OT-ympäristöjen kyberuhkiin varautumisen kehittämisen esiselvitys

Huoltovarmuusorganisaatio
Digipooli

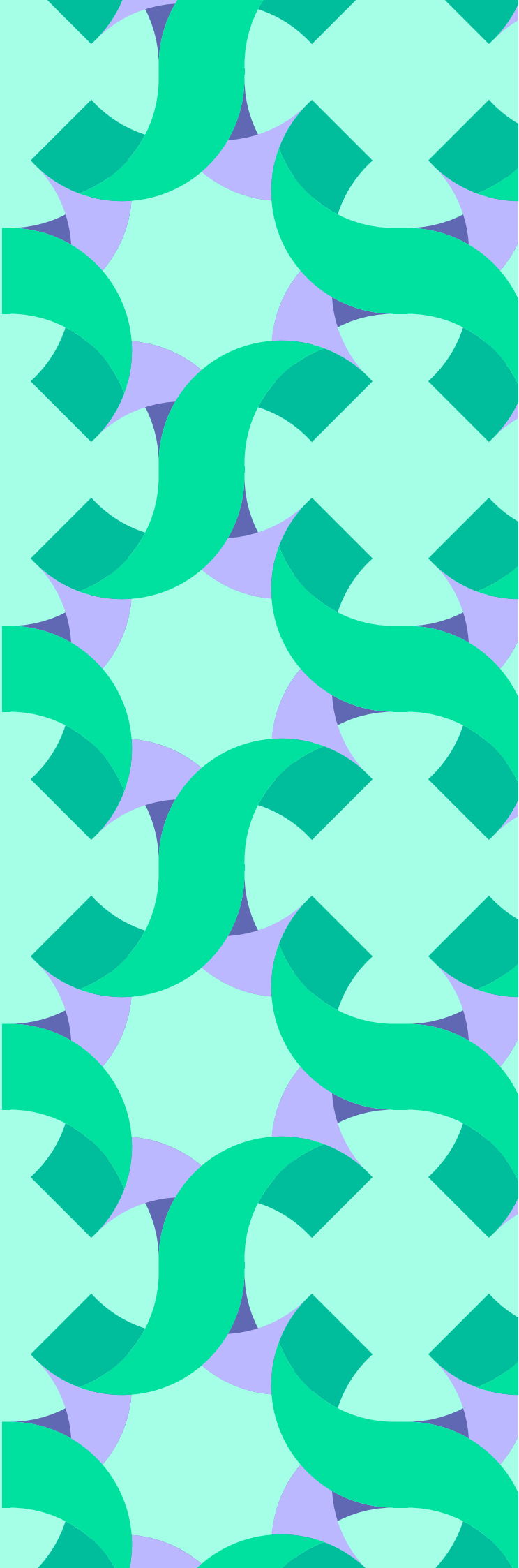
Huoltovarmuusorganisaatio
Digipooli

www.huoltovarmuuskeskus.fi

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa. Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta.

Julkaisija:
Huoltovarmuusorganisaatio, Digipooli.
Huoltovarmuusorganisaatio on verkosto, joka työskentelee yhdessä Suomen toimintakyvyn ja sen edellyttämän huoltovarmuuden hyväksi. Siihen kuuluvat Huoltovarmuuskeskus ja sen hallitus, Huoltovarmuusneuvosto sekä eri toimialojen sektorit ja poolit.

Laatinut: Deloitte Oy
Taitto: Deloitte Oy
Julkaisuvuosi: 2025
ISBN: 978-952-7470-38-1



Sisältö

1. Johdon yhteenveto

OT-ympäristöjen (Operational Technology) kyberturvallisuus on noussut kriittiseksi tekijäksi yrityksien toiminnan jatkuvuuden ja taloudellisen vakauden varmistamisessa. OT-ympäristöllä viitataan laitteisiin, ohjelmistoihin ja järjestelmiin, jotka ohjaavat ja valvovat fyysisiä prosesseja erilaisissa teollisuus- ja infrastruktuuriympäristöissä. Häiriöt näissä järjestelmissä voivat johtaa merkittäviin tuotannon toiminnan keskeytyksiin ja suuriin taloudellisiin menetyksiin. Tuotannon jatkuvuuden kannalta on ratkaisevan tärkeää, että OT-ympäristöjen jatkuvuus ja turvallisuus taataan myös kyberturvallisuusuhkien varalta.

Käytännön tasolla OT-kyberturvallisuuden toteuttamisen haasteena ovat usein OT-ympäristöjen tekniset ominaisuudet, kuten laitteiden pitkät käyttöiät, järjestelmien yksityiskohtaisuus ja eristyneisyys muista järjestelmistä sekä tarve keskeytymättömään toimintaan. OT-ympäristöjen erityispiirteiden vuoksi tietoturvakontrollien implementoiminen voi vaatia räätälöityjä erikoisratkaisuita, jotka ovat todennäköisesti tavallisia IT-toteutuksia kalliimpia ja monimutkaisempia toteuttaa. Tässä esiselvityksessä tarkasteltiin näiden haasteiden juurisyitä ja koostettiin suosituksia elinkeinoelämälle parannustoimenpiteiksi. Näiden toimenpiteiden avulla voidaan luoda pohja OT-kyberturvallisuuden hallinnalle ja kehitykselle ja varmistaa liiketoiminnan jatkuvuus ja kilpailukyvyn kyberuhkien kasvaessa.

Esiselvityksessä tarkasteltuja toimialoja olivat teollisuus, vesihuolto, energia, elintarviketeollisuus, kauppa ja jakelu, logistiikka, satamat ja merenkulku sekä terveydenhuolto, ja kaikkien toimialojen OT-kyberturvallisuuden hallinnan kokonaiskypsyystasot jäivät hyvän perustason alapuolelle. Samat haasteet nousivat esiin kaikilla toimialoilla ja niiden juurisyyt linkittyvät ja vaikuttavat toisiinsa. **Keskeiset haasteet ja juurisyyt OT-kyberturvallisuuden hallinnan kehittämisessä:**

- Kyberturvallisuuden hallintamalleissa ja prosesseissa puutteellinen OT-ympäristöjen kyberturvallisuuden huomiointi sekä haasteena sille asetettujen vaatimusten käytäntöön vienti.
- Resurssit ja budjetti koetaan riittämättömiksi OT-kyberturvallisuuden kehityksen tarpeisiin. Liian pienet resurssit näkyvät juurisyynä lähes kaikille osa-alueille.
- OT-kyberturvallisuuden tason kehittämisessä kyvykkyyksien seurannan ja raportoinnin puute korostuu. Ilman mitattuja havaintoja oman organisaation nykytilan tasosta ei voida arvioida kehittymistarpeita tai sitä, meneekö kehitys oikeaan suuntaan.
- Roolit ja vastuut ovat heikosti määriteltyjä. Jos OT jää turvallisuusasioiden suhteen määrittämättömään väliin, ei voida olettaa, että sitä kehitettäisiin määrätietoisesti.
- OT-ympäristöjen kyberriskejä tunnistetaan ja tiedostetaan, mutta systemaattista OT-kyberriskien raportointia ja omistajuuden määritystä tehdään vähemmän.
- Kolmansien osapuolien riskienhallinta korostuu selvityksessä ja se koetaan haastavana kokonaisuutena. Jos toimitusketjuihin liittyviä riskejä ei ole systemaattisesti tunnistettu, niitä ei voida hallita tehokkaasti, jos ollenkaan.
- OT-kyberturvallisuus on vähäisesti huomioitu kolmansien osapuolien sopimuksissa ja OT-ympäristöjen hankintavaiheessa, ja turvavaatimukset ovat puutteellisia jo OT-ympäristöjen kehittäessä.
- Henkilöstön osaaminen OT-kyberturvallisuuteen koetaan yleisesti riittämättömäksi. Tämä ei välttämättä johdu henkilöiden kyvyistä sellaisenaan tai siitä, että asiaa ei koettaisi tärkeäksi, vaan linkittyy resursseihin ja budjettiin.
- OT-ympäristöjen kyberturvallisuuden teknisen valvonnan toteuttaminen on haasteellista. Teknisiä tietoturvaratkaisuja ei ole yhtä laajasti ja helposti saatavilla kuin perinteisessä IT:ssä. Kyberturvallisuuden teknisen valvonnan ja monitoroinnin toteuttaminen vaatii usein soveltamista, osaamista ja asian huomioimista jo hankintavaiheessa.

Keskeiset suositukset elinkeinoelämälle: OT-kyberturvallisuuden asettaminen korkeammalle prioriteetille tuotannon jatkuvuuden varmistamiseksi on suositeltavaa kaikille toimialojen yrityksille, mihin yrityksen johdon tuki on välttämätöntä.

- Yrityksen lähtötason huomioiden on suositeltavaa aloittaa OT-ympäristöjen omaisuuden kartoituksella ja liiketoiminnan kannalta kriittisten kohteiden tunnistamisella.
- Kyberturvallisuus tulisi olla kiinteä osa tuotannon hallintaa, jotta se toimii saumattomasti osana tuotannollista järjestelmää ja tukee tuotannon tavoitteita osana päivittäistä toimintaa. Määrittelemällä ja jalkauttamalla selkeä OT-kyberturvallisuuden hallintamalli voidaan ratkaista haasteita, jotka liittyvät epäselviin rooleihin ja vastuisiin sekä operatiivisella että strategisella tasolla, tavoitteelliseen kehittämiseen sekä resursointiin ja budjetointiin.
- Toimivan hallintamallin luominen edellyttää systemaattista lähestymistapaa, jossa oikeat sidosryhmät tunnistetaan ja sitoutetaan yhteisten tavoitteiden saavuttamiseen. Näin voidaan varmistua paremmin OT-ympäristöjen kyberturvallisuusvaatimusten jalkauttamisen ja käytäntöön viennin onnistumisesta.
- On suositeltavaa asettaa OT-kyberturvallisuuden parantamiselle selkeät ja mitattavat tavoitteet, jotka tukevat organisaation liiketoimintatavoitteita. Investoinnit voivat jäädä tehottomiksi, kun investointeja ei suunnata liiketoiminta- tai riskilähtöisesti ja pitkäjänteisesti, vaan ne kohdistuvat yksittäisiin kontrolleihin.
- OT-kyberturvallisuuden osaamisen kehittäminen yrityksissä tulisi kytkeä tiiviisti hallintamalliin, riskienhallintaan ja selkeisiin tavoitteisiin. On tärkeää määrittää organisaation nykyinen kypsyystaso ja tunnistaa kehittämistarpeet, jotta osaamisen kehittäminen voidaan kohdentaa oikeisiin asioihin.
- Riskienhallinta, mukaan lukien kolmansien osapuolten riskienhallinta, on suositeltavaa linkittää resursointiin, jotta tunnistettuihin riskeihin voidaan kohdentaa oikeat resurssit. Riskienarvioinnin tulisi olla jatkuva, luonnollinen prosessi organisaatioiden toiminnassa, mikä linkittyy osaamiseen.
- Kolmansien osapuolien ja toimittajien riskienhallintaa on suositeltavaa kehittää systemaattisesti niin että kyberturvallisuuteen liittyviä vaatimuksia ja kontrolleja toteutetaan koko kumppanuuden keston ajan, hankinnasta operointiin.
- Teknisten haasteiden ratkaisemiseksi on tärkeää varmistaa, että turvallisuusvaatimukset toimittajille ovat selkeästi määriteltyjä ja sisällytettyjä hankintaprosessiin alusta alkaen. Olemassa oleviin järjestelmiin on suositeltavaa lisätä turvallisuusvaatimuksia tarvittaessa, esimerkiksi sopimusten uudelleentarkastelun yhteydessä.

2. Johdanto

Digipoolin vuosina 2020[1] ja 2022[2] teettämien kansallisten kyberkypsyyskartoitusten perusteella OT-ympäristöjen kyberuhkiin varautuminen ja tietoturvan hallinta ovat olleet toistuvasti heikommalla tasolla verrattuna IT-ympäristöjen (tietotekniikan ja tietojenkäsittelyn järjestelmäympäristöt) varautumiseen ja hallintaan. OT-ympäristöllä (Operational Technology) viitataan laitteisiin, ohjelmistoihin ja järjestelmiin, jotka ohjaavat ja valvovat fyysisiä prosesseja erilaisissa teollisuus- ja infrastruktuuriympäristöissä.

Digitalisaation myötä OT-ympäristöjen määrä on kasvanut monilla eri toimialoilla. Teollisuuden valmistusprosessien ohjaus- ja automaatiojärjestelmien lisäksi OT-ympäristöihin kuuluu myös huoltovarmuuskriittisten organisaatioiden toimintojen kannalta kriittiset OT-järjestelmät, kuten esimerkiksi vesihuollon vedenpuhdistus- ja jakelujärjestelmät, sähköntuotannon ja -jakelun ohjausjärjestelmät, satamien lastinkäsittelyn ja navigoinnin järjestelmät, logistiikan varastojen ja kuljetusjärjestelmien hallintajärjestelmät sekä terveydenhuollon sairaala-, ja kuvantamislaitteet.

OT-ympäristöt on perinteisesti rakennettu muusta maailmasta eristetyiksi saarekkeiksi, mutta digitalisaation ja kyberturvallisuusuhkien muutoksen myötä näihin ympäristöihin kohdistuvat kyberturvallisuusriskit ovat kasvaneet huomattavasti ja jatkavat edelleen kasvamistaan. Huoltovarmuuden kannalta on äärimmäisen tärkeää, että OT-ympäristöjen jatkuvuus varmistetaan myös lisääntyvien kyberturvallisuusuhkien edessä, mikä edellyttää nykyistä nopeampaa kehitystä kyberturvallisuuden parannustoimenpiteissä.

Tämän perusteella Digipoolissa päätettiin toteuttaa OT-ympäristöjen kyberuhkiin varautumisen kehittämisen esiselvitys, jonka tavoitteena oli saada lisätietoa kyberkypsyyskartoitusten havaintoon OT-ympäristöjen kyberuhkiin varautumisesta. Käytännön tasolla OT-kyberturvallisuuden toteuttamisen haasteena ovat usein OT-ympäristöjen tekniset ominaisuudet, kuten laitteiden pitkät käyttöiät, järjestelmien yksityiskohtaisuus ja eristyneisyys muista järjestelmistä sekä tarve keskeytymättömään toimintaan. OT-ympäristöjen erityispiirteiden vuoksi tietoturvakontrollien implementoiminen voi vaatia räätälöityjä erikoisratkaisuita, jotka ovat todennäköisesti tavallisia IT-toteutuksia kalliimpia ja monimutkaisempia toteuttaa. Esiselvityksessä keskityttiin selvittämään näiden aikaisemmin tunnistettujen haasteiden taustalla olevia juurisyitä ja tunnistaa OT-kyberturvallisuuden hallinnan haasteita, jotka hankaloittavat OT-kyberturvallisuuden tason kehittämistä. Esiselvityksestä saadun tiedon perusteella arvioidaan tarkemmin ja suunnitellaan mahdollisia tarvittavia tukitoimia OT-ympäristöjen kyberturvallisuuden hallinnan kypsyyden kasvattamiseksi.

Lisäksi esiselvityksen tavoitteena oli:

- Tarjota lisätietoa kyberkypsyysselvityksen havaintoihin OT-ympäristöjen kyberturvallisuuden hallinnan tilanteesta.
- Osallistuttaa usean toimialan yritysedustajia selvittämään syitä OT-ympäristöjen hallinnan eriarvoiselle tilanteelle sekä tekemään kehitystä aiheessa.
- Tuottaa ehdotuksia toimialakohtaisiksi toimenpiteiksi, joilla aihealueen kypsyyttä kasvatetaan.
- Arvioida tarvetta tuottaa OT-ympäristöjenhallintaan liittyvää uutta ohjeistusta.
- Suunnitella toimenpiteitä kypsyyden kehittämisen tukemiseksi.

2.1 Esiselvityksen lähtökohdat ja tavoitteet eri toimialoilla

Esiselvityksen lähtökohtana toimivat edelliset Digipoolin 2020 ja 2022 teettämät kyberkypsyyskartoitukset. Näissä kartoituksissa arvioitiin lukuisten suomalaisen yrityksen ja organisaation kyberturvallisuuden nykytilaa eri toimialoilta. **Tässä esiselvityksessä keskityttiin OT-ympäristöihin, ja toimialoihin, joilla OT-ympäristöt ovat merkittävässä asemassa kansallisen huoltovarmuuden kannalta.** Näitä toimialoja ovat muun muassa teollisuus, vesihuolto, energia, elintarviketeollisuus, kauppa ja jakelu, logistiikka, satamat ja merenkulku sekä terveydenhuolto. Kaikilla näillä toimialoilla on korkeat huoltovarmuustavoitteet. Monet näiden toimialojen toimijat kuuluvat myös Euroopan unionin kyberturvallisuusdirektiivin (NIS2) piirin, jonka myötä kyberturvallisuuden hallintaan on tulossa laajempia vaatimuksia.

1 https://teknologiateollisuus.fi/digipooli/johdon-ohjaus-on-ratkaisevaa-yrityksen-kyberkestavyyden-kannalta/
2 https://teknologiateollisuus.fi/digipooli/toimialojen-kyberkypsyys-2022-selvitys-kertoo-digitaalinen-turvallisuus-on-hyvalla-perustasolla/

2.2 Aikaisemmin tunnistetut OT-ympäristöjen kyberturvallisuuden haasteet

Aikaisemmassa Digipoolin vuoden 2022 tehdyssä selvityksessä tunnistettiin moninaisia OT-ympäristöjen kyberturvallisuuden haasteita. Näistä haasteista useat toistuivat monilla eri toimialoilla. Keskeisimmät OT-ympäristöjen kyberturvallisuuden haasteet liittyivät erityisesti niiden perinteiseen kehitykseen ja hallintaan. OT-ympäristöt ovat kehittyneet osaksi tuotannollista toimintaa, ja niiden ylläpito on ollut tuotannosta vastaavan liiketoiminnan vastuulla. Tämä vastuu oli perusteltu, sillä näillä yksiköillä on vuosien ajan kertynyt osaaminen ja asiantuntijuus. Haasteena oli kuitenkin ympäristöjen väliset integroinnit, kuten analytiikan tai vastaavien palveluiden toteutus, sekä kattavan tilannekuvan rakentaminen. Selvityksessä havaittiin, että tietoisuus ja tiedonvaihto IT- ja OT-ympäristöjen hallinnasta vastaavien tahojen välillä oli laajasti puutteellista. Kokonaiskyberturvallisuuden tilannekuvan tuottamiseksi vaaditaan myös OT-puolen tilanteen ja valvonnan ymmärtämistä.

Yksi selvityksen keskeisistä havainnoista liittyi IT- ja OT-ympäristöjen kyberturvallisuuden eri tasoiseen hallintaan, jossa toiminnan yhdenmukaistamisessa ei sitä edeltävään selvitykseen (vuoden 2020) verrattuna nähty juurikaan edistystä. Selvityksen mukaan OT-puolen heikko tai jopa olematon näkyvyys kyberturvallisuuden hallinnasta vastaaville toimijoille aiheutti huomattavan eron ympäristöjen kyberturvallisuuden kypsyyksissä. Selvitys korosti tarvetta parantaa OT-ympäristöjen näkyvyyttä ja integroida niiden hallinta osaksi organisaation kokonaisvaltaista kyberturvallisuusstrategiaa.

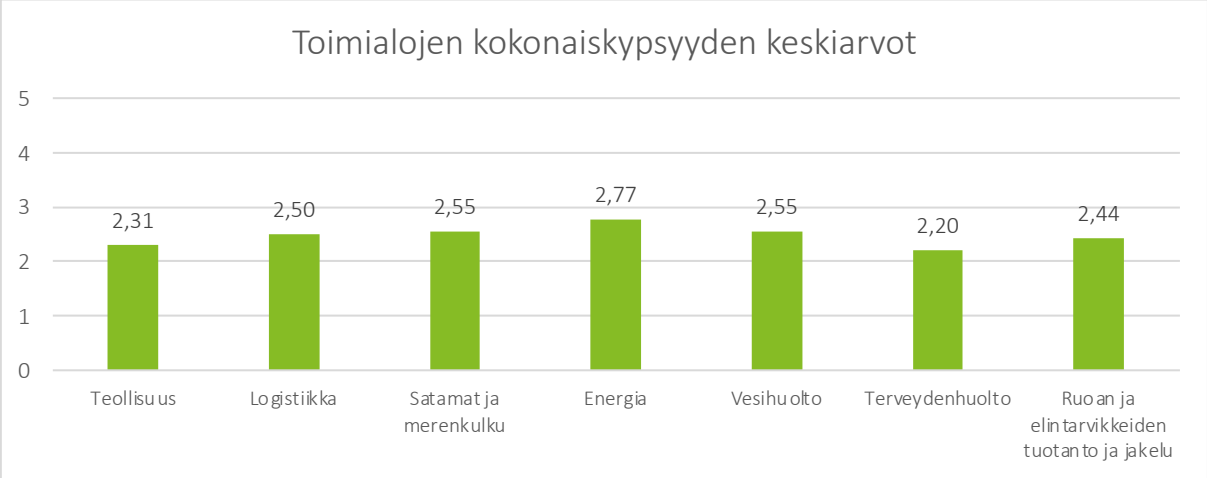
3. Havainnot

Esiselvityksen perusteella kaikkien toimialojen OT-kyberturvallisuuden hallinnan kokonaiskypsyystasot jäivät hieman hyvän perustason alapuolelle. Kypsyystasojen kuvaukset on kuvattu kappaleessa 7.1 taulussa 1. Hyvänä perustasona voidaan pitää tasoa kolme, mikä tarkoittaa, että OT-kyberturvallisuuden hallinnan prosessit on muodollisesti dokumentoitu, omistajuus ja laajuus on sovittu, ja ne ovat käytössä suurimmassa osassa organisaatiota. Johtamisjärjestelmä on määritelty ja prosessit perustuvat organisaation yhteisiin standardeihin ja linjauksiin, mutta jatkuvaa arviointia tai kehittämistä ei ole. Kaikki toimialat jäivät kokonaisuudessa hieman tämän kypsyystason alapuolelle.

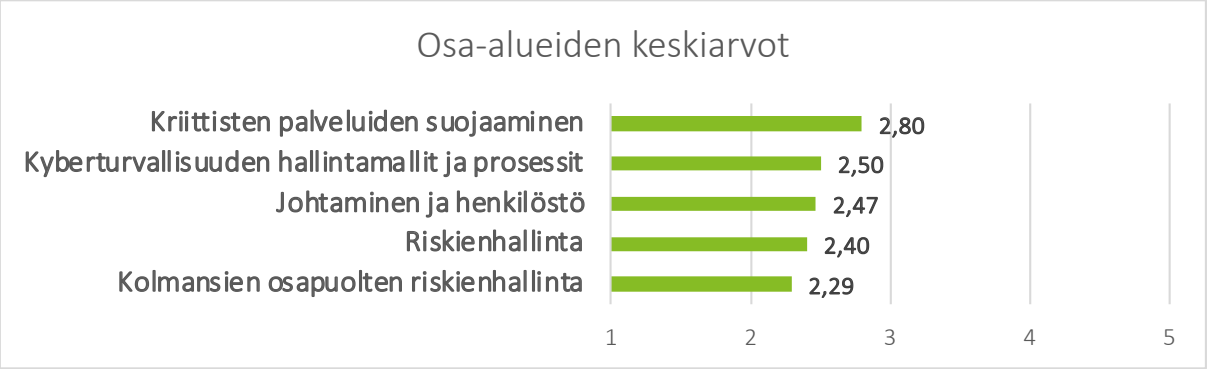
Keskiarvo toimialojen kokonaiskypsyydessä on esitetty taulukossa 1. Keskiarvon tarkastelu yksinään ja siitä johtopäätösten tekeminen voi antaa vääristyneen kuvan, joten kappaleen 7.2 taulukossa 14 on kuvattu vastausten hajonta ja mediaaniarvot. Lisäksi on huomioitava, että nykytilan kartoitus oli osana otoksenomaista kyselyä, ja kyselyyn vastanneiden henkilöiden asiantuntemusta OT-kyberturvallisuudesta ei ole erikseen arvioitu tai eroteltu, vaan yritykset valitsivat itse sopivat henkilöt vastaamaan kyselyyn. Kyselyn tulokset ovat suuntaa antavia, eivätkä välttämättä täysin tarkkoja tai kattavia. Tuloksia tulisi siis tarkastella ymmärtäen, että ne antavat yleiskuvan tilanteesta, mutta eivät välttämättä kuvaa kaikkia yksityiskohtia tai kaikkien yritysten tilannetta.

Kyselyssä käytetyt nykytilan arvioinnin osa- alueiden keskiarvot on esitetty taulukossa 2. Osa-alueiden kuvaukset on kuvattu kappaleessa 7.1 taulussa 2.

Kaikkien toimialojen osa-alueiden keskiarvojen välillä ei ollut suurta vaihtelua. Kriittisten palveluiden suojaaminen oli hieman korkeammalle tasolle arvioitu kuin muut osa-alueet ja kolmansien osapuolten riskienhallinta alhaisimmaksi. Eroa näiden välillä oli 0,51 mittayksikköä, ja muut kolme osa-aluetta sijoittuivat näiden välille.



Taulukko 1



Taulukko 2

3.1 OT-kyberturvallisuuden hallinnan haasteet ja niiden juurisyyt

OT-kyberturvallisuuden hallinnan haasteiden kartoittamiseksi vastaajat arvioivat väittämiä, jotka kuvasivat heidän näkökulmastaan, miten OT-kyberturvallisuutta hallitaan heidän organisaatioissaan. Samat juurisyyt haasteille nousivat esiin jossain määrin kaikilla toimialoilla ja ne linkittyvät ja vaikuttavat toisiinsa. Näitä haasteita ja juurisyitä on kuvattu tarkemmin seuraavissa kappaleissa.

Käytännön tasolla OT-kyberturvallisuuden haasteena ovat usein OT-ympäristöjen tekniset ominaisuudet, kuten laitteiden pitkät käyttöiät, järjestelmien yksityiskohtaisuus ja eristyneisyys muista järjestelmistä sekä tarve keskeytymättömään toimintaan. OT-ympäristöjen erityispiirteiden takia tietoturvakontrollien implementoiminen voi vaatia räätälöityjä erikoisratkaisuita, jotka ovat todennäköisesti tavallisia IT-toteutuksia kalliimpia. Tämä herättää kysymyksen, onko OT-ympäristöistä vastaavilla henkilöillä kyky perustella investoinnit johdon ymmärtämällä kielellä ja ymmärtääkö johto nämä erityistarpeet. Suurin osa esiselvitykseen osallistuneista on sitä mieltä, että yritysten johto on sitoutunut OT-kyberturvallisuuden kehittämiseen ja ymmärtää OT-ympäristöjen kyberriskejä. Tämä ymmärrys nähdään johtuvan pääosin kiristyneestä sääntelystä ja maailmalla tapahtuneista kyberiskuista. Strategisen tason jatkuva ja tavoitteellinen kehitys kuitenkin vaikuttaa jäävän vajaaksi ja tämä näkyy resursoinnissa ja hallintamalleissa.

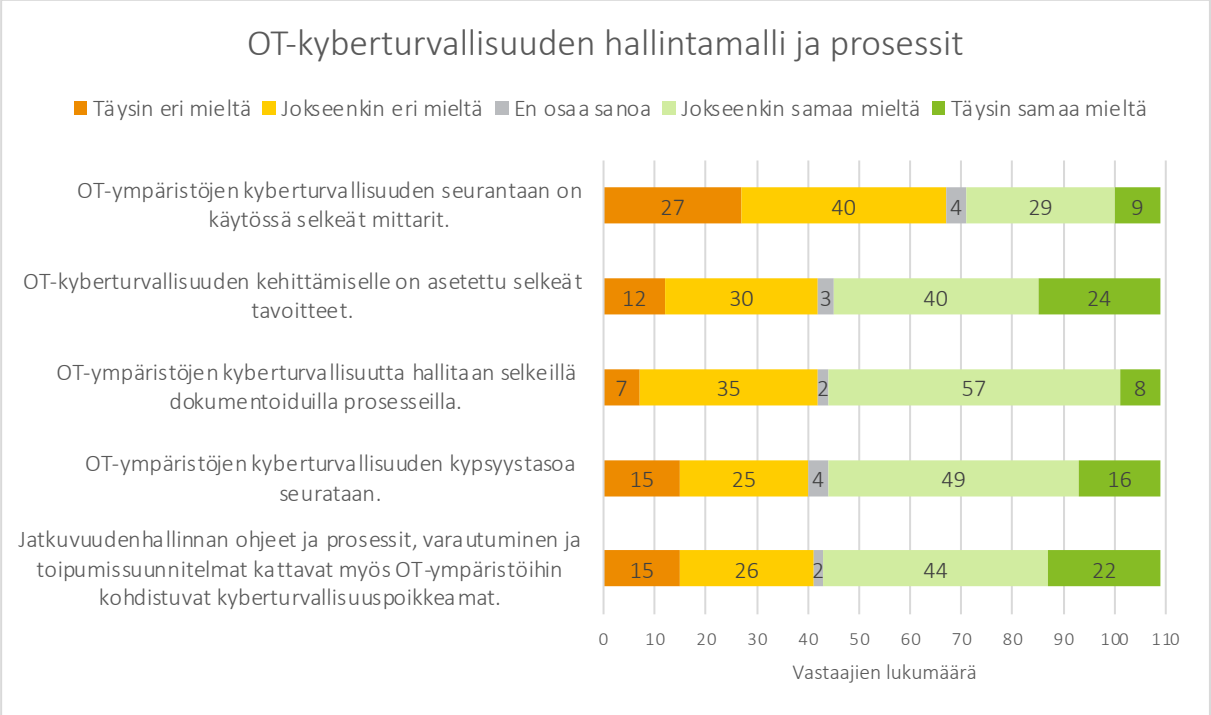
OT-ympäristöihin tietoturvakontrollien soveltamista voivat hankaloittaa myös vähäisten resurssien lisäksi muun muassa osaaminen sekä toimittajariippuvuus. Näihin puolestaan voivat vaikuttaa prosessien ja riskienhallinnan puutteet ja vastuiden määrittämättömyys. Selkeiden prosessien ja vastuiden määrityksen puutteeseen puolestaan voivat vaikuttaa yleinen ymmärryksen ja tietoisuuden puuttuminen OT-kyberturvallisuuden riskeistä. Toisin sanoen, jos OT-kyberturvallisuuden hallinnan perusasiat kuten hallintamalli ja prosessit, johtaminen, riskienhallinta, kolmansien osapuolien riskienhallinta ja kriittisten palvelujen tunnistaminen, eivät ole kunnossa, silloin voi olla hankala toteuttaa käytännön tietoturvakontrolleja systemaattisesti ja kullekin yritykselle ja OT-ympäritölle sopivalla tavalla.

3.1.1 OT-kyberturvallisuuden hallintamalli ja prosessit

Taulukossa 3 on kuvattu vastausten jakautuminen osa-alueen väittämissä vastaajien lukumäärän mukaan. Vastaajista lievä enemmistö (noin 60 %) oli täysin tai jokseenkin samaa mieltä sen kanssa, että OT-kyberturvallisuutta hallitaan selkeillä dokumentoiduilla prosesseilla, sen kypsyystasoa seurataan, sille on asetettu selkeät tavoitteet ja että jatkuvuudenhallinnan ohjeet ja prosessit, varautuminen ja toipumissuunnitelmat kattavat myös OT-ympäristöihin kohdistuvat kyberturvallisuuspoikkeamat. 62 % vastaajista oli jokseenkin tai täysin eri mieltä siitä, että OT-ympäristöjen kyberturvallisuuden tason seurantaan on käytössä selkeitä mittareita.

Selkeän OT-kyberturvallisuuden johtamis- ja hallintamallin jalkauttaminen ja seurannan mittareiden puuttuminen vaikuttaa kaikkiin muihin kehittämisen osa-alueisiin. Moni vastaaja kertoo hallintamallien olevan vielä kehitysvaiheessa OT-ympäristöjen osalta.

Vastaajien mukaan haasteena on OT-ympäristöjen kyberturvallisuudelle asetettujen vaatimusten jalkauttaminen ja käytäntöön vienti. Vaikka hyvät vaatimukset olisivat olemassa, niiden käytäntöön vieminen voi olla haasteellista, jos toiminnasta puuttuu IT-puolelle tyypillistä prosessien systemaattisuutta sekä tarvittavaa osaamista OT-ympäristöjen ja kyberturvallisuuden kontekstista, varsinkin jos toiminta on maantieteellisesti hyvin hajaantunutta. Yritysten IT-puolelta voi tulla vaatimuksia kyberturvallisuuteen, mutta ne eivät välttämättä sovellu sellaisinaan OT-puolelle teknisistä syistä. Toisaalta myös jotkin toimijat kertoivat, että he eivät ole vielä pyrkineet soveltamaan vaatimuksia OT-puolelle ajanpuutteen sekä puuttuvien OT-puolelle soveltuvien kriteeristöjen vuoksi.

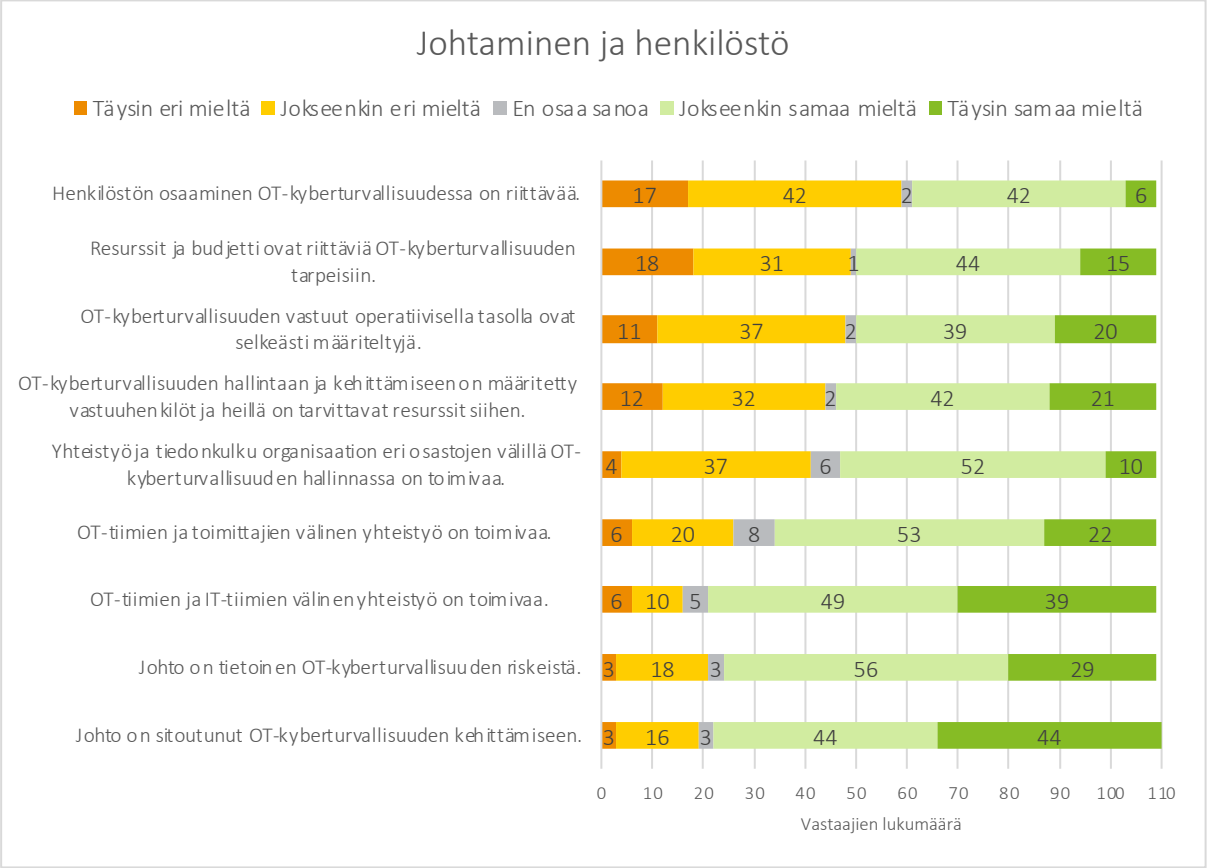


Taulukko 3

OT-kyberturvallisuuden tason kehittämisessä mittareiden puute korostuu kyselyssä ja haastatteluissa. Ilman mitattuja havaintoja oman organisaation nykytilan tasosta ei voida arvioida kehittymistarpeita tai sitä, meneekö kehitys oikeaan suuntaan. Vastaajien mukaan sopivien mittareiden löytäminen on haasteellista, ja mittaaminen nähdään aikaa vievänä, jolloin mieluummin keskitytään käyttämään vähäisiä resursseja esimerkiksi käytännön kontrollien toteuttamiseen.

3.1.2 Johtaminen ja henkilöstö

Taulukossa 4 on kuvattu vastausten jakautuminen osa-alueen väittämissä vastaajien lukumäärän mukaan. Noin 80 % vastaajista oli jokseenkin tai täysin sitä mieltä, että heidän organisaationsa johto on sitoutunut OT-kyberturvallisuuden kehittämiseen ja että johto on tietoinen OT-kyberturvallisuuden riskeistä. Hieman yli puolet vastaajista oli samaa mieltä siitä, että resurssit ja budjetti ovat riittäviä OT-kyberturvallisuuden tarpeisiin ja että vastuuhenkilöt on määritetty selkeästi. Enemmistö vastaajista pitää OT-tiimien ja IT-tiimien sekä OT-tiimien ja toimittajien välistä yhteistyötä toimivana. Kuitenkin 55 % vastaajista on sitä mieltä, että henkilöstön osaaminen OT-kyberturvallisuudessa ei ole riittävää.

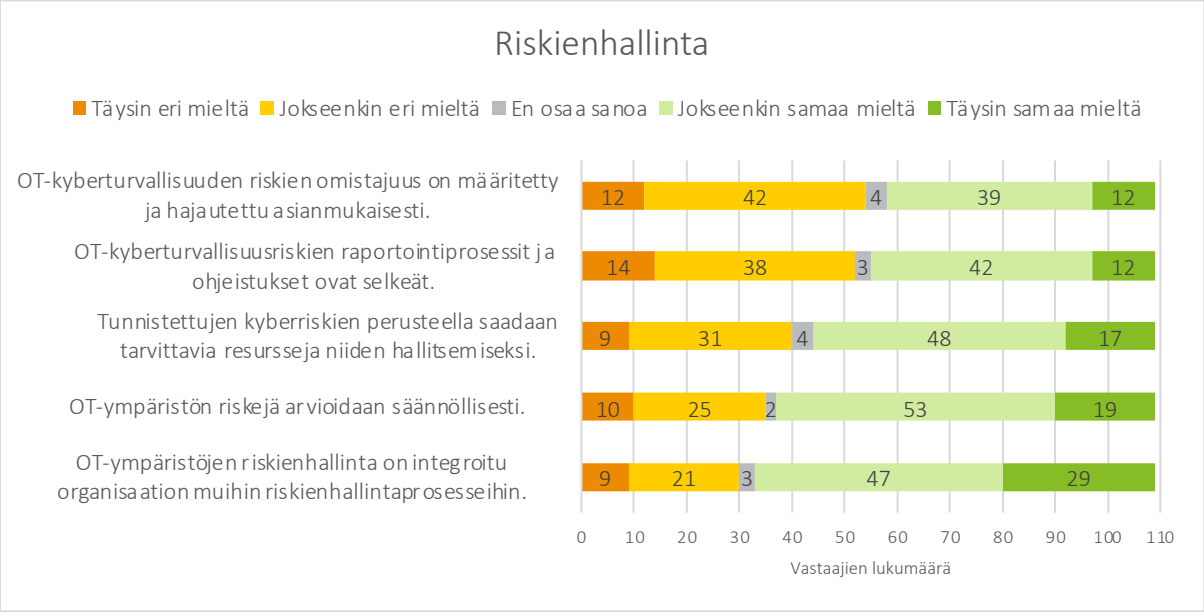


Taulukko 4

Resurssit ja budjetti koetaan riittämättömiksi OT-kyberturvallisuuden systemaattisen kehityksen tarpeisiin. Vastaajien mukaan yritysten johto on sitoutunut OT-kyberturvallisuuden kehittämiseen ja ymmärtää OT-ympäristöjen kyberriskejä, haastatteluiden mukaan tämä ymmärrys voi johtua kiristyneestä sääntelystä ja maailmalla tapahtuneista kyberiskuista. Strategisen tason jatkuva ja tavoitteellinen kehitys kuitenkin vaikuttaa jäävän vajaaksi ja tämä näkyy resursoinnissa ja hallintamalleissa. Liian pienet resurssit näkyvät puolestaan väistämättä juurisyynä lähes kaikille osa-alueille. Haastatteluiden mukaan moni toimija kokee saamansa resurssit riittäviksi hankintoihin ja pistemäisiin kehityksiin, mutta samalla esimerkiksi henkilöstöresurssit jäävät pääsääntöisesti rajalliksi, mikä vaikeuttaa OT-kyberturvallisuuden strategista ylläpitoa ja kehittämistä. Kun investointeja ei suunnata liiketoiminta- tai riskilähtöisesti ja pitkäjänteisesti, vaan ne kohdistuvat yksittäisiin kontrolleihin pitkäjänteinen kehitys voi jäädä vaille tarvittavaa resursointia.

OT-kyberturvallisuuden hallinnan ja kehittämisen sekä operatiivisen tason vastuiden selkeät määritykset koetaan tärkeänä. Jos roolit ja vastuut yritysten sisällä ja kolmansien osapuolten kanssa ovat heikosti määriteltyjä, se jättää avoimeksi sen, kuka vastaa järjestelmistä ja laitteista. Jos OT-ympäristöt jäävät kybertur-vallisuusasioiden suhteen määrittämättömään väliin, ei voida olettaa, että niiden kyberturvallisuutta kehitettäisiin määrätietoisesti.

Henkilöstön osaaminen OT-kyberturvallisuuteen koetaan yleisesti riittämättömäksi kyselyn mukaan. Tämä ei välttämättä johdu henkilöiden kyvyistä sellaisenaan tai siitä, että asiaa ei koettaisi tärkeäksi, vaan linkittyy resursseihin ja budjettiin. Ilman riittäviä taloudellisia resursseja ei ole varaa tai aikaa koulutukseen, tai vaihtoehtoisesti ei ole varaa palkata riittävästi henkilöitä, mikä johtaa ylityöllistymiseen ja ajan puutteeseen osaamisen kehittämiseksi. Vastaajien mukaan juurisyynä osaamisen puutteeseen voi olla myös vajaa ymmärrys OT-ympäristöjen kyberturvallisuudesta ja sen myötä tuleva välinpitämättömyys ja vastuiden laiminlyönti sekä liiallinen riippuvuus toimittajista. OT-ympäristöjen kyberturvallisuuden hallinta on vielä kehittymässä mikä tarkoittaa, että alan osaajia ja yleistä tietoisuutta aiheesta on vähemmän.



Taulukko 5

3.1.3 Riskienhallinta

Taulukossa 5 on kuvattu vastausten jakautuminen osa-alueen väittämissä vastaajien lukumäärän mukaan. Noin 70 % vastaajista oli joko täysin tai jokseenkin samaa mieltä siitä, että OT-ympäristön riskejä arvioidaan säännöllisesti ja että riskienhallinta on integroitu organisaation muihin riskienhallintaprosesseihin. Hieman yli puolet vastaajista oli jokseenkin tai täysin samaa mieltä siitä, että OT-kyberturvallisuusriskien raportointiprosessit ovat selkeät ja että tunnistettujen kyberriskien hallintaan saadaan tarvittavia resursseja. Vastaajat jakautuivat melkein tasan sen suhteen, onko OT-kyberturvallisuuden riskien omistajuus määritetty ja hajautettu asianmukaisesti.

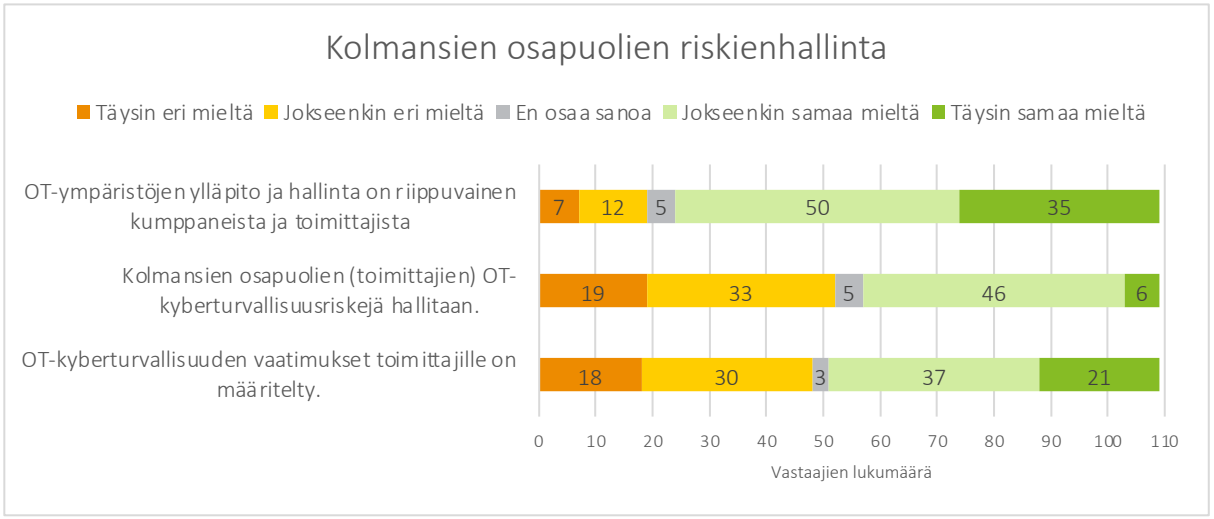
OT-ympäristöjen kyberriskejä tunnistetaan ja tiedostetaan, mutta systemaattista OT-kyberriskien raportointia ja omistajuuden määritystä tehdään vähemmän. Jos kyberriskejä ei systemaattisesti raportoida johdolle, se voi vaikuttaa siihen, että johdolla ei ole kattavaa kuvaa organisaation kyberturvallisuustilanteesta, mikä puolestaan voi johtaa aliresursointiin ja puutteellisiin toimenpiteisiin. Haastattelujen mukaan tähän voi vaikuttaa IT-turvallisuusajattelun puuttuminen OT-asioiden parissa työskenteleviltä sekä yhteistyön puute yrityksen sisällä, varsinkin jos toiminta on maantieteellisesti hyvin hajaantunutta. Yhteistyötä ja prosessinomaista riskienhallintaa on puolestaan vaikea toteuttaa ilman määriteltyjä prosesseja ja vastuita. Lisäksi juurisyynä voi prossien puuttumisen lisäksi vaikuttaa yritysten henkilöstön osaaminen ja vähäiset resurssit, mikä johtaa siihen, että OT-kyberriskienhallinta jää usein puutteelliseksi. OT-ympäristöjen riskienhallinnassa perinteisesti keskitytään enemmän fyysisen turvallisuuden riskienhallintaan ja yritykset eivät välttämättä omaa riittävää asiantuntemusta huomioidakseen OT-ympäristöjen erityispiirteitä kyberturvallisuuden kontekstissa.

3.1.4 Kolmansien osapuolien riskienhallinta

Taulukossa 6 on kuvattu vastausten jakautuminen osa-alueen väittämissä vastaajien lukumäärän mukaan. Vastaajat jakautuivat noin puoliksi sen suhteen, hallitaanko kolmansien osapuolien OT-kyberturvallisuusriskejä ja onko toimittajille määritelty vaatimuksia. Enemmistö (78 %) oli jokseenkin tai täysin sitä mieltä, että OT-ympäristöjen ylläpito ja hallinta on riippuvainen kumppaneista ja toimittajista.

Kolmansien osapuolien riskienhallinta korostuu esiselvityksen haastatteluissa ja se koetaan haastavana kokonaisuutena. Kyselyn vastaajien mukaan OT-ympäristöjen ylläpito ja hallinta on usein riippuvainen kumppaneista ja toimittajista, ja näiden OT -kyberturvallisuusriskejä hallitaan vaihtelevasti. Jos toimitusketjuihin liittyviä riskejä ei ole systemaattisesti tunnistettu, niitä ei voida hallita tehokkaasti, jos ollenkaan.

OT-kyberturvallisuus vaikutti haastattelujen perusteella olevan puutteellisesti huomioitu sopimuksissa ja hankintavaiheessa, ja turvavaatimukset voivat jäädä puutteellisiksi jo OT-ympäristöjä kehittäessä. Kolmansien osapuolien riskienhallinta ja kyberturvallisuuden vaatimusten asettaminen toimittajille on tärkeää, sillä järjestelmien rakentaminen ja ylläpito on suuresti toimittajasidonnaista. Tietoturvaa huomioidaan yleensä vakiomallisilla tietoturvaliitteillä sopimuksissa, mutta niitä ei välttämättä ole sovitettu OT-ympäristöihin. Haastatteluiden mukaan haasteena on se, että osataanko yrityksen sisällä vaatia oikeita asioita toimittajilta. Jos turvallisia ratkaisuja ei osata vaatia alusta asti, niiden vaatiminen jälkikäteen on huomattu olevan vaikeaa teknisistä syistä.

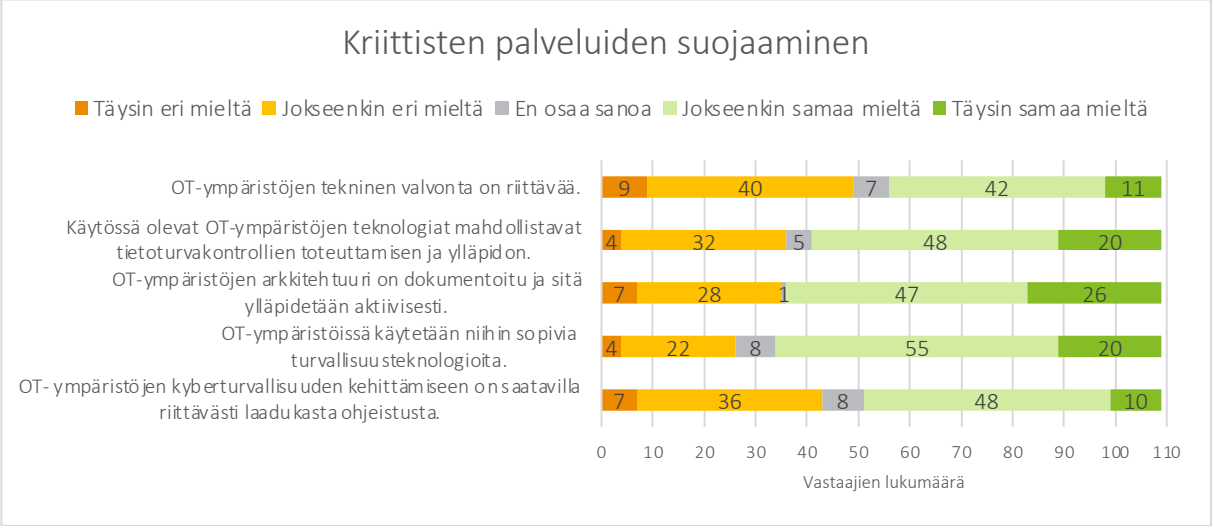


Taulukko 6

3.1.5 Kriittisten palveluiden suojaaminen

Taulukossa 7 on kuvattu vastausten jakautuminen osa-alueen väittämissä vastaajien lukumäärän mukaan. Noin 65 % vastaajista on jokseenkin tai täysin sitä mieltä, että OT-ympäristöjen arkkitehtuuri on dokumentoitu ja sitä ylläpidetään aktiivisesti ja että käytössä olevat OT-ympäristöjen teknologiat mahdollistavat tietoturvakontrollien toteuttamisen ja ylläpidon. Noin puolet vastaajista on sitä mieltä, että OT-ympäristöjen tekninen valvonta on riittävää, kun taas vähän alle puolet ovat eri mieltä. Hieman yli puolet vastaajista oli samaa mieltä siitä, että OT-kyberturvallisuuden kehittämiseen on saatavilla riittävästi laadukasta ohjeistusta.

OT-ympäristöjen kyberturvallisuuden teknisen valvonnan toteuttaminen koetaan kyselyn mukaan haasteellisena. OT-järjestelmät poikkeavat IT- järjestelmistä teknisesti sekä niiden käyttöiän perusteella. Jo vanhentuneiden järjestelmien käyttö on normaalia, vaikka niiden yhteensopivuus nykyaikaisten kyberturvakontrollien kanssa on puutteellista. Näiden järjestelmien päivittäminen voi olla työlästä ja kallista tai teknisesti mahdotonta. OT-ympäristöjen tietoturvan hallinta on yhä kehittymässä, joten teknisiä tietoturvaratkaisuja ei ole yhtä laajasti ja helposti saatavilla kuin perinteisessä IT:ssä. Kyberturvallisuuden teknisen valvonnan ja monitoroinnin toteuttaminen vaatii usein soveltamista, osaamista ja asian huomioimista jo suunnitteluvaiheessa. Alan osaajista on pulaa, mikä voi johtaa siihen, että sekä yrityksiltä että kolmansilta osapuolilta puuttuu tarvittavaa osaamista. Haastattelujen mukaan teknisen valvonnan toteuttamisen haasteet ovat yhteydessä siihen, että turvallisia ratkaisuja ei huomioida hankinta ja sopimusvaiheessa.



Taulukko 7

4. Suositukset elinkeinoelämälle

OT-kyberturvallisuuden asettaminen korkeammalle prioriteetille on suositeltavaa kaikille toimialojen yrityksille, johon yrityksen johdon tuki on välttämätöntä. OT-kyberturvallisuuden hallinnan tilaa voidaan kehittää liiketoimintalähtöisesti, ja on tärkeää yhdistää kyberturvallisuusstrategiat liiketoiminnan tavoitteisiin ja prosesseihin.

Yrityksen lähtötason huomioiden on suositeltavaa aloittaa OT-ympäristöjen omaisuuden kartoituksella ja liiketoiminnan kannalta kriittisten kohteiden tunnistamisella. Tämä perustavanlaatuinen vaihe luo pohjan tehokkaalle riskienhallinnalle ja kyberturvallisuuden kehittämiselle. Kartoituksen avulla voidaan tunnistaa ja priorisoida kriittiset resurssit, joiden suojaaminen on ensisijaista. Samalla voidaan tunnistaa kriittisiä kehityskohteita. Tämän jälkeen OT-kyberturvallisuuden hallinnan rakentaminen tulisi lähteä perusteista: selkeä hallintomalli sekä roolien ja vastuiden määritys.

Kyberturvallisuus tulisi olla kiinteä osa tuotannon hallintaa, jotta se toimii saumattomasti osana tuotannollista järjestelmää ja tukee tuotannon tavoitteita osana päivittäistä toimintaa. Määrittelemällä ja jalkauttamalla selkeä OT-kyberturvallisuuden hallintamalli voidaan ratkaista haasteita, jotka liittyvät epäselviin rooleihin ja vastuisiin sekä operatiivisella että strategisella tasolla, tavoitteelliseen kehittämiseen sekä resursointiin ja budjetointiin. Selkeiden vastuiden ja roolien määrittäminen kyberturvallisuudesta ja tuotannosta vastaavien kesken on tärkeää. Samalla on tärkeää lisätä tietoisuutta organisaation sisällä ja osallistaa IT- ja kyberturvallisuustiimin ulkopuoliset toimijat toimintaan. Kyberturvallisuuden kannalta on tärkeää määritellä OT-ympäristöjen prosessien keskinäisriippuvuudet ja yhteiset prosessit. OT-ympäristöt ovat monimutkaisia ja niillä on paljon riippuvuuksia, joten kokonaisuuksien ymmärtäminen ja yhteistyön vahvistaminen on välttämätöntä. Monissa yrityksissä OT-puolen hallinnan vastuut ovat erillään IT:stä ja kyberturvallisuudesta, mutta yhteistyön ja tietoisuuden lisääminen näiden välillä on olennaista.

Toimivan hallintamallin luominen edellyttää systemaattista lähestymistapaa, jossa oikeat sidosryhmät tunnistetaan ja sitoutetaan yhteisten tavoitteiden saavuttamiseen. Näin voidaan varmistua paremmin OT-ympäristöjen kyberturvallisuusvaatimusten jalkauttamisen ja käytäntöön viennin onnistumisesta. Kyberturvallisuuden kehittäminen edellyttää luonnollisesti myös riittäviä resursseja. Teollisuusympäristöjen toimintojen tehostamisen myötä henkilöstö on usein erittäin kuormittunut, ja ilman selkeää hallintamallia sekä roolien ja vastuiden jakoa kehitystyö saattaa olla haastavaa.

On suositeltavaa asettaa OT-kyberturvallisuuden parantamiselle selkeät ja mitattavat tavoitteet, jotka tukevat organisaation liiketoimintatavoitteita. Investoinnit voivat jäädä tehottomiksi, kun investointeja ei suunnata liiketoiminta- tai riskilähtöisesti ja pitkäjänteisesti, vaan ne kohdistuvat yksittäisiin kontrolleihin. Mittareilla voidaan osoittaa kyberturvakontrollien tehokkuus ja sitä kautta niiden taloudellinen arvo ja liiketoimintahyödyt voidaan viestiä johdolle selkeästi ja ymmärrettävästi, jotta johto voi aktiivisesti osallistua tarvittavien toimenpiteiden suunnitteluun. Johdon sitouttamisen kannalta on tärkeää, että tietoturvaa kommunikoidaan siten, että investointien vaikutukset liiketoiminnalle ovat hyvin kuvattuja.

OT-kyberturvallisuuden osaamisen kehittäminen yrityksissä tulisi kytkeä tiiviisti hallintamalliin, riskienhallintaan ja selkeisiin tavoitteisiin. On tärkeää määrittää organisaation nykyinen kypsyystaso ja tunnistaa kehittämistarpeet, jotta osaamisen kehittäminen voidaan kohdentaa oikeisiin asioihin ja varmistaa resurssien riittävyys. Kyselyn tulokset osoittavat, että osaamisen kehittäminen koetaan tärkeäksi, mutta suurin haaste on resurssien vähyys. Suosituksena on, että yritykset investoivat riittävästi resursseja OT-kyberturvallisuuden osaamisen kehittämiseen. Tämä voi sisältää säännöllisiä koulutuksia, mutta riittävän ajan ja resurssien allokointi on edellytys osaamisen kehittämiseksi.

Riskienhallinta, mukaan lukien kolmansien osapuolten riskienhallinta, on suositeltavaa linkittää resursointiin, jotta tunnistettuihin riskeihin voidaan kohdentaa oikeat resurssit. Riskienarvioinnin tulisi olla jatkuva, luonnollinen prosessi organisaatioiden toiminnassa, mikä linkittyy osaamiseen. Kyberriskejä arvioitaessa osaaminen ja yhteistyö eri toimijoiden välillä ovat tärkeitä, sillä tehokkaaseen riskien tunnistamiseen on oltava riittävä ymmärrys kyberturvallisuuden sekä OT-ympäristöjen kontekstista. Tunnistettujen riskien perusteella voidaan suunnitella kullekin yritykselle sopivien kontrollien kehittämistä, kuten kolmansien osapuolten riskienhallintaa sekä teknisten kontrollien implementointia ja monitoroinnin parantamista.

Kolmansien osapuolien ja toimittajien riskienhallintaa on suositeltavaa kehittää systemaattisesti niin että kyberturvallisuuteen liittyviä vaatimuksia

ja kontrolleja toteutetaan koko kumppanuuden elinkaaren ajan, hankinnasta operoinnin kautta mahdolliseen terminointiin asti. Kontrolleja voivat olla esimerkiksi selkeät OT-kyberturvavaatimukset ja auditointikäytännöt. Huomioimalla OT-kyberturvallisuus jo hankinta- ja sopimusvaiheessa, voidaan vähentää toimitusketjuista aiheituvia riskejä. Yhteistyön ja viestinnän parantaminen toimittajien kanssa on tärkeää, jotta voidaan luoda avoin ja läpinäkyvä suhde, joka mahdollistaa nopean reagoinnin mahdollisiin uhkiin ja haavoittuvuuksiin. Kyberturvallisuuden vaatimuksia tulisi pyrkiä tuomaan kanssa myös jo tuotannossa oleviin järjestelmiin. Tämän tulee tapahtua tiiviissä yhteistyössä järjestelmätoimittajien kanssa.

Teknisten haasteiden ratkaisemiseksi on tärkeää varmistaa, että turvallisuusvaatimukset toimittajille ovat selkeästi määriteltyjä ja sisällytettyjä hankintaprosessiin alusta alkaen. Riippuvuus toimittajista ja puutteet hankintaprosessissa voivat johtaa siihen, että turvallisuusratkaisuja ei osata vaatia riittävästi. Joskus hankintavaiheessa tehdyt ratkaisut tekevät turvallisuuden lisäämisen myöhemmin vaikeaksi tai kalliiksi. Olemassa oleviin järjestelmiin on suositeltavaa lisätä turvallisuusvaatimuksia tarvittaessa, esimerkiksi sopimusten uudelleentarkastelun yhteydessä. Keskusteluissa toimittajien kanssa sopimusten päivittämisestä ja turvallisuusvaatimusten lisäämisestä on suositeltavaa korostaa kyberturvallisuuden merkitystä ja esimerkiksi sääntelyn kautta tulevia vaatimuksia.

4.1 Eri toimialojen OT-ympäristöjen kyberturvallisuuden kehityskohteet

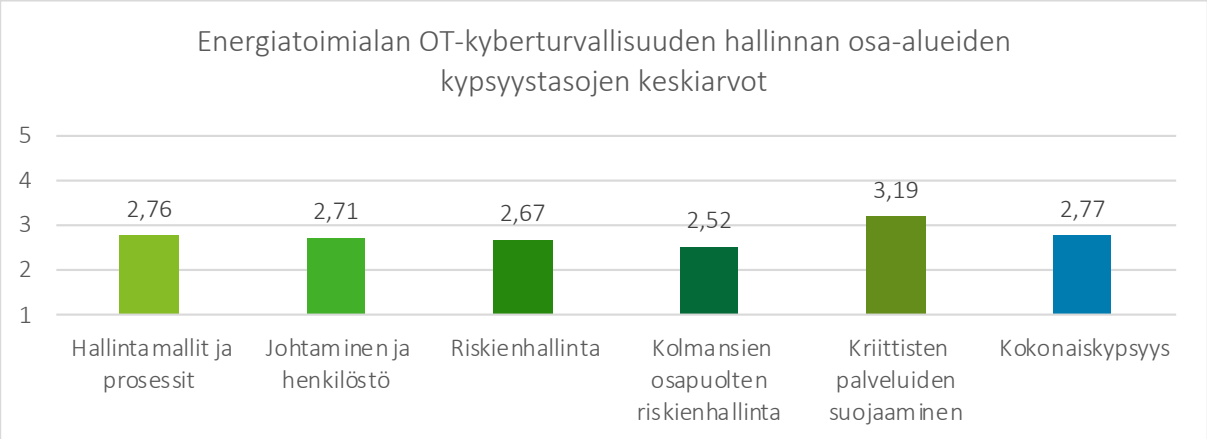
OT-kyberturvallisuuden hallinnan haasteet toistuvat kaikilla toimialoilla pitkälti samoina, joten yleiset suositukset kappaleessa 4 pätevät kaikille toimialoille. Seuraavissa kappaleissa on tiivistetty toimialoittain OT-kyberturvallisuuden hallinnan tila ja osa-alueet, joiden kehittäminen vaatii erityistä huomiota.

4.1.1 Energia

Energian toimiala kattaa kaikki toiminnot, jotka liittyvät energian tuotantoon, jakeluun ja kulutukseen. Energian toimiala on kriittistä infrastruktuuria, joka tukee talouden ja yhteiskunnan toimintaa, ja sen toiminnan häiriöt voivat aiheuttaa laajoja yhteiskunnallisia vaikutuksia. Energian toimialalle ominaista on infrastruktuurin laaja levinneisyys ja hajautus, mikä tekee OT-kyberturvallisuuden valvonnasta ja suojauksesta monimutkaisempaa.

Toimialan OT-kyberturvallisuuden hallinnan kokonaiskypsyyden keskiarvo oli tässä esiselvityksessä 2,77 eli hieman alle perustason. Osa-alueittain ainoastaan kriittisten palveluiden suojaaminen oli arvoitu perustasolle 3,19.

Toimialueen alhaisimmiksi arvioidut osa-alueet olivat riskienhallinta ja kolmansien osapuolten riskienhallinta. OT-kyberturvallisuuden tason nostattamiseksi toimialalla näihin tulisi kiinnittää erityistä huomioita. Kehittämisen painopisteenä tulisi vastaajien mukaan olla koulutus ja osaaminen, kuten jatkuva koulutus ja kybertietoisuuden jalkauttaminen kentän osaamiseksi, selkeitä ohjeita ja sääntöjä ja riittävästi resursseja tehokkaaseen ja osaavaan riskienhallintaan.



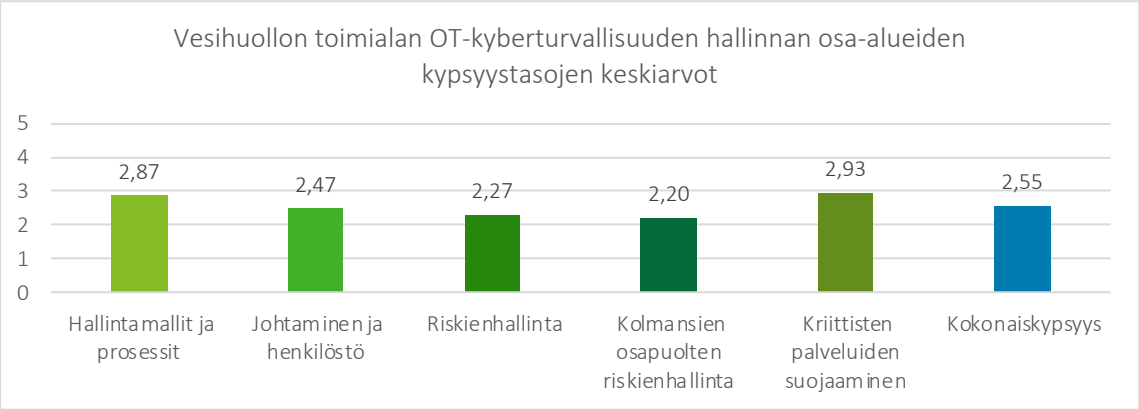
Taulukko 8

4.1.2 Vesihuolto

Vesihuollon toimiala varmistaa puhtaan juomaveden saatavuuden ja jäteveden käsittelyn, jotka ovat välttämättömiä yhteiskunnan toimivuuden kannalta. Sen on toimittava keskeytyksettä kaikissa olosuhteissa. Vesihuollon infrastruktuuri on laaja ja monimutkainen, ja se vaatii jatkuvaa ylläpitoa ja valvontaa.

Toimialan OT-kyberturvallisuuden hallinnan kokonaiskypsyyden keskiarvo oli tässä esiselvityksessä 2,55 eli alle perustason. Osa-alueittain hallintamallit ja prosessit sekä kriittisten palveluiden suojaaminen oli arvoitu lähelle perustasoa.

Toimialan alhaisimmiksi arvioidut osa-alueet olivat riskienhallinta, kolmansien osapuolten riskienhallinta sekä johtaminen ja henkilöstö. OT-kyberturvallisuuden tason nostattamiseksi toimialalla näihin on suositeltavaa kiinnittää erityistä huomioita. Kehittämisen painopisteenä tulisi vastaajien mukaan olla vastuiden selkeä määrittely ja riittävä resursointi sekä oman osaamisen kehittäminen erityisesti kolmansien osapuolien kanssa toimimiseen yhteistyössä OT-ympäristöjen turvaamiseksi.



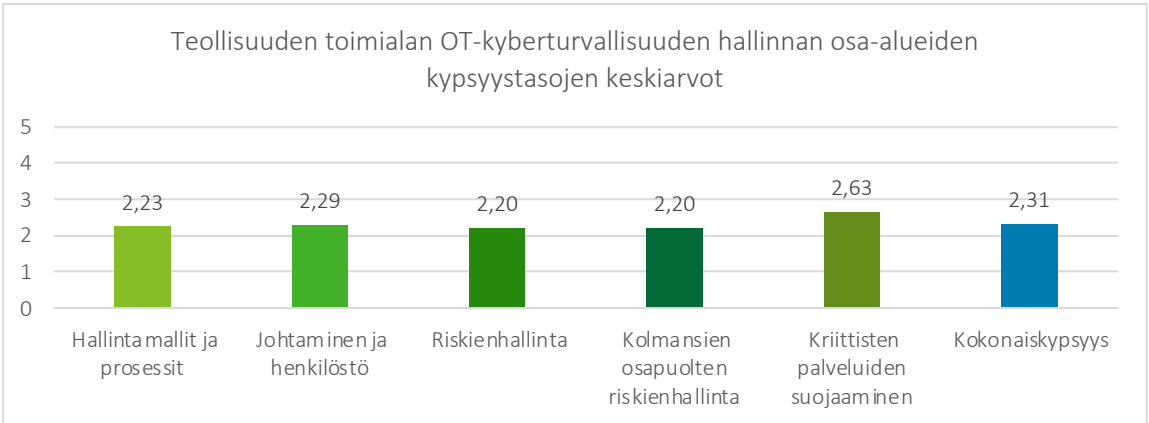
Taulukko 9

4.1.3 Teollisuus

Teollisuuden toimiala on laaja, valmistava teollisuus ja prosessiteollisuus tuottavat välttämättömiä tuotteita ja komponentteja, jotka ovat olennaisia muiden kriittisten toimialojen toiminnalle. Toimiala on riippuvainen toimitusketjujen häiriöttömyydestä ja on herkkä ympäröivän maailman muutoksille

Toimialan OT-kyberturvallisuuden hallinnan kokonaiskypsyyden keskiarvo oli tässä esiselvityksessä 2,31 eli alle perustason. Osa-alueittain kriittisten palveluiden suojaaminen oli arvoitu lähimmäksi perustasoa.

Toimialueen alhaisimmiksi arvioidut osa-alueet olivat riskienhallinta, kolmansien osapuolten riskienhallinta sekä kyberturvallisuuden hallintamallit ja prosessit. OT-kyberturvallisuuden tason nostamiseksi toimialalla on suositeltavaa kiinnittää näihin erityistä huomiota. Yritysten kyky hallita ja ylläpitää OT-ympäristöjen kyberturvallisuutta edellyttää dokumentoituja politiikkoja ja prosesseja sekä tavoitteellista kehittämistä mittareiden ja seurannan avulla. Näiden avulla voidaan toteuttaa vastuiden ja omistajuuden selkeä määrittely sekä yritysten sisällä että kumppaneiden kanssa. Lisäksi riittävä resursointi sekä oman osaamisen kehittäminen, erityisesti tietoisuuden kasvattamiseksi, on vastaajien mukaan tarpeellista, jotta tuotantoympäristöihin kohdistuvia kyberriskejä voidaan hallita tehokkaasti.



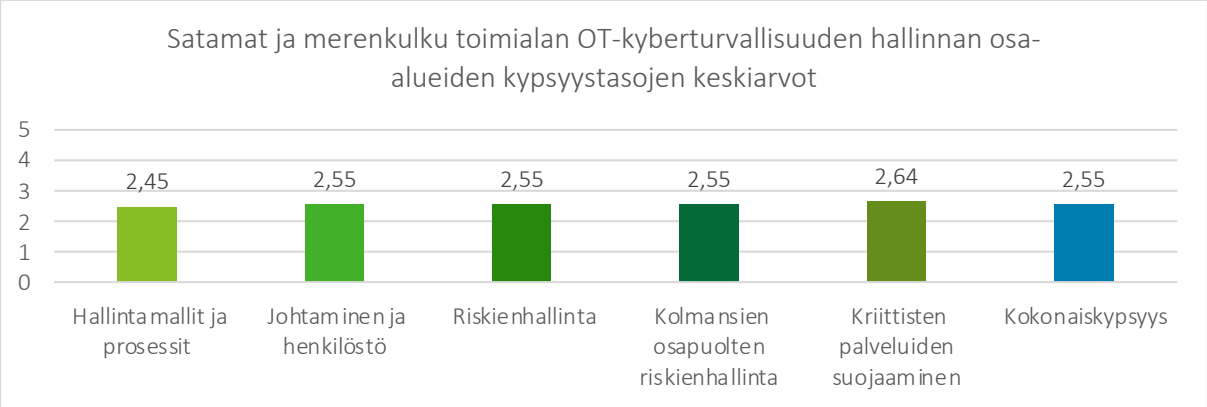
Taulukko 10

4.1.4 Satamat ja merenkulku

Satamien ja merenkulun toimiala mahdollistaa kansainvälistä kauppaa ja välttämättömien tuotteiden, kuten raaka-aineiden, elintarvikkeiden ja polttoaineiden, kuljetuksen.

Toimialan OT-kyberturvallisuuden hallinnan kokonaiskypsyyden keskiarvo oli tässä esiselvityksessä 2,55 eli alle perustason. Osa-alueittain kaikki olivat arvioitu lähelle toisiaan toisen ja kolmannen kypsyystason väliin.

Toimialan alhaisimmaksi arvioitu osa-alue oli kyberturvallisuuden hallintamallit ja prosessit. OT-kyberturvallisuuden tason nostamiseksi toimialalla on suositeltavaa kuitenkin kehittää kyvykkyyksiä kaikilla osa-alueilla. Kehittämiskohteena toimialan vastaajien mukaan tulisi olla osaamisen lisääminen, kuten kyberriskitietoisuuden ja OT-ympäristöjen kyberturvallisuuden erityispiirteiden ymmärtäminen. Painopiste kehitykseen toimialalle on OT-kyberturvallisuuden johtaminen selkeillä hallintamalleilla ja prosesseilla yritysten sisällä sekä yleisen tietoisuuden kehittämisessä koko toimialalla.



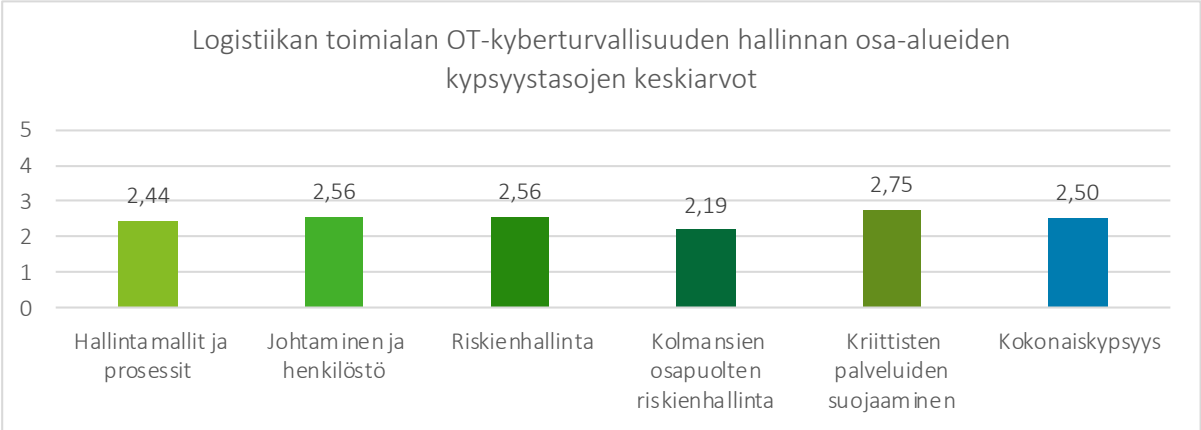
Taulukko 11

4.1.5 Logistiikka

Logistiikka-ala kattaa toiminnot tavaroiden ja palveluiden suunnitteluun, hallintaan ja kuljetukseen paikasta toiseen. Logistiikka-ala on keskeinen osa huoltovarmuutta, se varmistaa toimitusketjujen jatkuvuuden ja tehokkuuden, mikä on olennaista yhteiskunnan toiminnan ja talouden vakauden kannalta. Myös muut toimialat ovat riippuvaisia logistiikan toimialasta.

Toimialan OT-kyberturvallisuuden hallinnan kokonaiskypsyyden keskiarvo oli tässä esiselvityksessä 2,50 eli alle perustason. Osa-alueittain kriittisten palveluiden suojaaminen oli arvoitu lähimmäksi perustasoa.

Toimialan alhaisimmiksi arvioidut osa-alueet olivat kolmansien osapuolien riskienhallinta ja kyberturvallisuuden hallintamallit ja prosessit. OT-kyberturvallisuuden tason nostattamiseksi toimialalla näihin tulisi kiinnittää erityistä huomioita. Painopiste kehitykseen toimialalle on vastaajien mukaan kolmansien osapuolien riskienhallinnan lisäksi OT-kyberturvallisuuden johtaminen yrityksissä selkeillä hallintamalleilla ja prosesseilla, joiden jalkauttamiseksi tarvitaan yleisen OT-kybertietoisuuden kasvattamista toimialalla.



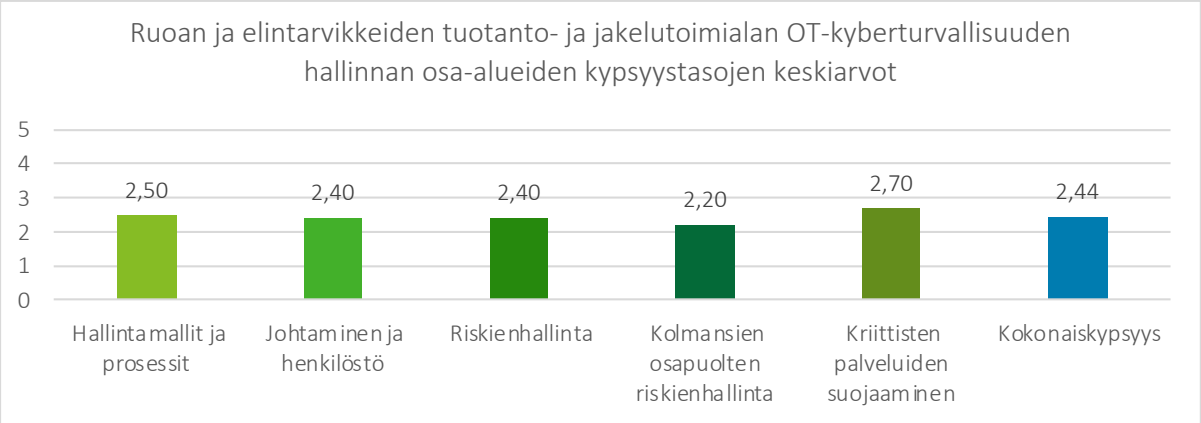
Taulukko 12

4.1.6 Ruoan ja elintarvikkeiden tuotanto- ja jakelu

Toimiala vastaa välttämättömien ravintoaineiden tuotannosta ja jakelusta, jotka ovat elintärkeitä väestön hyvinvoinnille ja terveydelle. Toimiala kattaa koko ketjun alkutuotannosta elintarvikkeiden jalostukseen, pakkaamiseen ja jakeluun. Tässä esiselvityksessä tätä toimialaa on tarkasteltu yhdessä kaupan, jakelun ja ruokapalveluiden toimialan kanssa, jonka tavoitteena on varmistaa, että tuotteet ja materiaalit ovat saatavilla kuluttajille ja muille toimijoille. Toimiala on riippuvainen toimitusketjuista, ruuan ja elintarvikkeiden tuotannon sekä logistiikan toimialoista.

Toimialan OT-kyberturvallisuuden hallinnan kokonaiskypsyyden keskiarvo oli tässä esiselvityksessä 2,44 eli alle perustason. Osa-alueittain kriittisten palveluiden suojaaminen oli arvoitu lähimmäksi perustasoa.

Toimialueen alhaisimmiksi arvioidut osa-alueet olivat riskienhallinta ja kolmansien osapuolten riskienhallinta, myös johtaminen ja henkilöstö arvoitiin matalalle. OT-kyberturvallisuuden tason nostamiseksi toimialalla on suositeltavaa kuitenkin kehittää kyvykkyyksiä kaikilla osa-alueilla. Kehittämisen painopisteenä tulisi vastaajien mukaan olla osaamisen ja ohjeistuksen kehittäminen, sekä resurssien tehokkaampi kohdentaminen, jotta kyberturvallisuuden tasoa voidaan systemaattisesti kehittää ja kolmansiin osapuoliin liittyviä kyberriskejä hallita.



Taulukko 13

4.1.7 Terveydenhuolto

Terveydenhuollon toimiala vastaa väestön terveyden ja hyvinvoinnin ylläpitämisestä ja hoitamisesta. Toimialan OT-ympäristöt eli lääkinnälliset laitteet vaativat jatkuvaa ja keskeytyksetöntä toimintaa. Toimialaan kohdistuva regulaatio tuo paljon rajoituksia lääkintälaitteiden hallintaan teknisellä tasolla.

Toimialan osallistuminen kyselyyn jäi vähäiseksi, mutta tätä täydennettiin toimialan haastattelulla. Toimialan OT-kyberturvallisuuden hallinnan kokonaiskypsyyden keskiarvo oli tässä esiselvityksessä 2,20 eli alle perustason.

Vastausten vähäisyyden vuoksi tämä ei kuiten kaan anna tarpeeksi kattavaa kuvaa toimialasta. Kehittämisen painopisteenä tulisi esiselvitykseen osallistujien mukaan olla riittävien resurssien varmistaminen sekä toimialaympäristöön soveltuvien ratkaisujen löytäminen OT-ympäristöjen tekniseen ylläpitoon. Tässä yhteydessä on suositeltavaa tehdä tiivistä yhteistyötä toimittajien kanssa, asettaa turvallisuusvaatimukset jo hankintavaiheessa ja seurata näiden vaatimusten täyttymistä yhdessä toimittajien kanssa. Lisäksi toimialalle tulisi kehittää sopivia mittareita OT-ympäristöjen kyberturvallisuuden arvioimiseksi ja parantamiseksi.

5. Ehdotukset elinkeinoelämän tukitoimiksi

Esiselvityksessä nousi esiin tarve toimialakohtaisille kevyille ja käytännönläheisille ohjeille OT-kyberturvallisuuden tason parantamiseen. Lisäksi haastatteluissa korostettiin verkostojen merkitystä tietoisuuden kasvattamisessa. Ohjeita ja tukea tarvitaan ja halutaan hyödyntää, kunhan ne ovat helposti käytäntöön sovellettavissa. Muutama vastaaja mainitsi hyödyntävänsä jo olemassa olevia ohjeita, kuten esimerkiksi KYBER-ENE- ja KYBER-VESI-projekteista tuotettuja ohjeita[3]. Näistä kuitenkin on suositeltavaa viestiä paremmin, jotta ohjeita osataan hyödyntää enemmän.

1. Toimialakohtaisia kevyitä ja käytännönläheisiä ohjeita OT-kyberturvallisuuden parantamiseen. Selvitykseen vastaajat kaipaavat selkeitä ja helposti sovellettavia ohjeita, jotka auttavat heitä parantamaan OT-kyberturvallisuutta käytännön tasolla. Käytännön ohjeita toivottiin etenkin OT-kyberturvallisuuden tason mittaamiseen ja minimivaatimusten määrittämiseen sekä kolmansien osapuolten OT-kyberriskienhallintaan. Ohjeiden tulee olla toimialakohtaisia, jotta ne vastaavat kunkin toimialan erityistarpeisiin ja haasteisiin. Tiedottamalla näistä ohjeista ja kannustamalla niiden käyttöön voidaan lisätä yritysten valmiuksia suojata OT-ympäristöjään. Kehitettäviä ohjeita voisivat olla esimerkiksi:

- **Kevyt kybermaturiteetin mittari OT-ympäristöihin ja selkeät minimivaatimukset.** Selvityksessä korostui soveltuvien mittareiden puute, mikä vaikeuttaa OT-kyberturvallisuuden tason arviointia ja parantamista. Yritykset tarvitsevat työkaluja, joiden avulla ne voivat arvioida kyberturvallisuuden nykytilaa ja tunnistaa kehityskohteita. Kevyt OT- kybermaturiteetin mittari auttaisi yrityksiä käymään läpi perusasiat ja arvioimaan kyberturvallisuuden tasoa yksinkertaisten kysymysten ja tarkistuslistojen avulla. Selkeät minimivaatimukset auttavat yrityksiä suojaamaan OT-ympäristönsä ja viestimään kyberturvallisuuden tasosta johdolle, mikä tukee parannustoimien aloittamista.
- **Tukea kolmansien osapuolten OT-kyberriskienhallintaan, erityisesti hankintavaiheessa.** Selvityksessä keskeiseksi tunnistettu haaste ja kehittämistä vaativa osa-alue oli kolmansien osapuolten OT-kyberriskienhallinta. Tukea tähän kaivataan OT-kyberturvallisuuden huomioimisesta jo hankintavaiheessa. Esimerkiksi tietoturvaliitteiden vaatimuksista, joita toimittajilta tulisi edellyttää, sekä toimittajien kyberturvallisuuden valvonnasta ja auditoinnista. Jos yrityksiä saadaan kannustettua vaatimaan OT-kyberturvallisuutta jo hankintojen suunnitteluvaiheessa, kyberturvallisuus voitaisiin huomioida OT-ympäristöjen toimituksissa jo alkuvaiheessa. Systemaattiset OT-kyberturvallisuusvaatimukset kolmansille osapuolille voisivat myös viestiä toimittajille, että heidän on jatkossa kiinnitettävä enemmän huomiota kyberturvallisuuteen.

2. Koulutuksia tuotantoautomaation asiantuntijoille ja johdolle OT-kyberturvallisuuden huomioimisesta. Yritykset kaipaavat henkilöstölleen soveltuvaa koulutusta OT-kyberturvallisuuden huomioimisesta, jotta henkilöstön osaaminen kehittyy ja OT-kyberturvallisuutta voidaan huomioida sekä operatiivisella että strategisella tasolla. Koulutukset, kuten webinaarit olemassa olevien ohjeiden käytöstä ja soveltamisesta toimialalla, olisivat tarpeeksi kevyitä ja matalan kynnyksen osallistumista, jolloin viestintää asiasta voidaan tehostaa ja auttaa yrityksiä ymmärtämään ja hyödyntämään saatavilla olevia resursseja tehokkaasti.

3. Yhteistyöverkostoja toimialoittain. Verkostojen merkitys tietoisuuden kasvattamisessa on keskeinen. Luomalla ja vahvistamalla verkostoja voidaan lisätä yhteistyötä ja tiedonvaihtoa yritysten ja Digipoolin välillä, sekä tuoda erityisesti pienempien yritysten tietoisuuteen tapoja kehittää OT-kyberturvallisuutta. Verkostojen avulla voidaan lisätä tietoisuutta julkisista työkaluista ja ohjeista sekä kannustaa yrityksiä hyödyntämään näitä resursseja OT-kyberturvallisuuden tason parantamiseksi.

Kaikkia näitä ehdotuksia voidaan toteuttaa joko erikseen tai osana suurempaa viestintäkampanjaa, jonka tavoitteena on tehostaa viestintää jo kehitettyjen ohjeistuksien hyödyntämiseksi sekä kehittää uuttaa ohjeistusta ja koulutusta kriittisen infrastruktuurin sektoreilla OT-kyberturvallisuuden tason parantamiseksi. Viestintäkampanja suositellaan kohdennettavaksi toimialoittain yritysten johdolle mutta sen käytännön osia kuten koulutuksia ja ohjeita suositellaan kohdennettavaksi tietoturvavastaavien lisäksi, IT- ja automaatiojärjestelmien hankinnoista vastaaville henkilöille sekä OT-ympäristöjen ylläpidosta vastaaville henkilöille.

3 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille/materiaaleja

6. Menetelmät

Esiselvityksen tiedonkeruumenetelmien suunnittelussa hyödynnettiin edellisiä kyberkypsyysselvityksiä. Näiden selvitysten tulokset tarjosivat tietoa OT-ympäristöjen nykytilasta ja aiemmista havainnoista, jotka toimivat pohjana jatkoselvitykselle.

Pääasiallinen tiedonkeruumenetelmä oli kysely, joka lähetettiin eri toimialojen organisaatioille. Kyselyn avulla kerättiin tietoa OT-ympäristöjen kyberturvallisuuden hallinnan nykytilasta, käytännöistä, haasteista ja kehitystarpeista. Kyselyyn osallistui edustajia useilta eri toimialoilta, mikä mahdollisti näkökulmien saamisen eri toimialoilta. Selvityksessä ei eroteltu vastaajia yrityksen koon mukaan. Kyselyä välitettiin lukuisille vastaanottajalle Digipoolin kautta ja se oli avoinna 18.11.2024 - 20.12.2024 välillä.

Vastauksia saatiin yhteensä 113 kappaletta ja näistä neljä tuli tämän esiselvityksen ulkopuolisilta toimialoilta, joten ne jätettiin pois kyselyn analyysistä, jolloin kyselyn vastauksen kokonaismäärä oli 109 kappaletta. Vastaajista 32 % oli teollisuuden toimialoilta, 19 % energian toimialalta, 14 % vesihuollon toimialalta, 15 % logistiikan toimialalta, 10 % satamien ja merenkulun toimialalta, terveydenhuollon toimialalta 1 % sekä ruoan ja elintarvikkeiden tuotannosta ja kaupan ja jakelun toimialoilta yhteensä 9 % vastauksista. Ruoan ja elintarvikkeiden tuotanto (elintarviketeollisuus, alkutuotanto) ja kauppa, jakelu ja ruokapalvelut yhdistettiin selvityksessä Ruoan ja elintarvikkeiden tuotanto ja jakelu -toimialaksi. Jokin muu toimiala -luokkaan kuuluvat vastaajat jaettiin sopiviin edellä mainittuihin toimialoihin tai jätettiin pois kyselyn analyysistä. Kyselyyn vastaajista 23 % oli CISO, CIO, CTO tai muussa vastaavassa teknologia johtajan roolissa, 18 % toimitusjohtajan roolissa ja 17 % COO tai muussa operatiivisessa johtajan roolissa, tuotantoautomaation asiantuntijoita 9 % ja IT-asiantuntijoita oli 17 % prosenttia. Tietoturvan tai kyberturvallisuuden asiantuntijoita oli yhteensä 15 % ja heistä 4 % oli OT-kyberturvallisuuden asiantuntijoita.

Kyselyaineisto muodostaa näytteen OT-kyberturvallisuuden hallinnan tilasta ja sen haasteista eri toimialoilla. Se ei kuitenkaan muodosta kattavaa kuvaa kaikilta näiltä toimialoilta, etenkin terveydenhuollon toimialalta vastauksien määrä jäi pieneksi toimialakohtaisten johtopäätösten mahdollistamiseksi. Kyselyyn tuli myös paljon avoimia vastauksia, joiden analysoinnissa keskityttiin tunnistamaan toistuvia teemoja ja kategorioita, muodostamaan kuva vastaajien yleisistä haasteista ja kehitystarpeista sekä näiden juurisyistä.

Kyselyä täydennettiin eri toimialojen organisaatioiden haastatteluilla. Haastattelut mahdollistivat syvällisemmän keskustelun ja analyysin, mikä auttoi tunnistamaan syitä OT-ympäristöjen hallinnan tilanteelle ja kehitystarpeille. Haastattelujen avulla saatiin yksityiskohtaisempaa tietoa organisaatioiden käytännön kokemuksista, haasteista ja parhaista käytännöistä. Haastatteluita pidettiin yhteensä seitsemän kappaletta ja haastateltaviksi tunnistettiin keskeisiä eri toimialojen organisaatioita, jotka osallistuivat haastatteluihin vapaaehtoisesti Digipoolin kontaktien kautta.

7. Liitteet

Tässä luvussa esitellään esiselvityksen käytetyt arviointikriteeristöt ja OT-kyberturvallisuuden hallinnan nykytila-arvion hajontakaavio. Luvussa 7.1 esitellään arviointikriteeristö ja nykytilan arvioinnissa käytetyt osa-alueet. Hajontakaavio esitellään luvussa 7.2

7.1 Arviointikriteeristö

Nykytilan arviointiasteikkona käytettiin yleisestä CMM- mallista (Capability Maturity Model) johdettua 5-tasoista kypsyysmallia. Eri kypsyystasojen kuvaukset on kuvattu alla taulussa 1.

Taso 1: Alkuvaihe	Toiminta on tyypillisesti dokumentoimatonta ja dynaamisessa muutostilassa, ja sitä ohjataan ad-hoc, hallitsemattomalla ja reaktiivisella tavalla.
Taso 2: Määritelty	Prosessit ovat suunniteltuja, dokumentoituja ja niiden toteutumista valvotaan mutta taustalta puuttuu johtamisjärjestelmä. Kattavuutta ei ole sovittu. Enimmäkseen määritellyllä tasolla toteutettu, mutta edelleen alkuvaiheen tasolla joissakin osissa.
Taso 3: Toistettava	Prosessit on muodollisesti dokumentoitu, omistajuus ja laajuus on sovittu, ja on käytössä suurimmassa osassa organisaatiota. Johtamisjärjestelmä määritelty ja prosessit perustuvat organisaation yhteisiin standardeihin ja linjauksiin. Ei jatkuvaa arviointia tai kehittämistä.
Taso 4: Hallittu	Prosesseja ylläpidetään aktiivisesti ja suorituskyvylle sekä prosessien laadulle on asetettu vaatimukset, joita seurataan. Edistynyt toteutustaso joissakin osissa, lähes täysi kattavuus.
Taso 5: Optimoitu	Prosesseja kehitetään jatkuvasti sekä asteittaisilla että innovatiivisilla muutoksilla. Edistynyt/alan johtava toteutustaso ja täysi kattavuus.

Taulu 1

Kyselyssä käytetyt nykytilan arvioinnin osa- alueet johdettiin Traficomin Kyberturvallisuuskeskuksen Kybermittarin[4] osa-alueista tiivistäen ja keskittäen etenkin OT-ympäristöille relevantteihin osa-alueisiin. Kybermittari on ilmainen kyberturvallisuuden arviointi- ja kehittämispalvelu. Se on organisaatioiden johdolle ja tietoturva-ammattilaisille suunnattu, konkreettinen väline kyberturvallisuuden hallintaan, toimialakohtaiseen vertailuun ja kehityspanostusten ohjaamiseen.

Osa-alueiden kuvaukset on kuvattu alla taulussa 2.

Kyberturvallisuuden hallintamallit ja prosessit	Osa-alueeseen kuuluu organisaation kyky hallita ja ylläpitää OT-ympäristöjen kyberturvallisuutta kyberturvallisuuden hallintamallien ja prosessien kautta. Osa-alueeseen kuuluu esimerkiksi: • Hallintamallin dokumentoidut politiikat ja prosessit kattaen OT-ympäristöt • OT-kyberturvallisuuden tavoitteellinen kehittäminen (mittarit, seuranta) • OT-arkkitehtuurin ja omaisuuden dokumentaatio • Jatkuvuudenhallinta ja varautumisen kehittäminen • Sääntelyvaatimusten noudattamisen kehittäminen (NIS2)

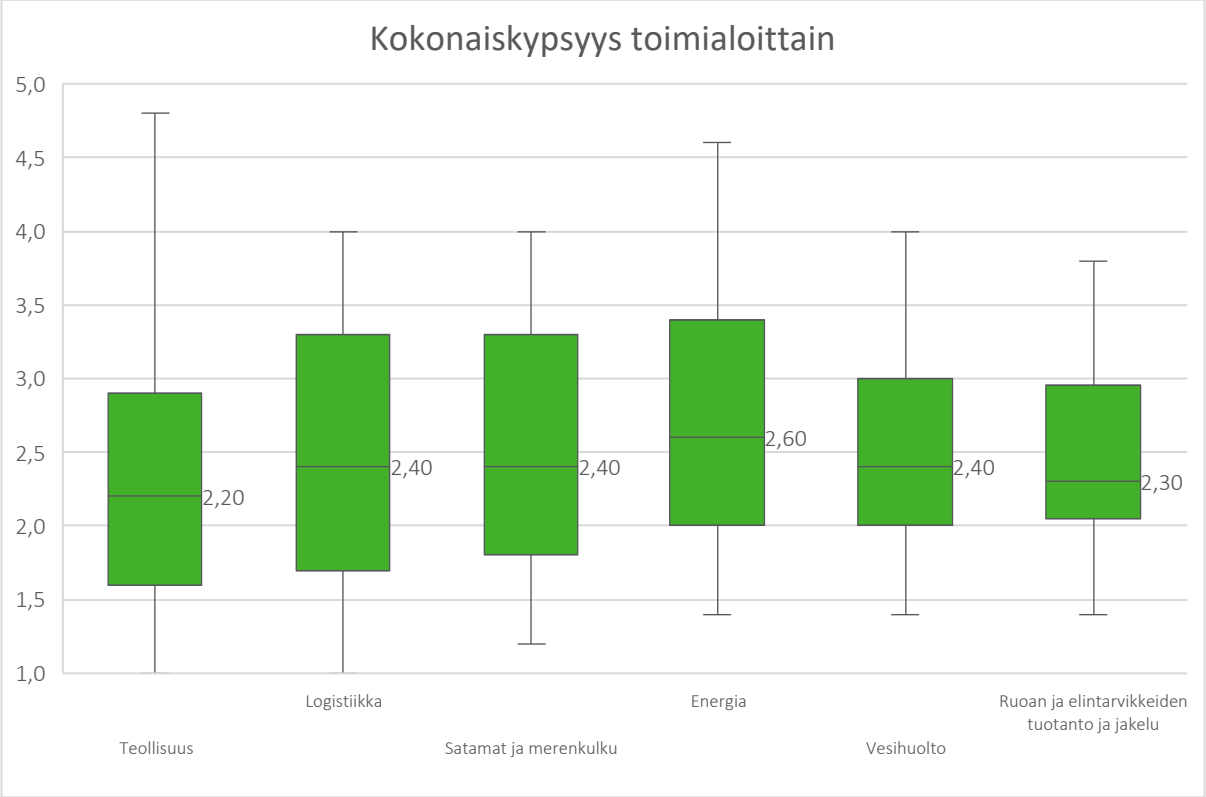
Johtaminen ja henkilöstö	Osa-alueeseen kuuluu OT-kyberturvallisuuden johtaminen sekä henkilöstön OT-kyberturvallisuustietoisuus, -osaaminen, sekä valmius reagoida erilaisiin OT-ympäristöjen kyberhäiriötilanteisiin. Osa-alueeseen kuuluu esimerkiksi: • OT-kyberturvallisuuden vastuiden jakaminen • OT-kyberturvallisuuden keskittyvän henkilöstön kehittäminen • Koulutus ja kybertietoisuuden lisääminen • Johdon sitoutuminen OT-kyberturvallisuuden kehittämiseen • Resursoinnin ja budjetin riittävyys OT-kyberturvallisuuden ylläpitoon ja kehittämiseen
Riskienhallinta	Osa-alueeseen kuuluu organisaation OT- kyberturvallisuuteen liittyvien riskien tunnistamisen ja hallinnan valmiudet. Osa-alueeseen kuuluu esimerkiksi: • OT-kyberriskienhallinnan suunnitelma • OT-kyberriskien tunnistaminen • OT-kyberriskien analysointi ja reagointi • OT-kyberriskien omistajuus
Kolmansien osapuolten riskienhallinta	Osa-alueeseen kuuluu organisaation kyky tunnistaa sekä hallinnoida OT-ympäristöjen toimitusketjuihin ja kolmansiin osapuoliin liittyviä kyberriskejä. Osa-alueeseen kuuluu esimerkiksi: • OT-ympäristön toimittajiin liittyvien kyberriskien hallinta • Kyberturvavaatimusten määrittely toimittajille
Kriittisten palveluiden suojaaminen	Osa-alueeseen kuuluu organisaation kyky tunnistaa omat kriittiset OT-ympäristöt, ja niihin vaikuttavat tekijät ja komponentit, joista kyberriskejä voi syntyä Osa-alueeseen kuuluu esimerkiksi: • Kriittisten OT-ympäristöjen ja niiden riippuvuuksien tunnistaminen • Kriittisten OT-ympäristöjen kyberhäiriöiden vaikutusten minimointi

Taulu 2

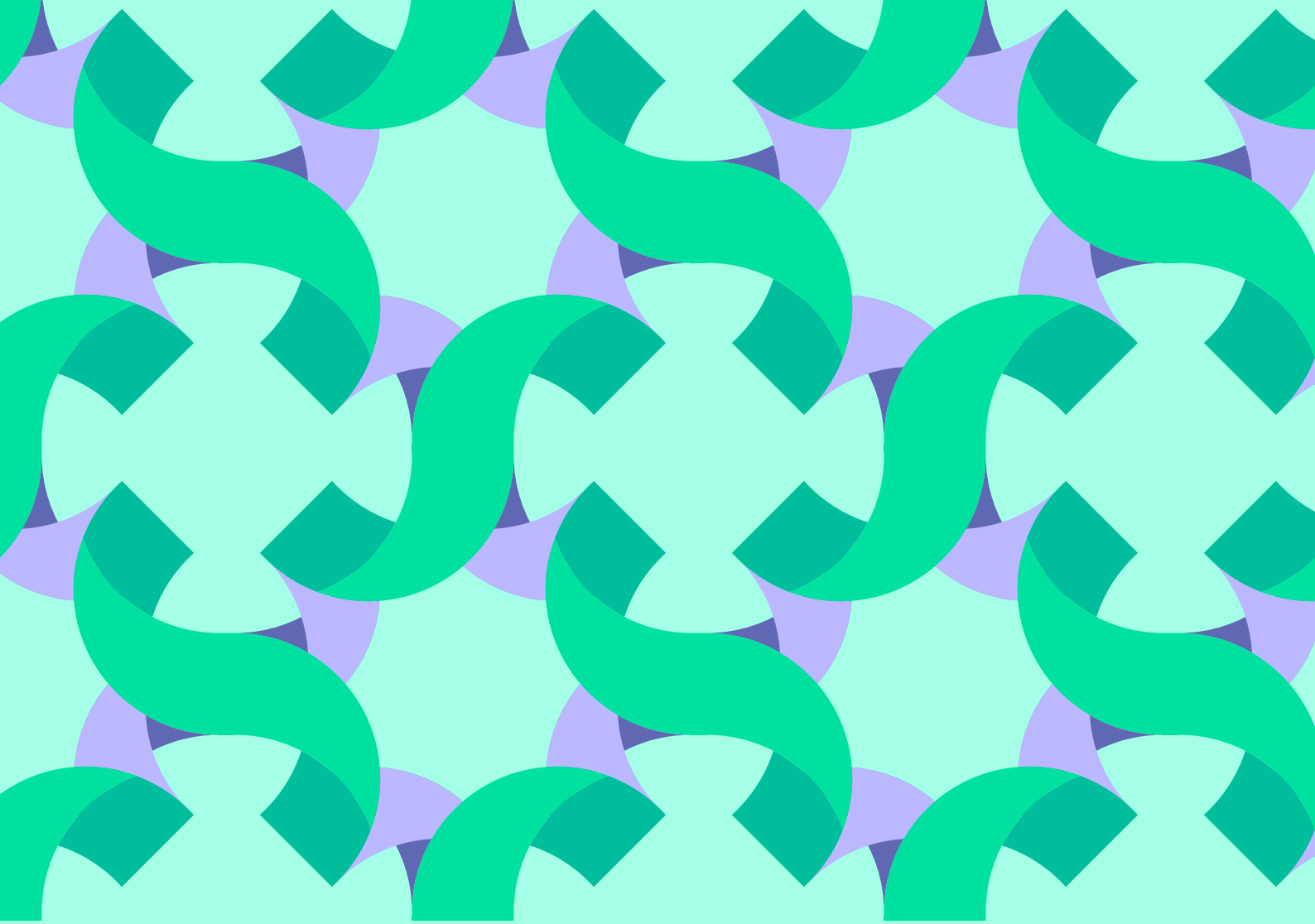
7.2 Hajontakaavio

Taulukossa 14 on kuvattu toimialoittain OT-kyberturvallisuuden hallinnan kokonaiskypsyystasojen vastausten hajonta ja mediaaniarvot. Terveydenhuollon toimialalta vastauksien määrä jäi liian pieneksi hajonnan laskemiseksi. Vihreä palkki kuvaa aluetta, johon 50 vastauksista osuivat, ja niiden ylä- ja alapuolella olevat viivat osoittavat, mihin ylimmät ja alimmat 25% vastauksista sijoittuivat. Mediaaniarvo näkyy taulukossa lukuna.

4 https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari?toggle=Mik%C3%A4%20on%20Kybermittari%3F


Kokonaiskypsyys toimialoittain
5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
2,20
2,40
2,40
2,60
2,40
2,30
Teollisuus
Logistiikka
Satamat ja merenkulku
Energia
Vesihuolto
Ruoan ja elintarvikkeiden tuotanto ja jakelu

Taulukko 14



Huoltovarmuusorganisaatio
Digipooli