AMK-opiskelijan

KYBER-TURVALLISUUS-OSAAMINEN

Osaamiskuvaukset ja -tasot opetussuunnitelmien tueksi

Kyberturvallisuuskoulutuksen ja siihen liittyvän yhteistyön kehittäminen korkeakouluissa

AMK-opiskelijan kyberturvallisuusosaaminen -materiaali on tuotettu osana Opetus- ja kulttuuriministeriön rahoittamaa 14 ammattikorkeakoulun *Kyberturvallisuuskoulutuksen ja siihen liittyvän yhteistyön kehittäminen korkeakouluissa* -yhteishanketta.

Yhteistyöhankkeen osapuolia 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.

Sisältö

Johdanto

Hyvä korkeakoulun edustaja,

Käsissäsi on yhteenveto osaamiskuvauksista, jotka on laadittu Opetus- ja kulttuuriministeriön rahoittamassa hankkeessa *"Kyberturvallisuuskoulutuksen ja siihen liittyvän yhteistyön kehittäminen korkeakouluissa"* vuosina 2023–2025.

Tämä julkaisu kokoaa eri aloihin liittyvät osaamiskuvaukset, osaamistasot sekä niitä konkretisoivat osaamislauseet tiivistetyssä ja helposti hyödynnettävässä muodossa. Osaamiskuvaukset on johdettu keskeisistä kansainvälisistä kyberturvallisuusalan ja opetuksen osaamisviitekehyksistä. Osaamiskuvasten pohjalta ja niitä hyödyntäen toteutettiin lisäksi eri aloille sopivia kyberturvallisuuden oppimateriaaleja, joita pilotoitiin hankkeen aikana. Piloteissa hyödynnetyt materiaalit ovat saatavilla avoimina oppimateriaaleina. Linkit oppimateriaaleihin on ilmoitettu osaamiskuvausten yhteydessä.

Osaamiskuvauksia voidaan käyttää kokonaisuudessaan esimerkiksi opintojakson pohjana tai vaihtoehtoisesti yksittäisiä osaamislauseita voidaan integroida täydentämään olemassa olevia opetussuunnitelmia. Korkeakoulutusta ohjaa akateeminen vapaus, ja siten hankkeen tulosten hyödyntäminen jää kunkin tutkinto-ohjelman ja opetussuunnitelmatyöstä vastaavien toimijoiden harkintaan. Hankkeessa tuotettuja opetusmateriaaleja saa vapaasti jatkokäyttää ja kehittää osana kaikkea koulutustoimintaa.

Suomen kyberturvallisuusstrategia ja sen toimeenpano-ohjelma ovat edistäneet kyberturvallisuuden koulutuksen systemaattista kehittämistä korkeakouluissa. Hankkeessa tehty työ tukee osaltaan kyberturvallisempaa Suomea edistämällä osaamista, koulutusta ja yhteistä ymmärrystä kyberturvallisuuden merkityksestä yhteiskunnassa.

Jyväskylässä helmikuussa 2026

Karo Saharinen
Jyväskylän ammattikorkeakoulu, IT-instituutti

1. Kyberturvallisuuden osaamisen viitekehykset

Osaamiskuvausten luomisessa on käytetty useita keskeisiä kyberturvallisuuden ja oppimisen viitekehyksiä, jotta osaamiskuvaukset muodostuisivat kattaviksi ja tasapainoisiksi. Usean viitekehyksen käyttö vahvistaa ymmärrystä alan osaamisvaatimuksista ja luo hyvän perustan opintokokonaisuuksien jatkokehitykselle. Tässä luvussa on tiivistetysti kuvattu kehitystyössä sovelletut viitekehykset ja niiden rooli.

1.1 Joint Research Center (JRC) – Kyberturvallisuuden taksonomia

JRC:n kyberturvallisuuden taksonomia (Nai et al., 2022) toimii kehitystyön rakenteellisena perustana. Taksonomia kokoaa 15 kyberturvallisuuden osa-aluetta:

- Auditointi ja sertifiointi (Assurnace, Audit and Certification)
- Kryptologia (Cryptology)
- Tietoturva ja tietosuoja (Data Security and Privacy)
- Opetus ja koulutus (Education and Training)
- Inhimilliset näkökulmat (Human Aspects)
- Identiteetin hallinta (Identity Management)
- Poikkeamien hallinta ja forensiikka (Incident Handling and Digital Forensics)
- Lainopilliset näkökulmat (Legal Aspects)
- Tietoverkot ja hajautetut järjestelmät (Network and Distributed Systems)
- Tietoturvan hallinta ja johtaminen (Security Management and Governance)
- Turvallisuuden mittaaminen (Security Measurements)
- Ohjelmisto- ja laitteistoturvallisuuden kehittäminen (Software and Hardware Security Engineering)
- Steganographia (Steganography, Steganalysis and Watermarking)
- Teoreettiset perusteet (Theoretical Foundations)
- Luottamuksen hallinta ja vastuullisuus (Trust Management and Accountability)

Näiden osa-alueiden pohjalta jäsennettiin tässä julkaisussa käytetty osaamiskuvausten taksonomia.

1.2 NICE Workforce Framework for Cybersecurity (NIST)

NISTin NICE-viitekehys (National Initiative for Cybersecurity Careers and Studies [NICCS], 2025) määrittelee kyberturvallisuuden työroolit, niihin liittyvät tehtävät sekä tietojen ja taitojen vaatimukset. Viitekehys rakentuu viidestä pääluokasta:

- valvonta ja johtaminen
- suunnittelu ja kehitys
- käyttöönotto ja operointi
- suojaus ja puolustus
- tutkinta.

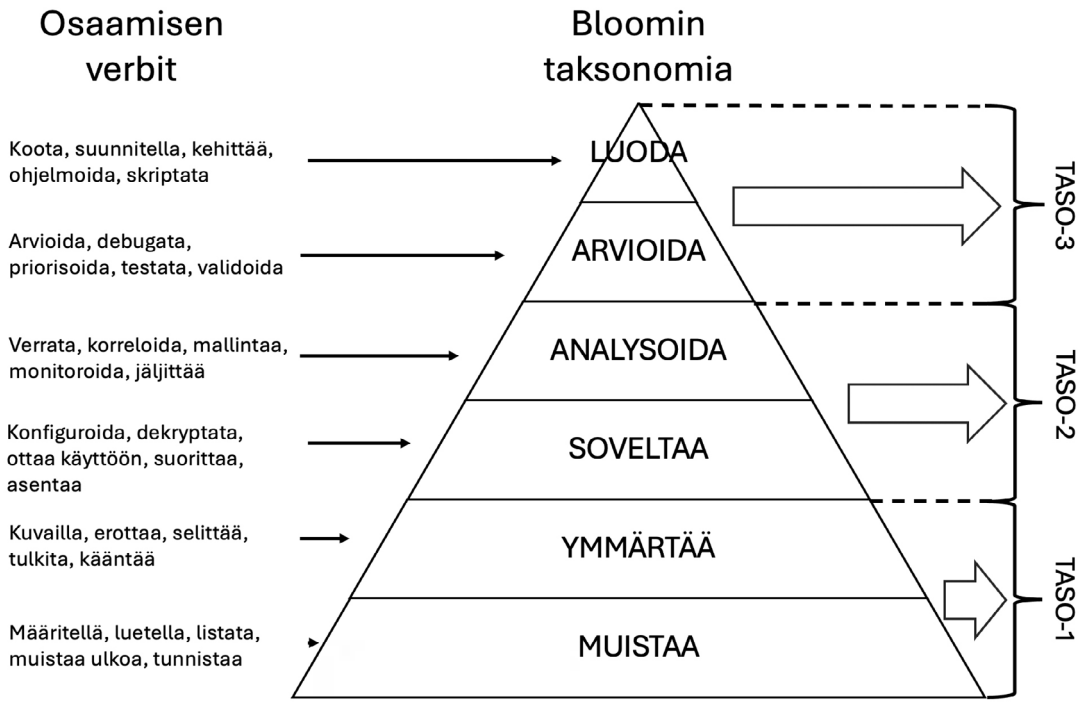
NICE-viitekehys auttaa sanallistamaan osaamisvaatimuksia erityisesti tilanteissa, joissa JRC:n osa-alue on liian laaja, ja joissa osaamisvaatimuksiin tarvitaan tarkempi työrooli-lähtöinen määrittely.

1.3 European Cybersecurity Skills Framework (ECSF)

ENISAn ECSF-viitekehys (European Union Agency for Cybersecurity [ENISA], 2025) tuo osaamisvaatimuksiin eurooppalaisen näkökulman. ECSF määrittelee 12 työroolia, kuten CISO:n, poikkeamien käsittelijän, kyberturvallisuusauditoijan ja uhkatiedustelun asiantuntijan, sekä niihin liittyvät tehtävät, tiedot ja osaamiset.

1.4 Bloomin taksonomia

Oppimisteorian klassikko, Bloomin taksonomia (van Niekerk & von Solms, 2008), tarjoaa rakenteen osaamisen syvyystasojen määrittelyyn. Se sisältää kuusi tasoa: 1) muistaa, 2) ymmärtää, 3) soveltaa, 4) analysoida, 5) arvioida ja 6) luoda. Osaamiskuvauksissa tasot on yhdistetty kolmeen päätasoon 1–3 (kuvio 1).



Kuvio 1. Bloomin taksonomian jako osaamistasoihin

Kutakin osaamisen tasoa kuvaavat osaamisverbit, jotka on esitetty kuviossa 1. Osaamisverbien valinnassa hyödynnettiin sekä opetuksen yleisiä ohjeistuksia (Kauppila, 2021) että tietotekniikan alalle kehitettyä, Bloomiin perustuvaa verbikirjastoa (ACM Committee for Computing Education in Community Colleges, 2023). Näin varmistettiin pedagogisesti johdonmukaiset ja oikean tasoiset osaamislauseet.

1.5 Viitekehyksien yhdistetty soveltaminen

Kehitystyö rakennettiin JRC-taksonomian (Nai et al., 2022) varaan. Osaamislauseet laadittiin hyödyntämällä NICE- (NICCS, 2025) ja ECSF-viitekehyksiä (ENISA, 2025) niillä osa-alueilla, joissa tarvittiin työrooliperusteista tarkennusta. Kaikille osaamisalueille määriteltiin lisäksi Bloomin taksonomian mukainen taso (1–3) hyödyntäen kirjallisuuden mukaisia verbilistoja (van Niekerk & von Solms, 2008; Kauppila, 2021; ACM Committee for Computing Education in Community Colleges, 2023).

Lopputuloksena saatiin kansainvälisesti yhdenmukaiset, pedagogisesti perustellut ja rakenteeltaan selkeät osaamiskuvaukset opintotarjonnan kehittämiseen.

2. Osaamiskuvaukset eri alojen opiskelijoille

Tässä luvussa on esitetty eri alojen opiskelijoiden kyberturvallisuuden osaamiskuvaukset sekä sellainen kyberturvallisuuden osaaminen, joka jokaisen AMK-opiskelijan tulisi hallita alasta riippumatta.

2.1 Kaikkien AMK-opiskelijoiden kyberturvallisuusosaaminen

Jokaisen AMK-opiskelijan tulee perehtyä kyberturvallisuuteen, jotta hän kykenee toimimaan yhteiskunnassa ja työelämässä vaarantamatta omaa, muiden tai organisaatioiden tietoturvaa. Kaikkien AMK-opiskelijoiden kyberturvallisuuden osaamiseen liittyvät osaamistavoitteet on kuvattu taulukossa 1.

Kaikille AMK-opiskelijoille suunniteltu verkkokurssi *Digiturvastartti - Kaikkien AMK-opiskelijoiden kyberturvallisuusosaaminen* auttaa saavuttamaan asetetut osaamistavoitteet. Kurssin tavoitteena on perehdyttää opiskelija digitaalisen turvallisuuden peruskäsitteisiin ja -käytäntöihin, oppia tunnistamaan digitaalisia riskejä sekä ymmärtää turvallisen toiminnan merkitys niin opiskelussa, työssä kuin arjessa.

Digiturvastartti-kurssin Moodle-pohja
Materiaali on saatavilla suomeksi ja englanniksi.

Taulukko 1. Kaikkien AMK-opiskelijoiden osaamistavoitteet.

JRC-taksonomia	Taso	Osaamiskuvaus
3. Tietoturva ja tietosuoja	1	Opiskelija ymmärtää digitaalisen turvallisuuden, tietoturvan ja tietosuojan periaatteet ja tunnistaa niihin liittyviä riskejä. Opiskelija ymmärtää tiedonhallintaprosessien merkityksen tiedon suojaamisessa ja osaa tarvittaessa ilmoittaa tietoturvahavainnoista organisaation vastuuhenkilöille.
4. Koulutus ja oppiminen	1	Opiskelija ymmärtää kyberturvallisen toiminta- ja työskentelykulttuurin merkityksen ja edistää omalla toiminnallaan organisaation turvallisuutta.
5. Inhimilliset tekijät	1	Opiskelija on tietoinen kyberturvallisuuteen vaikuttavista inhimillisistä tekijöistä, kuten sosiaalisesta manipuloinnista, stressistä, kiireestä ja väsymyksestä, ja osaa kuvailla toimintatapoja näiden riskien minimoimiseksi.
6. Identiteetin hallinta	1	Opiskelija ymmärtää henkilön identiteetin ja sen oikeellisuuden tunnistamisen merkityksen organisaation toiminnassa ja osaa tunnistaa sekä kuvata yleisimpiä tunnistautumistapoja.
8. Lainsäädännölliset näkökulmat	1	Opiskelija ymmärtää tietosuoja- ja immateriaalisäädösten periaatteet. Opiskelija ymmärtää säädösten merkityksen henkilötietojen ja aineettoman omaisuuden käsittelemisessä. Opiskelija ymmärtää säädöksiin liittyvät oikeudet, vastuut ja velvollisuudet.
10. Turvallisuuden hallinta ja hallinnointi	1	Opiskelija ymmärtää digitaalisen turvallisuuden merkityksen organisaation toiminnalle riskienhallinnan näkökulmasta. Opiskelija osaa noudattaa annettuja ohjeita.
14. Teoreettiset perustiedot	1	Opiskelija ymmärtää digitaaliseen turvallisuuteen liittyvää käsitteistöä sekä keskeisiä asiasisältöjä ja hallitsee organisaation kannalta olennaiset taidot.
15. Luottamuksen hallinta ja seuranta	1	Opiskelija osaa arvioida digitaalisen sisällön luotettavuutta yleisellä tasolla. Opiskelija tunnistaa informaatiovaikuttamisen menetelmiä.
16. Tekoäly ja koneoppiminen	1	Opiskelija ymmärtää tekoälyn käyttöön liittyviä tietoturva-, tietosuoja- ja aineistoriskejä. Opiskelija ymmärtää tekoälytyökalujen roolin kyberhyökkäyksissä.

2.2 ICT-alan kyberturvallisuuden osaamistavoitteet

ICT-alan opiskelijoiden osaamistavoitteisiin sisältyy kaikkien AMK-opiskelijoiden kyberturvallisuuden osaamistavoitteet. Lisäksi joidenkin aihealueiden osaamistavoite voi olla perustasoa korkeampi (taso 2 tai 3).

2.2.1 Ohjelmistotekniikka

Ohjelmistotekniikkaan suuntautuneen opiskelijan osaamistavoitteissa painottuvat syvällisempi ymmärrys tietoturvasta ja tietosuojasta, ohjelmisto- ja laiteturvallisuudesta sekä tekoälystä ja koneoppimisesta. Ohjelmistotekniikkaan suuntautuneen opiskelijan kyberturvallisuuden osaamistavoitteet on kuvattu taulukossa 2.

Osaamistavoitteiden saavuttamista tukeva kurssi *Ohjelmistoturvallisuus* on saatavilla materiaaleineen verkossa. Materiaali on saatavilla englanniksi.
Ohjelmistoturvallisuus-kurssin materiaalit.

Taulukko 2. Ohjelmistotekniikkaan suuntautuvan insinööriopiskelijan osaamistavoitteet.

JRC-taksonomia	Taso	Osaamiskuvaus
1. Luotettavuus, auditointi ja sertifiointi	1	Opiskelija ymmärtää auditoinnin merkityksen ja kykenee laatimaan sellaista varten teknisiä dokumentteja sekä osaa tulkita testausten tuloksia.
2. Kryptologia (Kryptografia ja kryptoanalyysi)	1	Opiskelija osaa selittää symmetrisen ja asymmetrisen salauksen toimintaperiaatteen sekä julkisen avaimen infrastruktuurin toiminnan.
3. Tietoturva ja tietosuoja	2	Opiskelija osaa arvioida datan tietosuojaan sekä tietoturvaan liittyviä riskejä sekä suunnitelmallisesti vähentää niitä hyödyntäen datan yksityisyyden suojaamiseen tarkoitettuja tekniikoita (Privacy Enhancing Technologies). Opiskelija osaa arvioida tietoturvaan, datan eheyteen, yksityisyyteen ja rekisteritietojen yhdistelyyn liittyviä riskejä niin, ettei tutkittavien epäsuora tunnistaminen ole mahdollista.
4. Koulutus ja oppiminen	1	Opiskelija ymmärtää tietoisuuden ja oman toimintansa merkityksen yrityksen kyberturvallisuuskulttuurin kehittämisessä.
5. Inhimilliset tekijät	1	Opiskelija osaa varautua käyttäjän manipulointiyrityksiin, joiden tavoitteena on saada käyttäjä paljastamaan salaisia tietoja tai antamaan pääsy salaisiin tietoihin. Opiskelija tiedostaa tietoturvaan ja tietosuojaan liittyvän lainsäädännön sekä eettiset säännöt ja toimintatavat.
6. Identiteetin hallinta	1	Opiskelija ymmärtää identiteetin hallinnan merkityksen tietoturvan ja tietoturvan kannalta ja on perehtynyt erilaisiin käyttäjien tunnistamistapoihin ja käyttöoikeuksien hallintaan.

JRC-taksonomia	Taso	Osaamiskuvaus
7. Tietoturvapoikkeamien hallinta ja tietoturvaloukkauksien tutkinta	1	Opiskelija on perehtynyt tietomurtojen ja poikkeavan verkkoliikenteen tunnistamistekniikoiden perusteisiin ja pystyy tarvittaessa hyödyntämään tekoälyn tarjoamia mahdollisuuksia niiden havaitsemisessa.
8. Lainsäädännölliset näkökulmat	1	Opiskelija tiedostaa tietoturva- ja tietosuojalainsäädännöstä tulevat vaatimukset osana ICT-järjestelmien kehitystyötä.
9. Tietoverkot ja hajautetut järjestelmät	1	Opiskelija tuntee tiedon eheyteen, luottamuksellisuuteen, saatavuuteen ja kiistämättömyyteen liittyvät näkökohdat hajautetuissa järjestelmissä.
10. Turvallisuuden hallinta ja hallinnointi	1	Opiskelija tietää riskienhallinnan merkityksen ja kykenee osallistumaan riskienhallintaan liittyviin suorittaviin tehtäviin.
12. Ohjelmisto- ja laitteistoturvallisuus	2	Opiskelija ymmärtää sumean, staattisen ja dynaamisen testauksen toimintaperiaatteet ICT-kehitystyössä. Opiskelija osaa soveltaa automaattisia järjestelmiä ja työkaluja ohjelmisto- ja laiterajapintojen testauksessa. Opiskelija tiedostaa erilaiset ohjelmistokehittäjiin kohdistuvat hyökkäykset. Opiskelija osaa ylläpitää kehitysympäristöjen tietoturvallisuutta ja tiedostaa turvallisen ohjelmistokehitysympäristön vaatimukset. Opiskelija ymmärtää tietoturvallisuuden merkityksen ohjelmistojen ja laitteiden koko elinkaarelle.
14. Teoreettiset perustiedot	1	Opiskelija tuntee kyberturvallisuuden merkityksen osana yhteiskunnan, yritystoiminnan ja yksilön toimintaa. Hän tietää yleisimpiä kyberuhkia ja niiden mahdollisia vaikutuksia sekä kykenee kehittämään ja ylläpitämään tietouttaan kyberturvallisuuden saralla. Opiskelija tuntee tietosuojan perusteet sekä luottamuksellisuuden, eheyden ja saavutettavuuden käsitteet tietoturvassa ja aitouden ja jäljitettävyyden merkityksen osana sitä.
15. Luottamuksen hallinta ja seuranta	1	Opiskelija ymmärtää luottamuksen ja luottamuksellisuuden käsitteet. Opiskelija tunnistaa niiden merkityksen yrityksen toiminnalle ja luottamuksellisen tiedon roolin yrityksen pääomana.
16. Tekoäly ja koneoppiminen	2	Opiskelija osaa soveltaa tekoälyn tarjoamia mahdollisuuksia kyberturvauhkien sekä haitallisen verkkoliikenteen tunnistamisessa ja torjumisessa. Opiskelija osaa arvioida tekoälymallien sekä datan ja eri datalähteiden luotettavuutta. Opiskelija tunnistaa erilaiset tavat, miten tekoälymalleja tai koulutusdataa voidaan manipuloida, ja osaa tunnistaa manipuloidun datasetin. Opiskelija osaa tunnistaa ja varautua kehittämiensä tekoälymallien manipulointiin liittyviin riskeihin.

2.2.2 IoT-teknologia

IoT-teknologiaan suuntautuneen opiskelijan osaamistavoitteissa korostuu erityinen perehtyneisyys tietoverkkoihin ja hajautettuihin järjestelmiin. IoT-teknologiaan suuntautuneen opiskelijan kyberturvallisuuden osaamistavoitteet on kuvattu taulukossa 4.

Osaamistavoitteiden saavuttamista tukeva kurssi *Cybersecurity Fundamentals* on saatavilla materiaaleineen verkossa. Materiaali on saatavilla englanniksi. Cybersecurity Fundamentals -kurssin materiaalit.

Taulukko 4. IoT-teknologiaan suuntautuvan insinööriopiskelijan osaamistavoitteet.

JRC-taksonomia	Taso	Osaamiskuvaus
1. Luotettavuus, auditointi ja sertifiointi	1	Opiskelija ymmärtää auditoinnin merkityksen ja kykenee laatimaan sellaista varten teknisiä dokumentteja sekä osaa tulkita testausten tuloksia.
2. Kryptologia (Kryptografia ja kryptoanalyysi)	2	Opiskelija osaa symmetrisen ja asymmetrisen salauksen toimintaperiaatteen sekä julkisen avaimen infrastruktuurin toiminnan ja ymmärtää miten julkisen avaimen infrastruktuuria sovelletaan eri käyttökohteissa.
3. Tietoturva ja tietosuoja	2	Opiskelija osaa arvioida datan tietosuojaan sekä tietoturvaan liittyviä riskejä sekä soveltaa teknisiin järjestelmiin niiden vähentämiseen tarkoitettuja menetelmiä.
4. Koulutus ja oppiminen	1	Opiskelija tietää turvallisuuskulttuurin merkityksen organisaation toimintojen ja teknisten järjestelmien suojaamisessa ja ymmärtää jatkuvan koulutuksen ja oppimisen merkityksen osana organisaation turvallisuusstrategiaa.
5. Inhimilliset tekijät	2	Opiskelija osaa varautua käyttäjän manipulointiyrityksiin ja järjestelmien saatavuuteen vaikuttaviin toimenpiteisiin sekä ymmärtää inhimillisten tekijöiden merkityksen organisaation tietoturvalle.
6. Identiteetin hallinta	2	Opiskelija ymmärtää identiteetin hallinnan merkityksen tietoturvan ja tietoturvan kannalta ja osaa soveltaa erilaisia käyttäjien tunnistamistapoja sekä käyttöoikeuksien hallintamenetelmiä.
7. Tietoturvapoikkeamien hallinta ja tietoturvaloukkauksien tutkinta	1	Opiskelija on perehtynyt tietomurtojen ja poikkeavan verkkoliikenteen tunnistamistekniikoiden perusteisiin ja tietomurtojen analysoinnin perusteisiin.
8. Lainsäädännölliset näkökulmat	1	Opiskelija on tietoinen kyberturvallisuuteen keskeisesti vaikuttavasti lainsäädännöstä sekä viranomaistoiminnasta.
9. Tietoverkot ja hajautetut järjestelmät	3	Opiskelija osaa arvioida tiedon eheyteen, luottamuksellisuuteen, saatavuuteen ja kiistämättömyyteen liittyvät näkökohdat hajautetuissa järjestelmissä sekä suunnitella ja suojata niitä.

JRC-taksonomia	Taso	Osaamiskuvaus
10. Turvallisuuden hallinta ja hallinnointi	1	Opiskelija tietää yleisimmät kyberturvallisuuden hallinnan viitekehykset ja vaatimuksenmukaisuuden määrittelyt sekä tuntee penetraatiotestauksessa sovellettavia standardeja.
11. Turvallisuuden mittaaminen	2	Opiskelija osaa analysoida ja arvioida teknisten järjestelmien turvallisuusnäkökohtia.
12. Ohjelmisto- ja laitteistoturvallisuus	2	Opiskelija ymmärtää ohjelmistojen keskeisimmät turvallisuusnäkökohdat ja pystyy testaamaan ohjelmistojen luotettavuutta.
14. Teoreettiset perustiedot	2	Opiskelija osaa kyberturvallisuuden keskeisimmät käsitteet, määritelmät ja perusperiaatteet
15. Luottamuksen hallinta ja seuranta	1	Opiskelija tietää luottamuksenhallinnan peruskäsitteet.
16. Tekoäly ja koneoppiminen	1	Opiskelija tietää tekoälyn tarjoamista mahdollisuuksista kyberturvauhkien sekä haitallisen verkkoliikenteen tunnistamisessa ja torjumisessa sekä ymmärtää, miten tekoälyä voidaan käyttää hyväksi kyberhyökkäyksen eri vaiheissa.
17. Muu osaaminen	3	Opiskelija pystyy suunnittelemaan, tuottamaan ja arvioimaan kyberturvallisia teknisiä ympäristöjä sekä ymmärtää jatkuvan kybertoimintaympäristön seuraamisen merkityksen.

2.2.3 Pilvipalvelut

Pilvipalveluihin suuntautuneen opiskelijan osaamistavoitteissa korostuu erityinen perehtyneisyys tietoverkkoihin ja hajautettuihin järjestelmiin. IoT-teknologiaan suuntautuneen opiskelijan kyberturvallisuuden osaamistavoitteet on kuvattu taulukossa 5.

Taulukko 5. Pilvipalveluihin suuntautuvan insinööriopiskelijan osaamistavoitteet.

JRC-taksonomia	Taso	Osaamiskuvaus
1. Luotettavuus, auditointi ja sertifiointi	1	Opiskelija ymmärtää auditoinnin merkityksen ja kykenee laatimaan sellaista varten teknisiä dokumentteja sekä osaa tulkita testausten tuloksia.
2. Kryptologia (Kryptografia ja kryptoanalyysi)	2	Opiskelija osaa symmetrisen ja asymmetrisen salauksen toimintaperiaatteen sekä julkisen avaimen infrastruktuurin toiminnan ja ymmärtää miten julkisen avaimen infrastruktuuria sovelletaan eri käyttökohteissa.
3. Tietoturva ja tietosuoja	2	Opiskelija osaa arvioida datan tietosuojaan sekä tietoturvaan liittyviä riskejä sekä soveltaa pilvipalvelujärjestelmiin niiden vähentämiseen tarkoitettuja menetelmiä.
4. Koulutus ja oppiminen	1	Opiskelija tietää turvallisuuskulttuurin merkityksen organisaation toimintojen ja teknisten järjestelmien suojaamisessa ja ymmärtää jatkuvan koulutuksen ja oppimisen merkityksen osana organisaation turvallisuusstrategiaa.
5. Inhimilliset tekijät	2	Opiskelija osaa varautua käyttäjän manipulointiyrityksiin ja järjestelmien saatavuuteen vaikuttaviin toimenpiteisiin sekä ymmärtää inhimillisten tekijöiden merkityksen organisaation tietoturvalle.
6. Identiteetin hallinta	2	Opiskelija ymmärtää identiteetin hallinnan merkityksen tietoturvan ja tietoturvan kannalta ja osaa soveltaa erilaisia käyttäjien tunnistamistapoja sekä käyttöoikeuksien hallintamenetelmiä pilvipalveluissa.
7. Tietoturvapoikkeamien hallinta ja tietoturvaloukkauksien tutkinta	1	Opiskelija on perehtynyt tietomurtojen ja poikkeavan verkkoliikenteen tunnistamistekniikoiden perusteisiin ja tietomurtojen analysoinnin perusteisiin.
8. Lainsäädännölliset näkökulmat	1	Opiskelija on tietoinen kyberturvallisuuteen keskeisesti vaikuttavasti lainsäädännöstä sekä viranomaistoiminnasta.
9. Tietoverkot ja hajautetut järjestelmät	3	Opiskelija osaa arvioida tiedon eheyteen, luottamuksellisuuteen, saatavuuteen ja kiistämättömyyteen liittyvät näkökohdat hajautetuissa järjestelmissä sekä suunnitella ja suojata niitä.
10. Turvallisuuden hallinta ja hallinnointi	1	Opiskelija tietää yleisimmät kyberturvallisuuden hallinnan viitekehykset ja vaatimuksenmukaisuuden määrittelyt sekä tuntee kyberturvallisuudessa sovellettavia standardeja.
11. Turvallisuuden mittaaminen	1	Opiskelija osaa analysoida ja arvioida pilvipalvelujen turvallisuusnäkökohtia.
12. Ohjelmisto- ja laitteistoturvallisuus	2	Opiskelija ymmärtää pilvipalvelujen keskeisimmät turvallisuusnäkökohdat ja pystyy arvioimaan palvelujen luotettavuutta.

JRC-taksonomia	Taso	Osaamiskuvaus
14. Teoreettiset perustiedot	2	Opiskelija osaa kyberturvallisuuden keskeisimmät käsitteet, määritelmät ja perusperiaatteet.
15. Luottamuksen hallinta ja seuranta	1	Opiskelija tietää luottamuksenhallinnan peruskäsitteet.
16. Tekoäly ja koneoppiminen	1	Opiskelija tietää tekoälyn tarjoamista mahdollisuuksista kyberturvauhkien sekä haitallisen verkkoliikenteen tunnistamisessa ja torjumisessa sekä ymmärtää, miten tekoälyä voidaan käyttää hyväksi kyberhyökkäyksen eri vaiheissa.
17. Muu osaaminen	3	Opiskelija pystyy suunnittelemaan, tuottamaan ja arvioimaan kyberturvallisia pilvipalveluympäristöjä sekä ymmärtää jatkuvan kybertoimintaympäristön seuraamisen merkityksen.

2.2.4 Tietoverkot

Tietoverkkoihin suuntautuneen opiskelijan osaamistavoitteissa korostuu erityinen perehtyneisyys tietoverkkoihin ja hajautettuihin järjestelmiin. Tietoverkkoihin suuntautuneen opiskelijan kyberturvallisuuden osaamistavoitteet on kuvattu taulukossa 6.

Osaamistavoitteiden saavuttamista tukeva materiaali *Tunkeutumistestauksen laboraatioharjoitukset* on saatavilla verkossa. Materiaali on saatavilla englanniksi. Tunkeutumistestauksen laboraatioharjoitukset -materiaali.

Taulukko 6. Tietoverkkoihin suuntautuvan insinööriopiskelijan osaamistavoitteet.

JRC-taksonomia	Taso	Osaamiskuvaus
1. Luotettavuus, auditointi ja sertifiointi	1–2	Opiskelija osaa tulkita kyberturvallisuuden auditointiraportteja ja tukea auditointiprosesseja. Opiskelijalla on kyky analysoida kyberturvallisuusratkaisujen tehokkuutta ja hän tuntee alan keskeiset standardit. Lisäksi opiskelija osaa arvioida tietoturvan menetelmiä, suorittaa tietoverkkojen turvallisuustarkastuksia ja valmistella verkkoympäristöjä sertifiointia varten, ymmärtäen sertifikaattien merkityksen luotettavuuden osoittamisessa.
2. Kryptologia (Kryptografia ja kryptoanalyysi)	1–2	Opiskelija hallitsee salaamisen perusteet ja osaa käyttää salaustekniikoita tietoverkoissa. Opiskelija tuntee keskeiset salausalgoritmit ja niiden toimintaperiaatteet, ymmärtää digitaalisten sertifikaattien merkityksen tiedonsiirron salauksessa ja osaa ottaa käyttöön salausjärjestelmiä. Opiskelija osaa varmistaa tiedon luottamuksellisuuden ja eheyden käyttämällä eri menetelmiä, arvioida kryptografisia protokollia turvallisuuden ja tehokkuuden näkökulmasta, ja opiskelija ymmärtää digitaalisten allekirjoitusten sekä sertifikaattien roolin identiteettien varmentamisessa.
3. Tietoturva ja tietosuoja	1	Opiskelija hallitsee tietoturvan ja tietosuojan periaatteet, osaa soveltaa niitä tietoverkkojen ja datan suojauksessa ja tiedonsiirron varmistamisessa. Opiskelija tunnistaa henkilötiedot sekä muut arkaluonteiset tiedot ja ymmärtää tarpeen niiden suojaamiselle.
4. Koulutus ja oppiminen	1–2	Opiskelija kykenee osallistumaan kyberturvallisuusharjoitukseen.
5. Inhimilliset tekijät	1	Opiskelija tunnistaa ja tiedostaa tiedonkalastelun sekä sosiaalisen hakkeroinnin merkityksen ja tietää, kuinka ihmisten manipulointi voi altistaa tietoturvariskeille. Opiskelija ymmärtää konfigurointivirheiden vaikutukset kyberturvallisuuteen ja tarpeen suojata järjestelmiä niiltä.
6. Identiteetin hallinta	2	Opiskelija ymmärtää identiteetinhallinnan tärkeyden tietoverkoissa ja tiedon suojaamisessa ja osaa käyttää identiteetinhallintajärjestelmiä käyttäjien tunnistamiseen ja valtuuttamiseen osana tietoverkkojen toimintaa. Opiskelija ymmärtää digitaalisten identiteettien merkityksen. Opiskelija tietää monivaiheisen tunnistautumisen sekä pääsynhallinnan teknisiä menetelmiä ja kykenee arvioimaan niiden vaikutusta.
7. Tietoturvapoikkeamien hallinta ja tietoturvaloukkauksien tutkinta	2	Opiskelija osaa analysoida kyberuhkia ja -hyökkäyksiä, tulkita ja reagoida kyberturvallisuushälytyksiin sekä selvittää kyberhäiriöitä. Opiskelija kykenee keräämään ja yhdistelemään tietoa eri lähteistä, tunnistamaan tietoturvapoikkeamia ja toteuttamaan niiden vaatimia vastatoimia. Opiskelija ymmärtää todisteiden keräämisen ja käsittelyn tärkeyden tietoturvaloukkauksissa ja osaa ylläpitää kyberuhkatapahtumien seurantajärjestelmiä.

JRC-taksonomia	Taso	Osaamiskuvaus
8. Lainsäädännölliset näkökulmat	1	Opiskelija tuntee tietoverkkoihin ja kyberturvallisuuteen liittyvän keskeisen lainsäädännön ja osaa huomioida sen käytännössä. Opiskelija ymmärtää sääntelyn merkityksen ja osaa noudattaa alan suosituksia ja parhaita käytäntöjä.
9. Tietoverkot ja hajautetut järjestelmät	3	Opiskelija osaa suunnitella ja hallita skaalautuvia tietoverkkoja, ymmärtää verkkoteknologioiden ja protokollien toimintaperiaatteet sekä pilvipalveluiden ja virtuaalisoinnin roolin. Opiskelija tuntee kyberturvallisuuden keskeiset elementit, kyberuhat ja niiden torjunnan, osaa käyttää verkon turvaamisen järjestelmiä ja kehittää niitä. Opiskelija osaa analysoida haavoittuvuuksia, kerätä kyberturvallisuustietoa ja soveltaa tietämystään pilvi- ja IoT-järjestelmien sekä muiden hajautettujen järjestelmien ratkaisuissa. Opiskelija osaa testata järjestelmiä ja tietoverkkoa haavoittuvuuksien ja muiden kyberuhkien varalta.
10. Turvallisuuden hallinta ja hallinnointi	2	Opiskelija ymmärtää riskienhallinnan perusteet ja kykenee soveltamaan niitä tietoverkkojen turvallisuuden ylläpitämiseen. Opiskelija osaa määritellä kyberturvallisuuden tilan, osallistua uhkamallinnukseen ja arvioida kyberuhkien vaikutuksia. Opiskelija kykenee kehittämään suojautumis- ja tietoturvasuunnitelmia, ymmärtää tietoturvan hallinnollisia prosesseja ja hallitsee kyberuhkien seurannan ja torjunnan teknisten järjestelmien käytön.
11. Turvallisuuden mittaaminen	2	Opiskelija osaa arvioida tietoverkkojen turvallisuutta. Opiskelija kykenee lukemaan ja hyödyntämään kyberuhka-analyysejä, raportoimaan kyberturvallisuustapahtumista käyttäen erilaisia datalähteitä. Opiskelija osaa arvioida kyberuhkien vaikutuksia, käyttää työkaluja tietoturvaloukkausten havaitsemiseen, analysointiin ja raporttien laadintaan.
12. Ohjelmisto- ja laitteistoturvallisuus	2	Opiskelija hallitsee tietoturvan keskeiset käsitteet, kyberuhkien tunnistamisen ja häiriötilanteiden selvittämisen laitteistoissa. Opiskelija pystyy havaitsemaan sekä raportoimaan järjestelmien poikkeavuuksia. Opiskelija ymmärtää haittaohjelmien toimintaperiaatteita ja osaa käyttää ja ylläpitää niiden havainnointijärjestelmiä ja torjuntakeinoja. Opiskelija tuntee kyberturvallisuustestauksen ja haavoittuvuusanalyysin menetelmiä ja kykenee parantamaan järjestelmien turvallisuutta suorittamalla kyberturvallisuustestauksia ja tekemällä analyysejä. Opiskelija osaa arvioida, käyttöönottaa, ylläpitää, käyttää ja kehittää erilaisia kyberturvallisuusjärjestelmiä.
14. Teoreettiset perustiedot	2	Opiskelija hallitsee kyberturvallisuuden terminologiaa ja pystyy kommunikoimaan asiantuntijoiden kanssa sekä tuottamaan alan raportteja. Opiskelijalla on valmiudet käyttää kyberturvallisuuden periaatteita työssään ja kehittää osaamistaan jatkossa. Opiskelija ymmärtää kyberhyökkääjien toimintatavat ja motiivit ja tuntee syvemmin kyberturvan teoreettisia konsepteja, kuten salaus ja autentikointi, ja osaa soveltaa tietämystään käytännön haasteisiin. Opiskelija tuntee tietoturvamalleja ja -standardeja ja ymmärtää niiden soveltamisen tärkeyden.
15. Luottamuksen hallinta ja seuranta	1	Opiskelija käsittää luottamuksen keskeisen roolin organisaation kyberturvallisuudessa ja osaa analysoida seurantajärjestelmien dataa.
16. Tekoäly ja koneoppiminen	1	Opiskelija tuntee tekoälyn ja koneoppimisen periaatteet ja niiden soveltamisen kyberturvallisuudessa sekä osaa käyttää tekoälyä hyödyntäviä järjestelmiä kyberturvallisuuden analysoinnissa ja parantamisessa.

2.2.5 Tieto- ja viestintätekniikka

Tieto- ja viestintätekniikkaan suuntautuneen opiskelijan osaamistavoitteissa korostuu erityinen perehtyneisyys turvallisuuteen liittyviin aiheisiin. Tieto- ja viestintätekniikan suuntautuneen opiskelijan kyberturvallisuuden osaamistavoitteet on kuvattu taulukossa 7.

Taulukko 7. Tieto- ja viestintätekniikkaan suuntautuvan insinööri- tai tradenomiopiskelijan osaamistavoitteet.

JRC-taksonomia	Taso	Osaamiskuvaus
1. Luotettavuus, auditointi ja sertifiointi	2	Opiskelija ymmärtää luotettavuuden merkityksen kyberturvallisuudessa. Opiskelija tuntee tavallisimmat kyberturvallisuuden auditointimenetelmät ja viitekehykset. Opiskelija osaa suorittaa arviointeja ja analysoida niiden tuloksia sekä toteuttaa toimenpiteitä poikkeamien korjaamiseksi. Opiskelija tuntee tärkeimmät sertifikaatit ja niiden sisällön pääpiirteittäin.
2. Kryptologia (Kryptografia ja kryptoanalyysi)	2	Opiskelija osaa hyödyntää symmetrisen ja asymmetrisen kryptografian ratkaisuja tiedon suojaamisessa sekä siirron, tallennuksen että käytön aikana. Opiskelija tuntee kryptoanalyysin perusteet ja ymmärtää valintojensa vaikutuksen algoritmien ja salausmenetelmien turvallisuuteen ja tehokkuuteen. Opiskelija osaa toteuttaa organisaation avaintenhallinnan ja noudattaa siihen liittyviä politiikkoja sekä hyödyntää julkiseen avaimeen perustuvaa infrastruktuuria oikein. Opiskelija ymmärtää vahvan satunnaisuuden perusteet ja osaa valita tarkoituksenmukaisen generointitavan satunnaisuudelle.
3. Tietosuoja ja yksityisyys	2	Opiskelija ymmärtää tietosuojan ja yksityisyyden merkityksen sekä vaikutuksen organisaatioiden toiminnalle. Opiskelija osaa hyödyntää teknisiä ja hallinnollisia menetelmiä organisaation tietojen suojaamiseen.
4. Koulutus ja oppiminen	2	Opiskelija osaa ohjata organisaatiokulttuuria kyberturvalliseen suuntaan ja ymmärtää toimintakulttuurin merkityksen kyberturvallisuudelle. Opiskelija osaa hyödyntää simulaatioita ja harjoituksia toimintatapojen parantamiseen.
5. Inhimilliset tekijät	2	Opiskelija noudattaa eettisiä toimintatapoja kyberturvallisuuden luomisessa ja ylläpidossa. Opiskelija osaa huomioida luottamuksen merkityksen rakentaessaan kyberturvallisuutta. Opiskelija ymmärtää kyberturvallisuusratkaisujen vaikutuksen saavutettavuuteen ja käytettävyyteen sekä osaa huomioida ne ratkaisuja valitessaan. Opiskelija tunnistaa kyberturvallisuuteen vaikuttavat inhimilliset tekijät kuten sosiaalisen hakkeroinnin ja sisäpiiriväärinkäytökset, ja osaa ryhtyä toimiin niihin liittyvien riskien minimoimiseksi organisaatiossa.
6. Identiteetin hallinta	2	Opiskelija osaa valita organisaation tarpeisiin soveltuvan identiteetinhallintaratkaisun ja ottaa sen käyttöön organisaatiossa. Opiskelija tuntee identiteetinhallinnan tärkeimmät mallit, viitekehykset ja työkalut kuten kertakirjautumisen, federoinnin ja nollaluottamusperiaatteen. Opiskelija tietää, mihin vahva tunnistautuminen perustuu ja tuntee eri todentamistekijät sekä niiden toimintaperiaatteet. Opiskelija tietää identiteetinhallintaa koskevat lait ja tärkeimmät toimialakohtaiset vaatimukset.

JRC-taksonomia	Taso	Osaamiskuvaus
7. Tietoturvapoikkeamien hallinta ja tietoturvaloukkauksien tutkinta	3	Opiskelija osaa rakentaa organisaation poikkeamienhallintaprosessiin soveltuvan tietoturvapoikkeamien hallintajärjestelmän. Opiskelija osaa tehokkaasti hyödyntää ja tarvittaessa muokata tietoturvapoikkeamien hallinnassa hyödynnettäviä työkaluja, kuten lokienhallintaa ja poikkeamienhavainnointijärjestelmiä. Opiskelija osaa toimia järjestelmällisesti poikkeamatilanteessa ja selvittää yleisimpiä poikkeamatilanteita itsenäisesti. Opiskelija tuntee digitaalisen forensiikan toimintatavat ja vaatimukset, ja osaa toimia poikkeamatilanteessa niin, etteivät forensiikan toimintaedellytykset vaarannu.
8. Lainsäädännölliset näkökulmat	1	Opiskelija tuntee kyberturvallisuuteen liittyvän kotimaisen ja EU-lainsäädännön ja osaa toimia lainsäädännön mukaisesti. Opiskelija ymmärtää kyberturvallisuuslainsäädännön vaikutuksen organisaation toimintatapoihin ja prosesseihin.
9. Tietoverkot ja hajautetut järjestelmät	2	Opiskelija tuntee tavallisimmat tietoverkkojen turvallisuusratkaisut kuten palomuurit, segmentoinnin ja mikrosegmentoinnin, hyökkäyksentunnistus- ja estojärjestelmät sekä liikenteensalausratkaisut, ja osaa hyödyntää niitä organisaation tietoliikenteen ja tietojärjestelmien suojaamiseen. Opiskelija tuntee pilvipalvelujen turvallisuusperiaatteet sekä niiden erot paikallisesti toteutettuihin ratkaisuihin. Opiskelija ymmärtää identiteetinhallinnan merkityksen pilvipalvelujen turvaamisessa. Opiskelija tuntee erilaiset paikalliset ja pilvipalveluarkkitehtuurit ja osaa arvioida niiden kyberturvallisuutta sekä etsiä ratkaisuja toteutusten turvallisuuden parantamiseksi.
10. Turvallisuuden hallinta ja hallinnointi	3	Opiskelija osaa suorittaa organisaation kyberturvallisuusriskien arvioinnin ja antaa suosituksia riskitason pienentämiseksi. Opiskelija osaa hyödyntää uhkamallinnusta tietojärjestelmien ja ohjelmistojen turvallisuuden arviointiin ja parantamiseen. Opiskelija tuntee tavallisimmat kyberturvallisuuden hallinnan viitekehykset ja osaa toimia niiden mukaisesti.
11. Turvallisuuden mittaaminen	3	Opiskelija osaa muodostaa ajantasaisen uhkatilannekuvan ja soveltaa sitä organisaation turvallisuuden parantamiseen. Opiskelija osaa tuottaa tilannekuvan muodostamiseen tarvittavaa informaatiota organisaation tietojärjestelmistä ja hallitsee tiedon esittämiseen ja raportointiin käytettävät työkalut.
12. Ohjelmisto- ja laitteistoturvallisuus	3	Opiskelija tuntee turvallisen ohjelmistokehityksen viitekehykset ja tavalliset ohjelmistokehitysprosessit. Opiskelija osaa määritellä kyberturvallisuusvaatimukset ohjelmistoille ja tietojärjestelmille, ja valvoa niiden toteutumista. Opiskelija tuntee ohjelmistojen, laitteiden ja ihmisten välisten rajapintojen heikkoudet ja turvallisuusriskit. Opiskelija osaa toteuttaa pieniä kyberturvallisuuteen liittyviä ohjelmistoprojekteja. Opiskelija tuntee tavallisten ohjelmointikielten ja ohjelmistokomponenttien turvallisuuteen vaikuttavat tekijät ja tunnistaa turvallisuusheikkoudet. Opiskelija osaa koventaa tavallisimmat käyttöjärjestelmät, ohjelmistokomponentit ja tietojärjestelmät. Opiskelija tuntee koventamisen viitekehykset ja menetelmät sekä kykenee hankkimaan ajantasaista tietoa käytössä olevien järjestelmien koventamisvaatimuksista. Opiskelija hallitsee murtautumistestauksen käytännöt ja viitekehykset sekä lainsäädännön ja etiikan. Opiskelija osaa hyödyntää murtautumistestausmenetelmiä ja -työkaluja, ja raportoida testauksen tuloksista eri kohderyhmille. Opiskelija osaa esittää korjaus- ja suojausehdotuksia löydettyihin haavoittuvuuksiin sekä yleisiä parannusohjeita systeemisten ongelmien korjaamiseksi. Opiskelija tuntee haittaohjelmien toimintaperiaatteet, kykenee analysoimaan niiden toimintaa ja tuottamaan tunnisteita ohjelmien havaitsemiseksi organisaation tietojärjestelmissä ja verkoissa.

JRC-taksonomia	Taso	Osaamiskuvaus
13. Steganografia ja vesileimat	1	Opiskelija tuntee tavallisimmat menetelmät tiedon piilottamiseen.
14. Teoreettiset perustiedot	2	Opiskelija ymmärtää kyberturvallisuuden peruskäsitteet kuten CIA-mallin, tiedon luokittelumallit ja alan terminologian ja taksonomiat. Opiskelija osaa soveltaa näitä kaikilla kyberturvallisuuden osa-alueilla.
15. Luottamuksen hallinta ja seurant	2	Opiskelija ymmärtää luottamuksen merkityksen kyberturvallisuudelle ja tuntee tärkeimmät luottamuksenhallinnan mallit ja arkkitehtuurit. Opiskelija ymmärtää luottamuksen yhteiskunnallisen merkityksen. Opiskelija osaa hyödyntää luottamuksenhallinnan ratkaisuja organisaation fyysisten ja digitaalisten järjestelmien kehityksessä.
16. Tekoäly ja koneoppiminen	2	Opiskelija tuntee tavallisimmat koneoppimismallit ja organisaatioissa hyödynnettävät tekoälysovellukset. Opiskelija osaa hyödyntää tekoälyratkaisuja kyberturvallisuuden parantamiseen. Opiskelija tuntee tekoälyyn ja koneoppimiseen kohdistuvat uhat ja hyökkäykset, ja osaa huomioida ne kyberturvallisuuden eri osa-alueilla.
17. Muu osaaminen	2	Opiskelija työskentelee oma-aloitteisesti ja tehokkaasti moniammatillisen tiimin jäsenenä ja osaa kommunikoida kyberturvallisuudesta sujuvasti eri kohderyhmille. Opiskelijalla on riittävät oppimistaidot ja kehittyneet opiskelustrategiat, jotta hän pysyy mukana kyberturvallisuusalan kehityksessä.

2.2.6 Data-analytiikka ja tekoäly

Data-analytiikkaan ja tekoälyyn suuntautuneen opiskelijan osaamistavoitteissa painottuvat syvällisempi ymmärrys tietoturvasta ja tietosuojasta sekä tekoälystä ja koneoppimisesta. Data-analytiikkaan ja tekoälyyn suuntautuneen opiskelijan kyberturvallisuuden osaamistavoitteet on kuvattu taulukossa 3.

Osaamistavoitteiden saavuttamista tukeva kurssi *Cybersecurity and data privacy* on saatavilla materiaaleineen verkossa. Materiaali on saatavilla englanniksi. Cybersecurity and data privacy -kurssin materiaalit.

Taulukko 3. Data-analytiikkaan ja tekoälyyn suuntautuvan insinööriopiskelijan osaamistavoitteet.

JRC-taksonomia	Taso	Osaamiskuvaus
2. Kryptologia (Kryptografia ja kryptoanalyysi)	1	Opiskelija osaa selittää symmetrisen ja asymmetrisen salauksen toimintaperiaatteen sekä julkisen avaimen infrastruktuurin toiminnan.
3. Tietoturva ja tietosuoja	1–2	Opiskelija osaa arvioida datan tietosuojaan sekä tietoturvaan liittyviä riskejä sekä suunnitelmallisesti vähentää niitä hyödyntäen datan yksityisyyden suojaamiseen tarkoitettuja tekniikoita (Privacy Enhancing Technologies). Opiskelija osaa arvioida tietoturvaan, datan eheyteen, yksityisyyteen ja rekisteritietojen yhdistelyyn liittyviä riskejä niin, ettei tutkittavien epäsuora tunnistaminen ole mahdollista.
5. Inhimilliset tekijät	1	Opiskelija osaa varautua käyttäjän manipulointiyrityksiin, joiden tavoitteena on saada käyttäjä paljastamaan salaisia tietoja tai antamaan pääsy salaisiin tietoihin. Opiskelija tiedostaa tietoturvaan ja tietosuojaan liittyvän lainsäädännön sekä eettiset säännöt ja toimintatavat.
6. Identiteetin hallinta	1	Opiskelija ymmärtää identiteetin hallinnan merkityksen tietoturvan ja tietoturvan kannalta ja on perehtynyt erilaisiin käyttäjien tunnistamistapoihin ja käyttöoikeuksien hallintaan.
7. Tietoturvapoikkeamien hallinta ja tietoturvaloukkauksien tutkinta	1	Opiskelija on perehtynyt tietomurtojen ja poikkeavan verkkoliikenteen tunnistamistekniikoiden perusteisiin ja pystyy tarvittaessa hyödyntämään tekoälyn tarjoamia mahdollisuuksia niiden havaitsemisessa.
9. Tietoverkot ja hajautetut järjestelmät	1	Opiskelija tuntee tiedon eheyteen, luottamuksellisuuteen, saatavuuteen ja kiistämättömyyteen liittyvät näkökohdat hajautetuissa järjestelmissä.
16. Tekoäly ja koneoppiminen	2	Opiskelija osaa soveltaa tekoälyn tarjoamia mahdollisuuksia kyberturvauhkien sekä haitallisen verkkoliikenteen tunnistamisessa ja torjumisessa. Opiskelija osaa arvioida tekoälymallien sekä datan ja eri datalähteiden luotettavuutta. Opiskelija tunnistaa erilaiset tavat, miten tekoälymalleja tai koulutusdataa voidaan manipuloida ja osaa tunnistaa manipuloidun datasetin. Opiskelija osaa tunnistaa ja varautua kehittämiensä tekoälymallien manipulointiin liittyviin riskeihin.

2.3 Tekniikan, teollisuuden ja rakentamisen alojen kyberturvallisuuden osaamistavoitteet

Tekniikan, teollisuuden ja rakentamisen opiskelijoiden osaamistavoitteisiin sisältyy kaikkien AMK-opiskelijoiden kyberturvallisuuden osaamistavoitteet. Lisäksi joidenkin aihealueiden osaamistavoite voi olla perustasoa korkeampi (taso 2 tai 3).

2.3.1 Teollisuus

Teollisuuteen ja tuotantoon suuntautuneen opiskelijan osaamistavoitteissa oletetaan, että opiskelijalla on perusosaaminen analogisista ja digitaalisista ohjausjärjestelmistä. Teollisuuteen ja tuotantoon suuntautuneen opiskelijan kyberturvallisuuden osaamistavoitteet on kuvattu taulukossa 8.

Osaamistavoitteiden saavuttamista tukeva materiaali *Automaation kyberturvallisuus* on saatavilla verkossa. Materiaali on saatavilla suomeksi. Automaation kyberturvallisuus -materiaalit.

Taulukko 8. Teollisuuteen suuntautuvan insinööriopiskelijan osaamistavoitteet.

JRC-taksonomia	Taso	Osaamiskuvaus
1. Luotettavuus, auditointi ja sertifiointi	1	Opiskelija ymmärtää auditoinnin merkityksen ja kykenee laatimaan sellaista varten teknisiä dokumentteja sekä osaa tulkita testausten tuloksia. Opiskelija pystyy arviomaan tuotantoympäristön ohjaus- ja tietoliikennejärjestelmän luotettavuutta ja toimintaa häiriö- ja vikatilanteissa.
3. Tietoturva ja tietosuoja	1	Opiskelija kykenee mittaustiedon luotettavuuden määritykseen ja arviointiin alkuperän ja sovelluskohteen perusteella. Opiskelija pystyy arvioimaan huomioimaan AD-muunnoksen vaikutuksen raakatiedon tarkkuuteen. Opiskelija pystyy tunnistamaan henkilötiedot ja huomioimaan tietosuojan vaatimukset laitteiden ja tuotantosolujen ohjausjärjestelmissä.
4. Koulutus ja oppiminen	2	Opiskelija seuraa omaan alaansa liittyviä kyberuhkia ja -ilmiöitä. Opiskelija pystyy arvioimaan erilaisten kyberuhkien ja -ilmiöiden muodostaman riskin oman alansa järjestelmissä. Opiskelija ymmärtää tietoisuuden ja oman toimintansa merkityksen yrityksen kyberturvallisuuskulttuurin kehittämisessä.
5. Inhimilliset tekijät	2	Opiskelija kykenee kriittiseen ajatteluun ja tunnistaa omaan käyttäytymiseensä liittyviä tekijöitä, jotka voivat altistaa hänet sosiaalisen hakkeroinnin kohteeksi.
8. Lainsäädännölliset näkökulmat	1	Opiskelija tuntee ja pystyy huomioimaan omassa toiminnassaan kyberturvallisuuteen, tietoturvaan ja tietosuojaan liittyvät keskeisimmät normit.

JRC-taksonomia	Taso	Osaamiskuvaus
9. Tietoverkot ja hajautetut järjestelmät	2	Opiskelija pystyy yhteistyössä tietoliikenneasiantuntijan kanssa määrittämään toimivan ja turvallisen tietoliikenneverkon, jossa on huomioitu teollisuudessa käytettyjen väylien ja protokollien erityispiirteet.
10. Turvallisuuden hallinta ja hallinnointi	2	Opiskelija pystyy osallistumaan asiantuntijan roolissa tuotantoympäristön ja siihen liittyen järjestelmien riskienarviointiin, dokumentointiin ja toimintaohjeiden kehitykseen. Opiskelija tuntee keskeisimmät kyberturvallisuuteen liittyvät standardit ja yleisimmät käytänteet. Opiskelija tietää riskienhallinnan merkityksen ja kykenee osallistumaan riskienhallintaan liittyviin suorittaviin tehtäviin.
12. Ohjelmisto- ja laitteistoturvallisuus	1	Opiskelija osaa tallentaa ja ylläpitää luotettavasti ohjausjärjestelmiin liittyviä ohjelmistoja.
14. Teoreettiset perustiedot	1	Opiskelija ymmärtää kriittisen infrastruktuurin yhteiskunnallisen merkityksen. Opiskelija pystyy tunnistamaan tuotantoympäristön kriittiset komponentit ja jaetut resurssit. Opiskelija tuntee kyberturvallisuuden merkityksen osana yhteiskunnan, yritystoiminnan ja yksilön toimintaa. Opiskelija tietää yleisimpiä kyberuhkia ja niiden mahdollisia vaikutuksia sekä kykenee kehittämään ja ylläpitämään tietouttaan kyberturvallisuuden saralla. Opiskelija tuntee tietosuojan perusteet sekä luottamuksellisuuden, eheyden ja saavutettavuuden käsitteet tietoturvassa ja aitouden ja jäljitettävyyden merkityksen osana sitä.
15. Luottamuksen hallinta ja seuranta	2	Opiskelija pystyy huomioimaan ja kehittämään tuotantoympäristön fyysistä turvallisuutta.
17. Muu osaaminen	3	Opiskelija ymmärtää ja pystyy ottamaan huomioon reaaliaikaisen tietojenkäsittelyn ja tietoliikenteen periaatteet. Opiskelija osaa arvioida yksittäisten ohjauslaitteen tai tietoliikennekomponentin vika- ja häiriötilanteiden vaikutuksen fyysiseen tuotantojärjestelmään ja yrityksen tuotannonohjaukseen. Opiskelija tuntee teollisuuden tietoliikenneväylien erityispiirteet ja reaaliaikavaatimukset sekä osaa tuoda ne esille. Opiskelija tiedostaa, että tuotantojärjestelmän tietoliikenneverkko on osa kokonaisuutta ja kykenee tekemään sen määritykset yhteystyössä tietoverkkoasiantuntijoiden kanssa.

2.3.2 Terveys- ja hyvinvointiteknologia

Terveys- ja hyvinvointiteknologiaan suuntautuneen opiskelijan osaamistavoitteissa painottuvat syvällisempi ymmärrys auditoinneista sekä turvallisuuden hallinnasta. Terveys- ja hyvinvointiteknologiaan suuntautuneen opiskelijan kyberturvallisuuden osaamistavoitteet on kuvattu taulukossa 9.

Osaamistavoitteiden saavuttamista tukeva materiaali *Kyberturvallisuus lääkinnällisissä laitteissa* on saatavilla verkossa. Materiaali on saatavilla suomeksi. Kyberturvallisuus lääkinnällisissä laitteissa -materiaali.

Taulukko 9. Terveys- ja hyvinvointiteknologiaan suuntautuvan insinööriopiskelijan osaamistavoitteet.

JRC-taksonomia	Taso	Osaamiskuvaus
1. Luotettavuus, auditointi ja sertifiointi	2	Opiskelija ymmärtää kyberturvallisuuteen liittyvien auditointien merkityksen ja kykenee laatimaan sellaista varten oman osaamisalueensa teknisiä dokumentteja sekä osaa tulkita testausten tuloksia.
3. Tietoturva ja tietosuoja	1	Opiskelija tuntee tietoturvan peruskonseptit kuten tiedon eheyden, luottamuksellisuuden ja saatavuuden merkityksen. Opiskelija ymmärtää tietojen luokittelun periaatteet ja merkityksen, osaa suojata omia tietoteknisiä laitteitaan yleisimmillä keinoilla. Opiskelija kykenee tunnistamaan yrityksen luottamuksellisen ja tärkeän tiedon sekä tietää tietosuojan keskeiset periaatteet ja merkityksen henkilötietojen suojauksessa.
4. Koulutus ja oppiminen	1	Opiskelija ymmärtää kyberturvallisuustietoisuuden ja oman toiminnan merkityksen yrityksen kyberturvallisuuskulttuurissa. Opiskelija kykenee seuraamaan omaan alaansa liittyviä kyberuhkia ja -ilmiöitä ja osallistumaan työpaikkansa kyberturvallisen toimintaympäristön kehittämiseen.
5. Inhimilliset tekijät	1	Opiskelija kykenee kriittiseen ajatteluun ja tunnistaa omaan käyttäytymiseensä liittyviä tekijöitä, jotka voivat altistaa hänet sosiaalisen hakkeroinnin kohteeksi. Opiskelija osaa toimia eettisesti tietoturvaan liittyvien asioiden kanssa omassa työympäristössään.
6. Identiteetin hallinta	1	Opiskelija ymmärtää henkilön identiteetin ja sen oikeellisuuden tunnistamisen merkityksen organisaation toiminnassa ja osaa tunnistaa sekä kuvata yleisimpiä tunnistautumistapoja.
7. Tietoturvapoikkeamien hallinta ja tietoturvaloukkauksien tutkinta	1	Opiskelija kykenee havaitsemaan perustasoisen kyberturvallisuushäiriön työskentely-ympäristössään ja raportoimaan sen eteenpäin.
8. Lainsäädännölliset näkökulmat	1	Opiskelija tietää oman alansa kyberturvallisuuteen liittyvät keskeiset normit.

JRC-taksonomia	Taso	Osaamiskuvaus
9. Tietoverkot ja hajautetut järjestelmät	1	Opiskelija ymmärtää yleisellä tasolla tietoverkkojen toiminta-periaatteet, kriittisten verkkoyhteyksien merkityksen ja näiden turvallisuuteen liittyviä periaatteita ja käytäntöjä.
10. Turvallisuuden hallinta ja hallinnointi	2	Opiskelija tietää standardeja, suosituksia ja parhaita käytänteitä riskinhallintaan. Opiskelija osaa tunnistaa, arvioida ja dokumentoida kyberturvallisuuteen liittyviä uhkia ja haavoittuvuuksia.
12. Ohjelmisto- ja laitteistoturvallisuus	1	Opiskelija ymmärtää järjestelmien kyberturvallisuusriskejä, tuntee kyberturvallisuuteen liittyviä työkaluja ja teknologioita, pystyy määrittelemään kyberturvallisuusvaatimuksia järjestelmille sekä osaa kehittää kyberturvallisuuteen liittyviä käyttötapauksia.
14. Teoreettiset perustiedot	1	Opiskelija tuntee kyberturvallisuuden merkityksen osana yhteiskunnan, yritystoiminnan ja yksilön toimintaa. Hän tietää yleisimpiä kyberuhkia ja niiden mahdollisia vaikutuksia sekä kykenee kehittämään ja ylläpitämään tietouttaan kyberturvallisuuden saralla.
15. Luottamuksen hallinta ja seuranta	1	Opiskelija ymmärtää luottamuksen ja luottamuksellisuuden käsitteet. Hän tunnistaa niiden merkityksen yrityksen toiminnalle ja luottamuksellisen tiedon roolin yrityksen pääomana.
16. Tekoäly ja koneoppiminen	1	Opiskelija ymmärtää tekoälyn käyttöön liittyviä tietoturva-, tietosuoja- ja aineistoriskejä. Hän ymmärtää tekoälytyökalujen roolin kyberhyökkäyksissä.

2.3.3 Rakentaminen

Rakentamiseen suuntautuneen opiskelijan osaamistavoitteissa painottuvat syvällisempi ymmärrys tietoturvasta ja tietosuojasta. Rakentamiseen suuntautuneen opiskelijan kyberturvallisuuden osaamistavoitteet on kuvattu taulukossa 10.

Osaamistavoitteiden saavuttamista tukeva materiaali *Managing and Sharing Construction Data with Security-minded Approach* on saatavilla verkossa. Materiaali on saatavilla englanniksi. Managing and Sharing Construction Data with Security-minded Approach -materiaali.

Taulukko 10. Rakentamiseen suuntautuvan insinööriopiskelijan osaamistavoitteet.

JRC-taksonomia	Taso	Osaamiskuvaus
1. Luotettavuus, auditointi ja sertifiointi	1	Opiskelija ymmärtää auditoinnin merkityksen ja kykenee laatimaan sellaista varten teknisiä dokumentteja sekä osaa tulkita testausten tuloksia.
2. Kryptologia (Kryptografia ja kryptoanalyysi)	1	Opiskelija tuntee kryptologian periaatteita ja käytäntöjä sekä osaa selittää symmetrisen ja asymmetrisen salauksen toimintaperiaatteen sekä julkisen avaimen infrastruktuurin toiminnan.
3. Tietoturva ja tietosuoja	1	Opiskelija ymmärtää tietojen luokittelun periaatteet ja merkityksen, osaa suojata omia tietoteknisiä laitteitaan yleisimmillä keinoilla ja tietää tietosuojan keskeiset periaatteet yleisellä tasolla. Opiskelija tunnistaa tyypilliset tietosisältöjen sensitiivisyyteen liittyvät tekijät (luottamuksellisuus, immateriaalioikeudet, yksityisyydensuoja, fyysinen turvallisuus) ja osaa huomioida kyberturvallisuuden tietoja käsiteltäessä.
4. Koulutus ja oppiminen	1	Opiskelija ymmärtää kyberturvallisuustietoisuuden ja -kulttuurin merkityksen ja oman toimintansa merkityksen siinä. Opiskelija tuntee kyberturvallisuuteen liittyvät roolit ja vastuut omassa organisaatiossaan ja organisaatioiden välisissä hankkeissa sekä osaa näissä edistää kyberturvallisuuskulttuuria. Opiskelija pystyy seuraamaan rakentamisalaan liittyviä kyberuhkia ja -ilmiöitä.
5. Inhimilliset tekijät	1	Opiskelija kykenee kriittiseen ajatteluun ja tunnistaa omaan käyttäytymiseensä liittyviä tekijöitä, jotka voivat altistaa hänet sosiaalisen hakkeroinnin kohteeksi. Opiskelija osaa toimia eettisesti kyberturvallisuuteen liittyvien asioiden kanssa.
7. Tietoturvapoikkeamien hallinta ja tietoturvaloukkauksien tutkinta	1	Opiskelija tuntee tietoturvapoikkeamiin reagointiin ja niiden hallintaan liittyvät standardinmukaiset prosessit ja osaa niitä noudattaa sekä pystyy osallistumaan poikkeamien tutkintaan.
8. Lainsäädännölliset näkökulmat	1	Opiskelija tuntee yleisimmät, kiinteistö- ja rakennusalan näkökulmasta relevantit, kyberturvallisuuteen liittyvät oikeudelliset näkökulmat.

JRC-taksonomia	Taso	Osaamiskuvaus
9. Tietoverkot ja hajautetut järjestelmät	1	Opiskelija tuntee tiedon eheyteen, luottamuksellisuuteen, saatavuuteen ja kiistämättömyyteen liittyvät näkökohdat hajautetuissa järjestelmissä.
10. Turvallisuuden hallinta ja hallinnointi	1	Opiskelija tietää riskienhallinnan merkityksen ja kykenee osallistumaan riskienhallintaan liittyviin suorittaviin tehtäviin.
14. Teoreettiset perustiedot	1	Opiskelija tuntee kyberturvallisuuden merkityksen kiinteistö- ja rakennusalan toiminnassa. Hän tietää yleisimpiä kyberuhkia ja niiden mahdollisia vaikutuksia sekä kykenee kehittämään ja ylläpitämään tietouttaan kyberturvallisuuden saralla. Hän tuntee tietosuojan perusteet sekä luottamuksellisuuden, eheyden ja saavutettavuuden käsitteet tietoturvassa sekä aitouden ja jäljitettävyyden merkityksen osana sitä.
15. Luottamuksen hallinta ja seuranta	1	Opiskelija ymmärtää luottamuksen ja luottamuksellisuuden käsitteet. Hän tunnistaa niiden merkityksen yrityksen toiminnalle ja luottamuksellisen tiedon roolin yrityksen pääomana.
16. Tekoäly ja koneoppiminen	1	Opiskelija ymmärtää tekoälyn ja koneoppimisen käyttämiseen liittyvät riskit kiinteistö- ja rakennusalan tehtävissä.

2.3.4 Robotiikka

Robotiikkaan suuntautuneen opiskelijan osaamistavoitteissa korostuu erityinen perehtyneisyys tietoverkkoihin ja hajautettuihin järjestelmiin. Robotiikkaan suuntautuneen opiskelijan kyberturvallisuuden osaamistavoitteet on kuvattu taulukossa 11.

Osaamistavoitteiden saavuttamista tukeva kurssi *Robotiikan kyberturvallisuus* on saatavilla materiaaleineen verkossa. Materiaali on saatavilla suomeksi. Robotiikan kyberturvallisuus -kurssin materiaalit.

Taulukko 11. Robotiikkaan suuntautuvan insinööriopiskelijan osaamistavoitteet.

JRC-taksonomia	Taso	Osaamiskuvaus
1. Luotettavuus, auditointi ja sertifiointi	1	Opiskelija ymmärtää auditoinnin merkityksen ja kykenee laatimaan sellaista varten teknisiä dokumentteja sekä osaa tulkita testausten tuloksia.
2. Kryptologia (Kryptografia ja kryptoanalyysi)	2	Opiskelija osaa symmetrisen ja asymmetrisen salauksen toimintaperiaatteen sekä julkisen avaimen infrastruktuurin toiminnan ja ymmärtää miten julkisen avaimen infrastruktuuria sovelletaan eri käyttökohteissa.
3. Tietoturva ja tietosuoja	2	Opiskelija osaa arvioida datan tietosuojaan sekä tietoturvaan liittyviä riskejä sekä soveltaa teknisiin järjestelmiin niiden vähentämiseen tarkoitettuja menetelmiä.
4. Koulutus ja oppiminen	1	Opiskelija tietää turvallisuuskulttuurin merkityksen organisaation toimintojen ja teknisten järjestelmien suojaamisessa ja ymmärtää jatkuvan koulutuksen ja oppimisen merkityksen osana organisaation turvallisuusstrategiaa.
5. Inhimilliset tekijät	2	Opiskelija osaa varautua käyttäjän manipulointiyrityksiin ja järjestelmien saatavuuteen vaikuttaviin toimenpiteisiin sekä ymmärtää inhimillisten tekijöiden merkityksen organisaation tietoturvalle.
6. Identiteetin hallinta	2	Opiskelija ymmärtää identiteetin hallinnan merkityksen tietoturvan ja tietoturvan kannalta ja osaa soveltaa erilaisia käyttäjien tunnistamistapoja sekä käyttöoikeuksien hallintamenetelmiä.
7. Tietoturvapoikkeamien hallinta ja tietoturvaloukkauksien tutkinta	1	Opiskelija on perehtynyt tietomurtojen ja poikkeavan verkkoliikenteen tunnistamistekniikoiden perusteisiin ja tietomurtojen analysoinnin perusteisiin.
8. Lainsäädännölliset näkökulmat	1	Opiskelija on tietoinen kyberturvallisuuteen keskeisesti vaikuttavasti lainsäädännöstä sekä viranomaistoiminnasta.
9. Tietoverkot ja hajautetut järjestelmät	3	Opiskelija osaa arvioida tiedon eheyteen, luottamuksellisuuteen, saatavuuteen ja kiistämättömyyteen liittyvät näkökohdat hajautetuissa järjestelmissä sekä suunnitella ja suojata niitä.

JRC-taksonomia	Taso	Osaamiskuvaus
10. Turvallisuuden hallinta ja hallinnointi	1	Opiskelija tietää yleisimmät kyberturvallisuuden hallinnan viitekehykset ja vaatimuksenmukaisuuden määrittelyt sekä tuntee penetraatiotestauksessa sovellettavia standardeja.
11. Turvallisuuden mittaaminen	2	Opiskelija osaa analysoida ja arvioida teknisten järjestelmien turvallisuusnäkökohtia.
12. Ohjelmisto- ja laitteistoturvallisuus	2	Opiskelija ymmärtää ohjelmistojen keskeisimmät turvallisuusnäkökohdat ja pystyy testaamaan ohjelmistojen luotettavuutta.
14. Teoreettiset perustiedot	2	Opiskelija osaa kyberturvallisuuden keskeisimmät käsitteet, määritelmät ja perusperiaatteet.
15. Luottamuksen hallinta ja seuranta	1	Opiskelija tietää luottamuksenhallinnan peruskäsitteet.
16. Tekoäly ja koneoppiminen	1	Opiskelija tietää tekoälyn tarjoamista mahdollisuuksista kyberturvauhkien sekä haitallisen verkkoliikenteen tunnistamisessa ja torjumisessa sekä ymmärtää, miten tekoälyä voidaan käyttää hyväksi kyberhyökkäyksen eri vaiheissa.
17. Muu osaaminen	3	Opiskelija pystyy suunnittelemaan, tuottamaan ja arvioimaan kyberturvallisia teknisiä ympäristöjä sekä ymmärtää jatkuvan kybertoimintaympäristön seuraamisen merkityksen.

2.4 Terveys- ja hyvinvointialan kyberturvallisuuden osaamistavoitteet

Terveys- ja hyvinvointialan opiskelijoiden osaamistavoitteisiin sisältyy kaikkien AMK-opiskelijoiden kyberturvallisuuden osaamistavoitteet. Lisäksi joidenkin aihealueiden osaamistavoite voi olla perustasoa korkeampi (taso 2). Terveys- ja hyvinvointialan opiskelijan kyberturvallisuuden osaamistavoitteet on kuvattu taulukossa 12.

Osaamistavoitteiden saavuttamista tukeva opintokokonaisuus *Sosiaali- ja terveysalojen kyberturvallisuus* on saatavilla materiaaleineen verkossa. Materiaali on saatavilla suomeksi ja englanniksi. Sosiaali- ja terveysalojen kyberturvallisuus -opintokokonaisuuden materiaalit.

Taulukko 12. Terveys- ja hyvinvointialan opiskelijan osaamistavoitteet.

JRC-taksonomia	Taso	Osaamiskuvaus
3. Tietoturva ja tietosuoja	1	Opiskelija tuntee henkilökohtaisen terveystiedon suojaamisen standardit, kuten Personal Health Information (PHI), GDPR ja IPR-vastineet. Opiskelija tuntee ja ymmärtää sisäisten ja ulkoisten kumppanien välisen raportoinnin säädökset. Opiskelija tuntee ja ymmärtää tietosuojavaikutusten arviointistandardit, menetelmät ja viitekehykset.
4. Koulutus ja oppiminen	1–2	Opiskelija tuntee ja ymmärtää yrityksen kyberturvallisuusharjoittelun politiikat, prosessit, toimintatavat ja järjestelmät. Opiskelija tuntee kyberuhat ja järjestelmähaavoittuvuudet. Opiskelija osaa hyödyntää olemassa olevia kyberturvallisuusharjoitusresursseja. Opiskelija pystyy soveltamaan perehdytys- ja oppimateriaalia kyberturvallisuuteen liittyen.
5. Inhimilliset tekijät	1–2	Opiskelija ymmärtää fyysisiä ja fysiologisia käyttäytymismalleja, jotka voivat viitata epäilyttävään tai poikkeavaan toimintaan. Opiskelija osaa toimia eettisesti ja itsenäisesti ilman sisäisten tai ulkoisten toimijoiden painetta.
6. Identiteetin hallinta	1	Opiskelija tuntee tunnistus-, valtuutus- ja kulunvalvontamenetelmät, mukaan lukien biometriset tunnisteet.
7. Tietoturvapoikkeamien hallinta ja tietoturvaloukkauksien tutkinta	1	Opiskelija tuntee yrityksessä käytettävät kyberpoikkeamien hallintajärjestelmät, roolit ja vastuut. Opiskelija tuntee ja ymmärtää kyberoperaatioiden kriisitoiminnan ja niiden aikaherkkyyden. Opiskelija tuntee yleisimmät haittaohjelmatyypit.
8. Lainsäädännölliset näkökulmat	1	Opiskelija tuntee ja ymmärtää kyberturvallisuuteen ja yksityisyyteen liittyvän lainsäädännön, säädökset, politiikat, prosessit ja etiikan oman alansa näkökulmasta.
10. Turvallisuuden hallinta ja hallinnointi	1	Opiskelija tuntee ja ymmärtää luottamuksellisuuden, eheyden ja saatavuuden periaatteet ja tarpeet.
15. Luottamuksen hallinta ja seuranta	1	Opiskelija tuntee ja ymmärtää työelämässä käytettävien viestintäkanavien ja ohjelmistojen tarkoituksen.
17. Muu osaaminen	1	Opiskelija ymmärtää tietokoneen peruskäyttöä ja osaa hakea tietoa.

2.5 Kaupan ja hallinnon alan kyberturvallisuuden osaamistavoitteet

Kaupan ja hallinnon alan opiskelijoiden osaamistavoitteisiin sisältyy kaikkien AMK-opiskelijoiden kyberturvallisuuden osaamistavoitteet. Kaupan ja hallinnon alan opiskelijan kyberturvallisuuden osaamistavoitteet on kuvattu taulukossa 13.

Taulukko 13. Kaupan ja hallinnon alan opiskelijan osaamistavoitteet.

JRC-taksonomia	Taso	Osaamiskuvaus
2. Kryptologia (Kryptografia ja kryptoanalyysi)	1	Opiskelija ymmärtää symmetrisen ja asymmetrisen salauksen toimintaperiaatteen sekä julkisen avaimen infrastruktuurin toiminnan.
3. Tietoturva ja tietosuoja	1	Opiskelija tunnistaa datan tietosuojaan sekä tietoturvaan liittyviä riskejä sekä tietää datan yksityisyyden suojaamiseen tarkoitettuja tekniikoita (Privacy Enhancing Technologies). Opiskelija tunnistaa tietoturvaan, datan eheyteen, yksityisyyteen ja rekisteritietojen yhdistelyyn liittyviä riskejä, että tutkittavien epäsuora tunnistaminen ei olisi mahdollista.
4. Koulutus ja oppiminen	1	Opiskelija osaa kehittää organisaation kyberturvatietoisuutta sekä edistää toiminnallaan organisaation tietoturvakulttuuria.
5. Inhimilliset tekijät	1	Opiskelija osaa varautua ja reagoida käyttäjän manipulointiyrityksiin, joiden tavoitteena on saada käyttäjä paljastamaan salaisia tietoja tai antamaan pääsy salaisiin tietoihin. Opiskelija tiedostaa tietoturvaan ja tietosuojaan liittyvän lainsäädännön sekä eettiset säännöt ja toimintatavat.
6. Identiteetin hallinta	1	Opiskelija ymmärtää identiteetin hallinnan merkityksen tietoturvan ja tietoturvan kannalta ja on perehtynyt erilaisiin käyttäjien tunnistamistapoihin ja käyttöoikeuksien hallintaan.
7. Tietoturvapoikkeamien hallinta ja tietoturvaloukkauksien tutkinta	1	Opiskelija tietää miten toimia havaitessaan tietoturvapoikkeaman.
8. Lainsäädännölliset näkökulmat	1	Opiskelija osaa kuvata kyberturvallisuutta ja immateriaalioikeuksia koskeviin tilanteisiin soveltuvat lait ja säädökset sekä eettiset näkökohdat.
14. Teoreettiset perustiedot	1	Opiskelija osaa kuvata liiketoiminnan vaikutusanalyysin kuten Business Impact Analysis (BIA)-mallin, kerroksellisen suojauksen, tietosuojan ja tiedon luokittelun periaatteet. Opiskelija osaa selittää omaan toimialaansa liittyvät yleisimmät kyberuhkat ja niihin liittyvät liiketoimintariskit.
15. Luottamuksen hallinta ja seuranta	1	Opiskelija tunnistaa olevansa sosiaalisen manipuloinnin kohteena ja hän osaa toimia tilanteen vaatimalla tavalla. Opiskelija tunnistaa epäluotettavat tietolähteet toimiessaan digitaalisessa toimintaympäristössä. Opiskelija ymmärtää tietosuojaan liittyvät oikeudet, vastuut ja velvollisuudet. Opiskelija ymmärtää oman roolinsa merkityksen ja vastuun organisaation tietoturvakulttuurin osana.
17. Muu osaaminen	1	Opiskelija osaa arvioida tekoälymallien sekä datan ja eri datalähteiden luotettavuutta. Opiskelija tunnistaa toimitusketjuun liittyvät kyberturvallisuusriskit.

Lähteet

ACM Committee for Computing Education in Community Colleges. (2023). Bloom's for computing: Enhancing Bloom's revised taxonomy with verbs for computing disciplines. Association for Computing Machinery. https://doi.org/10.1145/3587276

European Union Agency for Cybersecurity. (2025). European cybersecurity skills framework – Role profiles. Haettu 2.4.2026 osoitteesta https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

Kauppila, A. (2021). Osaamistavoitteet – avain hyvään oppimiseen. Karelia Ammattikorkeakoulu. Haettu 2.4.2026 osoitteesta https://vasu.karelia.fi/2021/02/15/osaamistavoitteet-avain-hyvaan-oppimiseen/

Nai, F. I., Hernandez, R. J. L., & Neisse, R. (2022). JRC cybersecurity taxonomy. European Commission, Joint Research Centre. https://publications.jrc.ec.europa.eu/repository/handle/JRC111441

National Initiative for Cybersecurity Careers and Studies. (2025). NICE workforce framework for cybersecurity (NICE Framework). Haettu 2.4.2026 osoitteesta https://niccs.cisa.gov/tools/nice-framework

van Niekerk, J., & von Solms, R. (2008). Bloom's taxonomy for information security education. Haettu 2.4.2026 osoitteesta https://www.academia.edu/1951994/Blooms_taxonomy_for_information_security_education