidoksi.

**Viestintä (Communication)**: Hyvä viestintä on välttämätöntä tehokkaalle yhteistyölle ja tiedonvaihdolle tiimin sisällä ja ulkopuolella. Kyky viestiä erottui selkeästi toiseksi tärkeimpänä taitona, ja vastaajat, jotka sen valitsivat, asettivat sen kaikkein useimmin kolmen tärkeimmän taidon joukkoon.

**Oppimaan oppiminen (Learning to learn)**: Jatkuva oppiminen on välttämätöntä alalla, jossa uudet uhat ja teknologiat kehittyvät nopeasti. Oppimaan oppiminen, aloitteellisuus, vastuuntunto ja sopeutumiskyky nähtiin tärkeinä ja tasavahvoina osaamisina.

**Aloitteellisuus (Taking initiative)**: Aloitteellisuus auttaa työntekijöitä löytämään ja ratkaisemaan ongelmia itsenäisesti.

**Vastuuntunto (Sense of responsibility)**: Vastuuntunto on olennaista, jotta työntekijät ottavat omistajuutta tehtävistään ja varmistavat työnsä laadun.

**Sopeutumiskyky (Adaptability)**: Sopeutumiskyvyn tärkeys osoittaa, että työntekijöiden on kyettävä mukautumaan nopeasti muuttuviin tilanteisiin ja teknologioihin.

**Autonomia (Autonomy)**: Autonomiaa eli itsenäisyyttä arvostettiin korkealle, koska kyberturvallisuustehtävät vaativat usein itsenäistä työskentelyä ja ongelmanratkaisukykyä ilman jatkuvaa ohjausta.

**Tehokkuus (Efficiency)**: Tehokkuus auttaa saavuttamaan tuloksia nopeasti ja vähentää resurssien hukkaa.

**Eettinen ajattelu (Sense of ethics)**: Eettinen ajattelu varmistaa, että työntekijät toimivat rehellisesti ja vastuullisesti.

**Ennakoimiskyky (Ability to anticipate)**: Ennakoimiskyky auttaa ennustamaan ja ehkäisemään mahdollisia uhkia ennen niiden toteutumista.

**Sääntöjen kunnioittaminen (Respect of rules)**: Sääntöjen kunnioittaminen varmistaa, että työntekijät toimivat organisaation politiikkojen ja standardien mukaisesti.

**Johtajuus (Leadership)**: Johtajuustaidot ovat välttämättömiä tiimien ja projektien tehokkaalle ohjaamiselle.

**Tunneäly (Emotional Intelligence)**: Tunneäly auttaa työntekijöitä hallitsemaan stressiä ja yhteistyötä tiimissä.

**Esitystaidot (Presentation)**: Esitystaidot ovat välttämättömiä monimutkaisten kyberturvallisuuskysymysten kommunikoinnissa.

**Organisointikyky (Sense of organisation)**: Hyvä organisointikyky auttaa hallitsemaan useita tehtäviä ja projekteja samanaikaisesti.

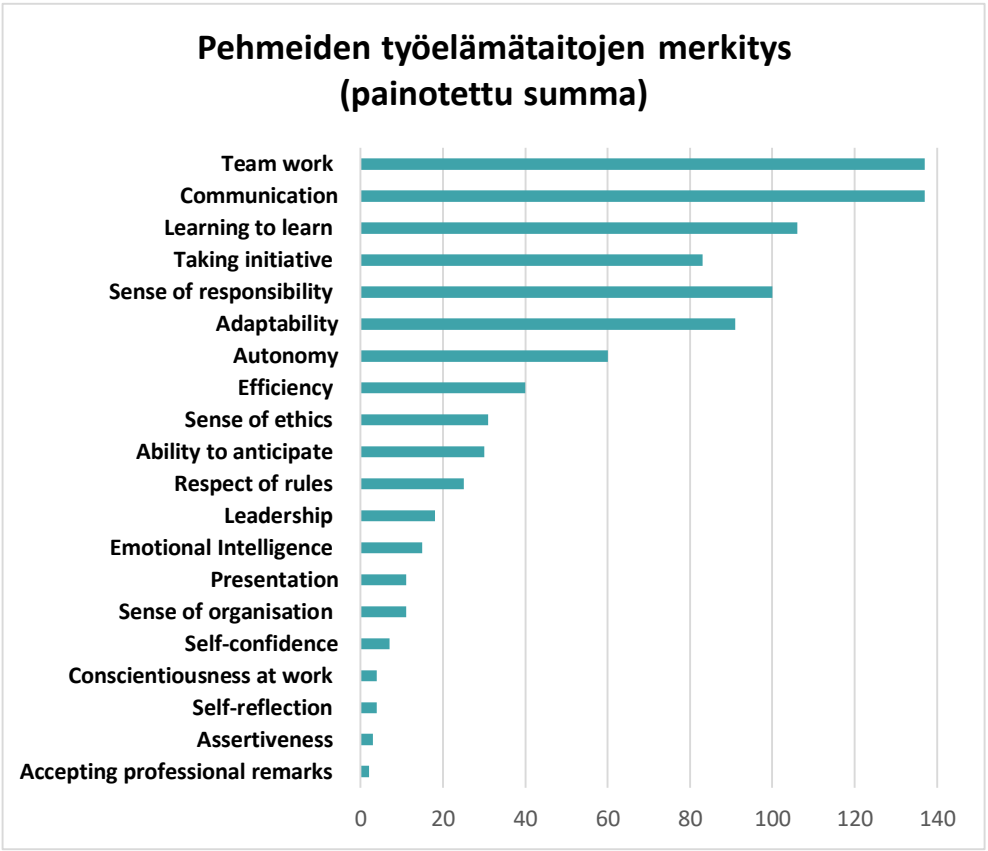
**Itsevarmuus (Self-confidence)**: Itsevarmuus on tärkeää, jotta työntekijät voivat tehdä päätöksiä nopeasti ja tehokkaasti paineen alla.

**Tunnollisuus työssä (Conscientiousness at work)**: Tunnollisuus varmistaa, että työntekijät suorittavat tehtävänsä huolellisesti ja tarkasti.

**Itsearviointi (Self-reflection)**: Kyky arvioida omaa työtään ja oppia virheistä on olennainen osa ammatillista kasvua.

**Jämäkkyys (Assertiveness)**: Jämäkkyys auttaa työntekijöitä tekemään päätöksiä ja pitämään kiinni omista näkemyksistään.

**Ammattimaisten huomautusten hyväksyminen (Accepting professional remarks)**: Kyky ottaa vastaan ja hyödyntää rakentavaa palautetta on olennaista jatkuvan parantamisen kannalta.




**Kuva 12.** Työelämätaitojen tärkeysjärjestys sijaluvulla painotettuna

Vastausten painottaminen sijaluvuilla (tärkein 5 pistettä, 2. tärkein 4, … 5. tärkein 1 piste) ei oleellisesti muuta taitojen keskinäistä järjestystä ja kuuden tärkeimmän taidon ryhmä erottuu edelleen samana (Kuva 12). Ainoastaan aloitteellisuuden (taking initiative) merkitys pienenee, mutta se on edelleen kuudenneksi tärkein taito. Tällä tavalla arvioituna viestintä ja tiimityöskentely nähdään yhtä tärkeinä.

## 3.4 Haastatteluista kerättyjä odotuksia korkeakouluille kyberturvallisuustaitojen kouluttamisesta

Korkeakouluilta odotetaan kyberturvallisuuskoulutuksessa sekä teoreettista että käytännön asiantuntemuksen opettamista ja kehittämistä. Korkeakoulujen rooli on tarjota vahva perusta hallinnollisesta tietoturvaosaamisesta, joka kattaa lait, asetukset, säädökset, direktiivit ja standardit, sekä käytännön taidoista, jotka liittyvät riskienhallintaan ja teknologioiden toimintaperiaatteisiin.

Odotetaan, että korkeakoulut tarjoavat opiskelijoille yleiskuvan kyberturvallisuusalasta, mukaan lukien teknologiat, niiden toimintaperiaatteet ja keskeiset käsitteet kuten CIA-periaate, Defense in Depth, Least Privilege ja Zero Trust. Myös sosiaaliset taidot ja pehmeät arvot, kuten viestintä- ja yhteistyötaidot, ovat tärkeitä.

Yritykset arvostavat myös käytännön osaamista jostakin teknologiasta tai ratkaisusta, jota voidaan soveltaa työssä heti valmistumisen jälkeen. Erityisesti tärkeää on kyky ymmärtää ja käyttää verkkotekniikoita, palomuurikokemus, verkon valvonta (IDS/IPS) sekä hallinnollinen puoli, kuten standardien vaatimusten täyttäminen ja riskienhallinta.

Myös valmistavan teollisuuden tarpeet kyberturvallisuuden osaamisessa tulisi huomioida paremmin. Vaikka mielikuvatasolla valmistava teollisuus ei välttämättä ole etulinjassa kyberturvallisuuden soveltamisessa, eräät teollisuuden alat valmistavat tuotteita tai tuotekokonaisuuksia, joihin kohdistuu huomattavia vaatimuksia kyberturvallisuuden kannalta. Esimerkiksi laivanrakennus-teollisuudessa lopputuote eli laiva on käytännössä kelluva älykaupunki, jonka turvallisen toiminnan takaavat kyberturvallisuusvaatimukset sekä -ratkaisut voiva olla hyvinkin vaativia.

Yritykset odottavat korkeakoulujen auttavan opiskelijoita kehittämään kykyä etsiä tietoa ja dokumentoida asioita tarkasti ja ammattimaisesti. Käytännön osaamista ja sertifikaatteja, kuten CEH (Certified Ethical Hacker) ja erilaisia pilvipalveluihin liittyviä sertifikaatteja, pidetään myös arvokkaina. Yritykset tarjoavat usein omaa koulutusportaalien kautta tuotteisiin ja ratkaisuihin liittyvää koulutusta, mutta korkeakoulut voivat tarjota pohjan, jonka päälle nämä yritysten tarjoamat koulutukset rakentuvat.

Koulutuksen kehitysehdotuksena korkeakouluille suositellaan:

1. Monipuolisen perusosaamisen varmistaminen: Tarjottava kattava perusosaaminen kyberturvallisuuden eri osa-alueista, mukaan lukien teknologiat, standardit ja periaatteet.
2. Käytännön taitojen kehittäminen osana opintoja: Sisällytetään enemmän käytännön harjoituksia ja laboratoriotyöskentelyä, joissa opiskelijat voivat soveltaa oppimaansa käytännössä.
3. Pehmeiden taitojen oppimisen tärkeys: Korostetaan ja harjoitellaan viestintä- ja yhteistyötaitoja, joita tarvitaan tehokkaassa työskentelyssä ja tiimityössä.
4. Sertifikaattivalmiudet: Valmistetaan opiskelijoita ammatillisiin sertifikaatteihin, jotka ovat arvokkaita työmarkkinoilla. Opintojen aikana nostetaan esille jatkuvan oppimisen tärkeys ja ammatillisen osaamisen ylläpitäminen läpi työuran.
5. Ajankohtaiset opetussuunnitelmat: Opetussuunnitelmat tulisi pitää ajan tasalla uusimpien teknologioiden ja trendien, kuten tekoälyn ja pilvipalveluiden, osalta.
6. Yhteistyö yritysten kanssa: Korkeakoulujen tulisi tiivistää yhteistyötä yritysten kanssa, jotta koulutuksen sisältö vastaa työelämän tarpeita ja opiskelijoilla on mahdollisuus saada käytännön kokemusta esimerkiksi harjoittelujaksojen kautta.

Jatkuvan oppimisen merkityksen korostaminen ja koulutuksen arvostus nousi haastatteluissa esille. Myös ilmaisia koulutuksia arvostetaan osana jatkuvan oppimisen tarjontaa. Ilmaisia koulutuksia pidetään tarpeellisina ja niitä kannustetaan hyödyntämään. Esimerkiksi FiTech-kursseja pidetään arvokkaina, ja työajalla tapahtuvaa koulutusta voidaan tukea tarjoamalla opintovapaata. Vastaavanlaisia ilmaisia koulutuksia on tarjolla avointen yliopistojen kautta, jolloin koulutuksen rahoittajana toimii mm. Opetus- ja Kulttuuriministeriö/Jotpa (Jatkuvan oppimisen ja työllisyyden palvelukeskus).Ilmaisten koulutusten arvostus ilmeni haastatteluissa siten, että kaikki relevantti koulutus on tarpeellista, riippumatta siitä, onko se ilmaista vai maksullista. Työnantajat voivat kannustaa työntekijöitään osallistumaan ilmaisiin kursseihin, kuten FiTech-kursseille, jotka tarjoavat mahdollisuuksia kehittää osaamistaan. Työpaikat voivat tarjota opintovapaata tietyin ehdoin, mikä mahdollistaa työntekijöiden osallistumisen koulutuksiin työajan puitteissa. Ilmaiset koulutukset ovat osa laajempaa jatkuvan oppimisen strategiaa, jolla pyritään

pitämään työntekijöiden taidot ajan tasalla ja vastaamaan muuttuviin työelämän tarpeisiin.

Koulutuksesta saadut opintopisteet tai todistus eivät ole keskeisessä roolissa, kun arvioidaan koulutuksen merkitystä. Joissakin tapauksissa opintopisteet riittävät, ja niitä arvostetaan, erityisesti silloin kun halutaan varmistaa, että opiskelijat valmistuvat ajoissa. Joissakin tilanteissa taas sertifikaateilla on enemmän merkitystä, erityisesti silloin kun osaamisen todistaminen on tärkeää (esim. julkishallinnon kilpailutuksissa). Sertifikaatit voivat olla tärkeitä esimerkiksi tiettyjen tehtävien tai roolien vaatiman osaamisen osoittamiseksi. Sisällöllä ja koulutuksen laadulla on suurempi merkitys kuin sillä, saako koulutuksesta opintopisteitä tai todistuksen. Tärkeintä on, että koulutus on relevanttia ja käytännönläheistä, ja että se tarjoaa tarvittavat taidot ja tiedot. Osaamisen näyttämisellä on suuri merkitys. On tärkeää, että työntekijät voivat käytännössä osoittaa, mitä he ovat oppineet.

# 4 Yhteenveto

Tässä raportissa kuvattiin Kansallisen kyberturvallisuuskoulutuksen yhteistyöverkoston rakentaminen -hankkeen kysely- ja haastattelututkimuksen tuloksia. Hankkeeseen osallistuu yhdeksän suomalaista yliopistoa ja 14 ammattikorkeakoulua, jotka kaikki tarjoavat kyberturvallisuusalan koulutusta. Yliopistojen ja ammattikorkeakoulujen yhteisenä toteutuksena järjestettiin sidosryhmäkysely, jonka tarkoituksena oli kartoittaa yritysten ja organisaatioiden kyberturvallisuus-taitoja ja -tarpeita. Kartoitus toteutettiin 28.1.2024 - 31.3.2024, ja kyselyyn vastasi 61 yrityksen tai julkishallinnon organisaation edustajaa. Kyselyä täydennettiin myös 14 haastattelulla, jotta saatiin syvällisempää tietoa vastaajien näkemyksistä ja tarpeista.

Kyselyn perusteella yritykset ja organisaatiot tarvitsevat monipuolista osaamista kyberturvallisuuden eri osa-alueilla. Tärkeimmät osa-alueet tällä hetkellä ovat tietoturva ja yksityisyyden suoja, koulutus ja jatkuva oppiminen, identiteetin hallinta sekä turvallisuuden hallinta ja hallintotavat. Näitä osa-alueita pidetään kriittisinä yritysten toiminnan kannalta. Lisäksi oikeudelliset näkökohdat, ohjelmisto- ja laitteistoturvallisuus sekä ihmistekijät ovat keskeisiä nykyhetken tarpeita. Vähemmän tärkeinä pidettiin steganografiaa, teoreettisia perustuksia ja kryptologiaa.

Tulevaisuudessa tärkeimmiksi osa-alueiksi arvioidaan tietoturva ja yksityisyyden suoja, turvallisuuden hallinta ja hallintotavat, ohjelmisto- ja laitteistoturvallisuus, identiteetin hallinta, sekä oikeudelliset näkökohdat. Myös tekoäly ja koneoppiminen nähdään merkittävinä osa-alueina tulevaisuudessa.

Yritykset odottavat uusilta työntekijöiltä vahvaa kyberturvallisuusalan osaamis- ja tietoperustaa sekä kykyä jatkuvaan oppimiseen ja opittujen taitojen soveltamiseen käytännössä. Pehmeät taidot, kuten ymmärrys laajasta kybertoimintaympäristöstä, resilienssiajattelu ja lainsäädännön perusteet, ovat tärkeitä. Teknisiin taitoihin kuuluvat kiristyshaittaohjelmien tuntemus, digitaalinen forensiikka, koodaus- ja skriptaustaidot sekä verkko-osaaminen.

Uusien työntekijöiden perehdytys yrityksissä vaatii laaja-alaista ja monipuolista koulutusta. Tämä sisältää ohjelmistotuotannon tuottavuuden parantamisen, erilaiset direktiivit ja sertifioinnit, biometrisen tunnistuksen ja turvaratkaisujen haastamisen,

sekä toimialakohtaisten vaatimusten ymmärtämisen ja soveltamisen. Perehdytysprosessin parantamiseksi olisi hyödyllistä tarjota systemaattista sisääntuloperehdytystä, mentoreita ja säännöllisiä tarkistuspisteitä.

Korkeakoulujen roolina on tarjota sekä teoreettista että käytännön asiantuntemusta kyberturvallisuudessa. Tämä sisältää vahvan perustan hallinnollisesta tietoturvaosaamisesta, joka kattaa lait, asetukset, säädökset, direktiivit ja standardit, sekä käytännön taidot riskienhallinnassa ja teknologioiden toimintaperiaatteissa. Korkeakoulujen tulisi tarjota opiskelijoille yleiskuva kyberturvallisuusalasta, mukaan lukien teknologiat, niiden toimintaperiaatteet ja keskeiset käsitteet kuten CIA-periaate, Defense in Depth, Least Privilege ja Zero Trust.

Yritykset arvostavat käytännön osaamista jostakin teknologiasta tai ratkaisusta, jota voidaan soveltaa työssä heti valmistumisen jälkeen. Erityisen tärkeää on kyky ymmärtää ja käyttää verkkotekniikoita, palomuurikokemus, verkon valvonta sekä hallinnollinen puoli, kuten standardien vaatimusten täyttäminen ja riskienhallinta.

Koulutuksen kehitystarpeiden osalta nousee esille tarve tarjota kattava perusosaaminen kyberturvallisuuden eri osa-alueista, mukaan lukien teknologiat, standardit ja periaatteet. Opintoihin tulisi sisällyttää enemmän käytännön harjoituksia ja laboratoriotyöskentelyä, joissa opiskelijat voivat soveltaa oppimaansa käytännössä. Koulutuksessa tulee harjoitella viestintä- ja yhteistyötaitoja, joita tarvitaan tehokkaassa työskentelyssä ja tiimityössä. Koulutuksen on hyvä valmistaa opiskelijoita ammatillisiin sertifiointeihin, jotka ovat arvokkaita työmarkkinoilla, ja opintojen aikana on tarpeen nostaa esille jatkuvan oppimisen tärkeys sekä ammatillisen osaamisen ylläpitäminen läpi työuran. Opetussuunnitelmat tulisi pitää ajan tasalla uusimpien teknologioiden ja trendien, kuten tekoälyn ja pilvipalveluiden, osalta. Tiivistetään yhteistyötä yritysten kanssa, jotta koulutuksen sisältö vastaa työelämän tarpeita ja opiskelijoilla on mahdollisuus saada käytännön kokemusta esimerkiksi harjoittelujaksojen kautta.

Ilmaisia koulutuksia arvostetaan osana jatkuvan oppimisen tarjontaa. Ilmaiset koulutukset, kuten FiTech-kurssit tai Avoimen yliopiston kautta tarjotut kurssit, ovat arvokkaita ja niitä kannustetaan hyödyntämään. Työpaikat voivat tarjota opintovapaata tietyin ehdoin, mikä mahdollistaa työntekijöiden osallistumisen koulutuksiin työajan puitteissa. Ilmaiset koulutukset ovat osa laajempaa jatkuvan oppimisen strategiaa, jolla pyritään pitämään työntekijöiden taidot ajan tasalla ja vastaamaan muuttuviin työelämän tarpeisiin.

Koulutuksesta saadut opintopisteet tai todistus eivät ole keskeisessä roolissa, kun arvioidaan koulutuksen merkitystä. Tärkeämpää on koulutuksen sisältö ja kyky soveltaa oppimaansa käytännössä. Osaamisen näyttämisellä on suuri merkitys; on tärkeää, että työntekijät voivat käytännössä osoittaa, mitä he ovat oppineet.

Kansallisella tasolla kyberturvallisuusalan korkeakoulutuksen kehittämisen tueksi ja lisätarpeiden tunnistamiseksi on tässä raportissa esitetyn tutkimuksen

lisäksi suoritettu tutkimus kyberturvallisuusalan koulutusta tarjoavien yliopistojen koulutuksen osaajaprofiileista ja kurssien painotusaloista. Tästä 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)

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

# Liitteet

## Liite 1: Yrityksille lähetetty Webropol-kysely

Cybersecurity education needs in Finland

Mandatory questions are marked with a star (*)

Background:

This survey examines cybersecurity education, needs, and skills development in companies and organizations in Finland. The survey focuses on three main topics: 1) the cybersecurity themes and topics where skills and training are needed now and in the future, 2) how much time is spent training new cybersecurity employees in the organization, and 3) what soft skills are needed in employees. General

background information about the organization is also asked.

The purpose: The survey will be used to identify the current situation and future needs for cybersecurity skills in companies and organizations. The survey is part of a Ministry of Education and Culture cybersecurity project involving higher education institutions (universities and universities of applied sciences) that provide cybersecurity education. The results will be used to develop and improve education in higher education institutions.

There are a total of 17 questions. If you would like to participate in the interview, contact information will be requested at the end of the questionnaire. The survey takes about 20-25 minutes to answer all questions.

How your answers are used: All the data will be handled anonymously, and no information will be delivered "as-is" to any third party. Partial summaries and anonymized quotes might be published as a part of academic publications, but with all references to names, locations, or any identifying information removed. Published results will include aggregated statistical observations from where it is impossible to identify individual answers. For any further questions and comments, please contact the signatories.

Thank you for your valuable input!

This survey is a collaboration between 9 universities and 14 universities of applied sciences:

Piia Perälä (piia.m.h.perala@jyu.fi), Faculty of Information Technology, University of Jyväskylä

Martti Lehto (martti.j.lehto@jyu.fi), Faculty of Information Technology, University of Jyväskylä

Seppo Virtanen (seppo.virtanen@utu.fi), Department of Computing, University of Turku

Tuomas Aura (tuomas.aura@aalto.fi), Department of Computer Science, Aalto University

Marko Helenius (marko.helenius@tuni.fi), Unit of Computing Sciences, Network and Information Security Group, Tampere University

Kimmo Halunen (kimmo.halunen@oulu.fi), Faculty of Information Technology and Electrical Engineering, University of Oulu

Valtteri Niemi (valtteri.niemi@helsinki.fi), Department of Computer Science, University of Helsinki

Marina Waldén (marina.walden@abo.fi), Information Technology, Faculty of Science and Engineering, Åbo Akademi University

Emmanuel Anti (x5164390@student.uwasa.fi), Department of Computing Sciences, University of Vaasa

Bilal Naqvi (syed.naqvi@lut.fi), School of Engineering Sciences, LUT University

Karo Saharinen (karo.saharinen@jamk.fi), Jyväskylän ammattikorkeakoulu

Pasi Kämppi (pasi.kamppi@laurea.fi), Laurea-ammattikorkeakoulu

Henry Paananen (henry.paananen@centria.fi), Centria-ammattikorkeakoulu

Tero Ulvinen (tero.ulvinen@vamk.fi), Vaasan ammattikorkeakoulu

Antti Piironen (antti.piironen@metropolia.fi), Metropolia ammattikorkeakoulu

Mikko Korpela (mikko.korpela@tuni.fi), Tampereen ammattikorkeakoulu

Jari Uimonen (jari.uimonen@karelia.fi), Karelia-ammattikorkeakoulu

Jani Ekqvist (jani.ekqvist@turkuamk.fi), Turun ammattikorkeakoulu

Jarkko Hänninen (jarkko.hanninen@xamk.fi), Kaakkois-Suomen ammattikorkeakoulu

Jussi Ala-Hiiro (jussi.ala-hiiro@kamk.fi), Kajaanin ammattikorkeakoulu

Ari Affekt (ari.affekt@lapinamk.fi), Lapin ammattikorkeakoulu

Markku Kellomäki (markku.kellomaki@savonia.fi), Savonia-ammattikorkeakoulu

Instructions:

Next, we ask about the various cybersecurity themes and topics that your organization needs to address in terms of skills development.

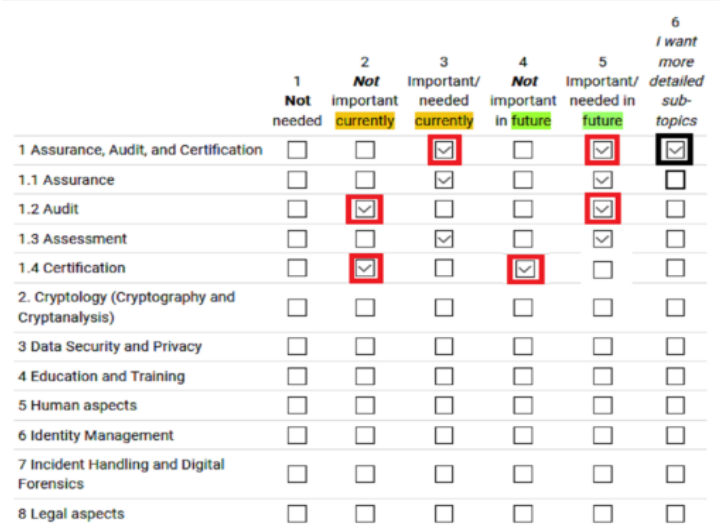
The survey is based on the JRC's European Cybersecurity Taxonomy. It covers 15 cybersecurity domains. You can download the framework from this link if you want more information. Link to Taxonomy.

This is a multiple-choice question where we ask you to consider the need for the topic now and in the future. This information will provide cybersecurity training institutions with useful information to outline and plan the content of future studies and courses, as well as the focus of different topics.

In the example below, 1. Assurance, Audit and Certification are identified as important now and in the future.

In a more detailed sub-theme description, 1.2 Audit is not important now, but will be important in the future, and 1.4 Certification is important currently, but not important in the future.

When you select "6. I want to answer more detailed sub-questions", more detailed sub-questions will appear.A maximum of 4 subtopics per main theme will open.



| | 1 **Not** needed | 2 ***Not*** important currently | 3 Important/ needed currently | 4 ***Not*** important in future | 5 Important/ needed in future | 6 *I want more detailed sub-topics* |
|---|---|---|---|---|---|---|
| 1 Assurance, Audit, and Certification | ☐ | ☐ | ☑ | ☐ | ☑ | ☑ |
| 1.1 Assurance | ☐ | ☐ | ☑ | ☐ | ☑ | ☐ |
| 1.2 Audit | ☐ | ☑ | ☐ | ☐ | ☑ | ☐ |
| 1.3 Assessment | ☐ | ☐ | ☑ | ☐ | ☑ | ☐ |
| 1.4 Certification | ☐ | ☑ | ☐ | ☑ | ☐ | ☐ |
| 2. Cryptology (Cryptography and Cryptanalysis) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 3 Data Security and Privacy | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 4 Education and Training | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5 Human aspects | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 6 Identity Management | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 7 Incident Handling and Digital Forensics | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 8 Legal aspects | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

You can select as many answers as applicable.

Please use the open-ended question field to further describe your organization's cybersecurity training needs - all information, needs, and perspectives will help us understand and address training needs when designing education and course content.

You can answer open text questions in English or Finnish!

More information: Link to the project website and privacy notice

1.Describe your organization's skills needs in these themes: now and in the future?

There are 16 cybersecurity themes in total and in this survey the themes are divided into two pages. The themes are based on the cybersecurity taxonomy defined by the JRC.

Select "6. I want detailed subtopics" to answer detailed list of topics per theme. A maximum of 4 subtopics per main theme will open. You can select as many answers as applicable.

| | 1 **Not** needed | 2 ***Not*** important currently | 3 Important/ needed currently | 4 ***Not*** important in future | 5 Important/ needed in future | 6 **I want more detailed sub-topics** |
|---|---|---|---|---|---|---|
| **1 Assurance, Audit, and Certification** * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2. Cryptology (Cryptography and Cryptanalysis)** * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3 Data Security and Privacy** * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4 Education and Training** * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5 Human aspects** * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6 Identity Management** * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7 Incident Handling and Digital Forensics** * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8 Legal aspects** * | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

2. Please elaborate further on your answers (in English or Finnish)

3. Describe your organization's skills needs in these themes: now and in the future?

There are 16 cybersecurity themes in total and in this survey the themes are divided into two pages.

Select "6. I want detailed subtopics" to answer detailed list of topics per theme. A maximum of 4 subtopics per main theme will open. You can select as many answers as applicable.

| | 1 **Not** needed | 2 ***Not*** important currently | 3 Important/ needed currently | 4 ***Not*** important in future | 5 Important/ needed in future | 6 **I want more detailed sub-topics** |
|---|---|---|---|---|---|---|
| **9 Network and Distributed Systems *** | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10 Security management and governance *** | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11 Security Measurements *** | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12 Software and Hardware Security Engineering *** | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| **13 Steganography, Steganalysis and Watermarking *** | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| **14 Theoretical Foundations *** | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| **15 Trust Management and Accountability *** | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| **16 Artificial intelligence and machine learning *** | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

4. Please elaborate further on your answers (in English or Finnish)

5. What are the soft skills required for new hires in your organization? Rank the top five in order of importance

Soft skills are adapted from: http://www.softskills-project.eu/assets/materials/en/soft-skills-list-with-pictograms.pdf

Lista kysytyistä työelämätaidoista: Adaptability; Accepting professional remarks; Autonomy; Learning to learn; Presentation; Emotional intelligence; Self-confidence; Self-reflection; Sense of organization; Sense of responsibility; Taking initiative; Ability to anticipate; Respect of rules; Efficiency; Sense of ethics; Conscientiousness at work; Communication; Leadership; Assertiveness; Team work.

Jokaisella työelämätaidolla oli valittavana seuraavat vaihtoehdot:

- The first and most important
- The second most important
- The third most important

- The fourth most important
- The fifth most important

6. Describe what is the skill level of a typical cybersecurity junior hire in your organization (in English or Finnish)?

We aim to understand the potential skill gap between new graduates and productive junior employees.

7. What is the average training effort in hours that is needed to bring a junior hire up to the standards of your organization (e.g. self-education, guided learning and/or external courses/certification training)?

Vastausvaihtoehdot:

- None
- 1-3 hours
- 4-10 hours
- 11-30 hours
- 31-100 hours
- >101 hours

8. Does your organization have the possibility to employ international students/graduates?

Vastausvaihtoehdot:

- Yes
- Only from European Union / European Economic Area
- No, please specify the main reason (In English of Finnish)
- No answer/I don’t know

9. What are the main economic activities of your organization? (Following the EU NACE v2.1 / Finnish Toimialaluokitus 2025 main level codes)

Vastausvaihtoehdot (erottimena puolipilkku): Agriculture, forestry and fishing; Mining and quarrying; Manufacturing; Electricity, gas, steam and air conditioning supply; Water supply, sewerage, waste management and remediation; Construction; Wholesale and retail trade; Transportation and storage; Accommodation and food service; Publishing, broadcasting and content production and distribution; Telecommunication, computer programming, consulting, computing infrastructure and other information services; Financial and insurance;

Real estate; Professional, scientific and technical; Administrative and support service; Public administration and defence, compulsory social security; Education; Human health and social work; Arts, sports and recreation; Other services.

10. Does your organization provide cybersecurity services to other companies?

Vastausvaihtoehdot:

- Yes
- No

11. What is the number of employees in the organization

Vastausvaihtoehdot:

- <= 10 Micro
- 11-50 Small
- 51-250 Medium
- > 250 Large

12. What is the number of cybersecurity professionals currently employed?

Vastausvaihtoehdot:

- 0
- 1-3
- 4-10
- 11-30
- 31-100
- >101

13. How many cybersecurity professionals your organization is planning to hire during 2024?

Vastausvaihtoehdot:

- 0
- 1-3
- 4-10
- 11-30
- 31-100
- >101

14. What is your current role in your organization (in English or Finnish)?

15. Which of the following options best describes your current role in your organisation?

Vastausvaihtoehdot:

- Organization’s internal cybersecurity services, securing the organization itself
- Organization’s customer-facing cybersecurity services, securing goods or services offered to customers
- Cybersecurity services offered to customers
- Some other, please specify:

16. Any other comments, ideas of feedback (in English or Finnish)?

17. Are you interested in participating in an interview to help us understand your needs better?

Vastausvaihtoehdot:

- Yes
- No

# Liite 2: Haastatteluiden kysymykset

- Yrityksen toimiala?
    - Rooli (kyberturvallisuuden teknologiakehittäjä, kyberturvallisuutta soveltava palveluntarjoaja, kyberturvallisuutta organisaatiossa tarvitseva, jne)?
    - Yrityksen ala huomioiden, perustele tärkeimpien ja vähiten tärkeiden kyselyn Kyberturvallisuustaitojen valintoja
- Kyselyn rakenteesta
    - Mitä tulkitset kunkin kyselyssä esitetyn taidon tarkoittavan?
    - Miten olet ymmärtänyt kyselyn täyttöohjeen?
- Avasitko alakategoriat ja jätitkö rastit myös pääkategoriaan?
    - Tarkoittaako sinulle “tarvitaan nyt” sitä, että tarvitaan myös tulevaisuudessa, vai oletko siinä tapauksessa rastittanut molemmat?
    - Onko kyselyn taksonomia relevantti työnantajan tarpeiden kannalta?
- Mitä valmistuneet oikeasti osaavat, kun tulevat töihin? Millainen tutkinto heillä on (IT-ala yleisesti / kyberturvallisuuden tutkinto)?
    - Mitä työnantajat arvostavat? Millainen vastavalmistunut on hyvä työntekijä?
- Mitä perehdytystä ja koulutusta joudutaan antamaan työpaikalla, jotta voidaan laskea tuottavaksi työntekijäksi?
- Mikä on korkeakoulujen rooli kyberturvallisuusasiantuntijoiden tietämyksen ja osaamisen kehittämisessä?
    - Miten vertautuu yritysten omaan vastuuseen koulutuksesta ja perehdytyksestä?
- Mitä odotetaan korkeakouluista alalta valmistuneilta sisällöllisesti?
    - Mitä puutteita on havaittu?
    - Onko eroa, onko valmistunut yliopistosta vai ammattikorkeakoulusta?
- Minkälaista kyberturvallisuuden opetusta teidän näkökulmastanne kaivataan?
- Mitkä osaamiset ovat kaikkein tärkeimpiä, mitkä toivomuslistalla (esim. työpaikkailmoituksissa)?
- Onko odotuksia ammatillisesta sertifioinnista?

    - Onko tiettyjä sertikursseja, joihin uudet työntekijät joudutaan lähes aina laittamaan? Miksi?

- Arvostatteko ilmaisia koulutuksia?
- Onko kilpailutuksissa tai alihankintaketjuissa vaatimuksia tietyille sertifioinneille tai jollekin muulle tietylle erityisosaamiselle?
- Onko sillä merkitystä, kuka toimii kouluttajana (yksityinen yritys / julkinen toimija)?

o Opintopisteet vai sertifikaatti tietystä osaamisesta?

University of Turku
Reports from the Faculty of Technology

1. **Anne-Maarit Majanoja, Antti Hakkala, Jari Lehto & Seppo Virtanen**. Suomen kyberturvallisuuskoulutusta tarjoavien yliopistojen koulutuksen osaajaprofiilit ja kurssien painotusalat. 2024.
2. **Anne-Maarit Majanoja, Jani Ekqvist, Antti Hakkala & Seppo Virtanen**. Kyberturvallisuuskoulutuksen kehittäminen Suomessa: yritysten osaamistarve-kartoitus. 2024.