IoT-TOIMITTAJIEN JA RATKAISUJEN ARVIOINNIN TARKASTUSLISTAT

SISÄLLYSLUETTELO

IoT – TOIMITTAJIEN JA RATKAISUJEN ARVIOINNIN TARKASTUSLISTAT

Tässä dokumentissa esitellyt tarkastuslistat on tarkoitettu energiayritysten IoT-ratkaisuja tai palveluja suunnittelevien ja evaluoivien asiantuntijoiden käyttöön.

Tavoitteena on helpottaa IoT-palvelutarjoajien luotettavuuden ja erityisesti kyberturvallisuuteen liittyvien kyvykkyyksien arviointia.

Listat ovat osin päällekkäisiä ja niitä voidaan käyttää tarvittaessa itsenäisesti.

Kysymyslistat on laadittu pyritty laatimaan tarkentuvaksi listaksi, ensin pääkysymykset ja sitten tarkentavat kysymykset.

Kysymykset ovat laadittu käyttäen pohjana ENISA:n dokumenttia “Baseline Security Recommendations for IoT, in the context of Critical Information Infrastructures”.

Viittaukset (kuten [GP-PS-01]) osoittavat pohjana olleen ENISA-dokumentin vaatimuksiin, joista kysymykset on johdettu.

TIETOTURVAPOLITIIKKOIHIN LIITTYVIÄ KYSYMYKSIÄ

Miten kyberturvallisuus on otettu huomioon tarjoamanne IoT-järjestelmän kehityksen ja käytön aikana?

- Onko teillä käytössä jokin (jos niin mikä) turvallisen ohjelmistokehityksen toimintamalli?
  - Miten tietoturvapolitiikoiden ja vaatimusten mahdolliset muutokset viedään teidän kehitysprosessiinne?
- Kertokaa miten tarjoamanne IoT-järjestelmän osat sijoittuvat suhteessa IEC-62443:n referenssiarkkitehtuuriin ja millaisia suojauksia (luottamusrajoja) eri komponenttien välillä käytetään?
  - Sijoittakaa IoT-ratkaisunne komponentit verkkoaluekuvaan
- Miten, milloin ja kenen toimesta tarjoamanne IoT-järjestelmän ja siihen kuuluvien sovellusten kyberturvallisuutta on testattu?
  - Miten testaaminen on dokumentoitu?
- Onko järjestelmässä käytettyjen sovellusten ohjelmistokoodi katselmoitu?
- Miten katselmointi on dokumentoitu?

[GP-PS-01 GP-PS-02 GP-PS-05 GP-PS-06 GP-PS-07]

Miten henkilö- ja ympäristöturvallisuus on otettu huomioon tarjoamanne IoT-järjestelmän kehityksen ja käytön aikana?

- Miten käyttäjän fyysinen turvallisuus on varmistettu?

Miten laitteen fyysinen turvallisuus on otettu huomioon tilanteessa, jossa jotkin IoT-järjestelmään kuuluvat laitteet käyttävät tehonsäästöä?

- Miten laitteen toiminnan luotettavuus ja turvallisuus on huomioitu virransäästötilassa?

[GP-PS-03 GP-PS-04]

Miten yksityisyyden suojaaminen on otettu huomioon tarjoamanne IoT-järjestelmän kehityksen ja käytön aikana?

- Miten IoT-järjestelmän käyttäjien ja IoT-mittauskohteen yksilöiden yksityisyyden suojaaminen on toteutettu?
- Miten käsittelemänne tieto on kuvattu ja miten siitä kerrotaan käyttäjille?
- Onko järjestelmän tarjoamaa yksityisyyden suojaa arvioitu suhteessa
  - paikalliseen lainsäädäntöön ja kulttuuriin,
  - mihin tarkoitukseen ja missä käyttötapauksissa järjestelmää käytetään?

[GP-PS-08 GP-PS-09]

Miten tarjoamanne IoT-järjestelmän sisältämät riskit on tunnistettu ja arvioitu?

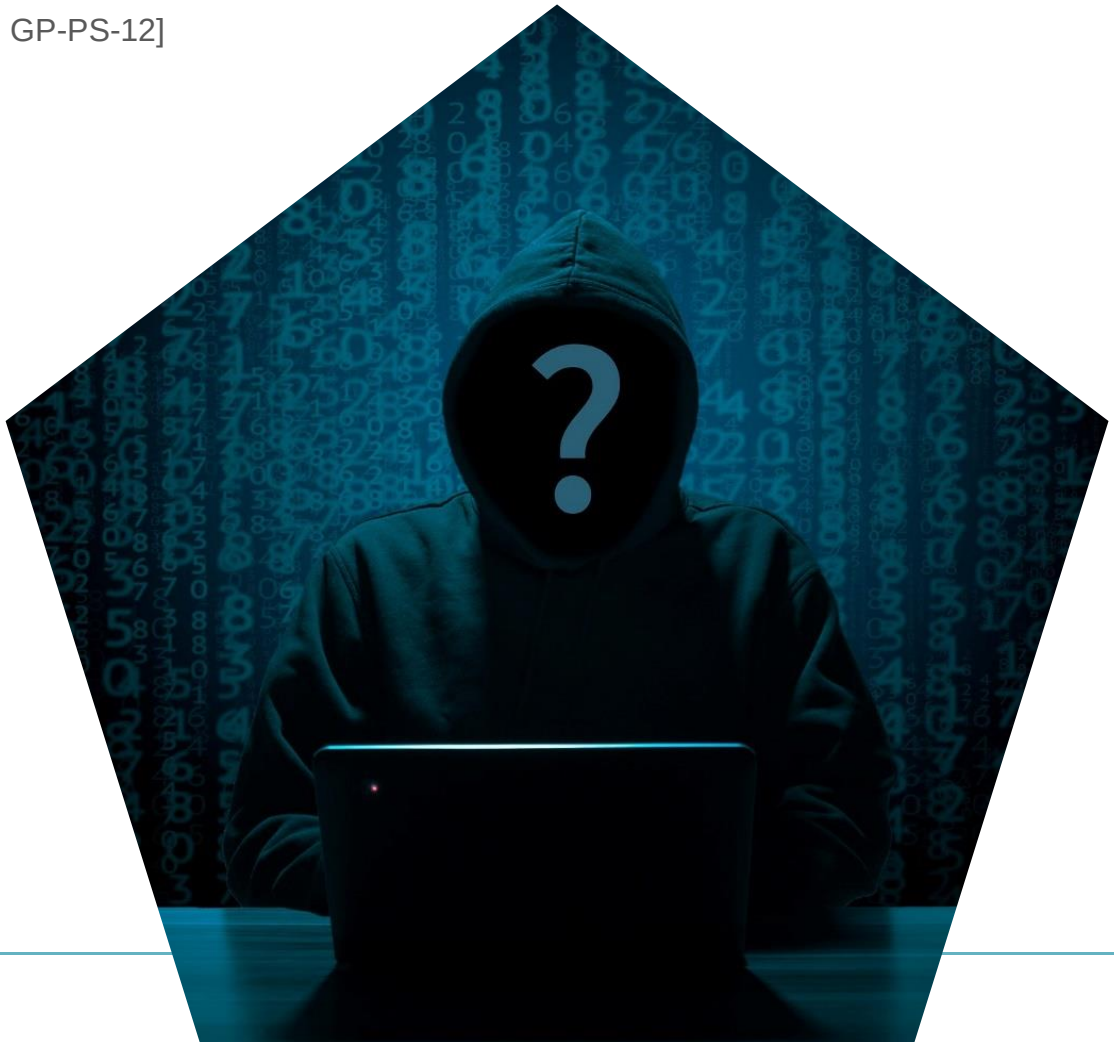
- Onko IoT-järjestelmän toiminnallisuus, käyttötarkoitus ja -ympäristö kuvattu?
- Onko riskien arviointiin otettu mukaan järjestelmässä käytetyt kolmannen osapuolen ohjelmistot, komponentit ja palvelut?
    - Kuka vastaa kolmannen osapuolen toimittamien osien kyberturvallisuuden seuraamisesta ja ratkaisujen arvioinnista?
- Onko IoT-järjestelmän riskejä arvioitu suhteessa
    - paikalliseen lainsäädäntöön ja kulttuuriin,
    - mihin tarkoitukseen ja missä käyttötapauksissa järjestelmää käytetään?

[GP-PS-11 GP-PS-12]

Miten omaisuuden hallinta on otettu huomioon tarjoamanne IoT-järjestelmän kehityksen ja käytön aikana?

- Miten konfiguraation hallita on toteutettu tarjoamassanne IoT-järjestelmässä?

[GP-PS-10]



ORGANISAATIOON, HENKILÖSTÖÖN JA PROSESSEIHIN LIITTYVIÄ KYSYMYKSIÄ

Kuinka tarjoamanne IoT-järjestelmän turvallisuudesta huolehditaan käyttöiän lähestyessä loppua ja sen loputtua?

- Kuinka pitkään toimittamanne IoT-järjestelmän tuki jatkuu?
  - Kuinka pitkään järjestelmän pilvipalvelussa toteutetut osat on tuettu?
  - Kuinka pitkään järjestelmään kuuluvat IoT-laitteet on tuettu?
    - Miten IoT-laitteet päivitetään?
    - Pitääkö laitteet vaihtaa niiden päivittämiseksi?
  - Kuinka pitkään järjestelmän eri osiin on saatavilla kriittisiä korjauksia (käyttöiän mukaisten päivitysten loputtua) tietoturvan tai yksityisyyden vaarantaviin vikoihin?
- Miten seuraatte sitä, että esiintyykö toimittamassanne järjestelmässä uusia tietoturvaongelmia?
  - Kuinka kauan seuraatte uusien vikojen esiintymistä toimituksessa?
  - Miten ilmoitatte vioista asiakkaalle?

[GP-OP-01 GP-OP-02 GP-OP-03]

Onko tarjoamanne IoT-järjestelmän toteuttamisessa käytetty yleisesti hyviksi tunnettuja ratkaisuja?

- Perustuvatko järjestelmässä käytetyt tietoliikenneprotokollat ja salausalgoritmit avoimiin standardeihin vai suljettuihin (*proprietary*) ratkaisuihin?
  - Miksi käytetyt ratkaisut on valittu?
  - Käytetäänkö salausalgoritmien toteutuksessa valmiita kirjastoja vai onko toteutus tehty itse?
  - Mitkä järjestelmässä käytetty ratkaisut ovat suljettuja? Miksi ne eivät ole avoimia?

[GP-OP-04]

Miten etsitte, analysoitte ja käsittelette haavoittuvuuksia ja tietoturvaloukkauksia?

- Miten ja mille tahoille ilmoitatte löydetyistä haavoittuvuuksista ja tietoturvaloukkauksista?
- Mitä tahoja (verkkopalveluita, sähköpostilistoja yms.) seuraatte saadaksenne tietoa haavoittuvuuksista jotka voivat koskea teidän toimittamianne IoT-järjestelmiä tai niissä käytettyjä kolmannen osapuolen toimittamia palveluja, ohjelmistoja tai laitteita?
- Miten ulkopuolisen tahon löytämä haavoittuvuus voidaan ilmoittaa teille?
  - jotka liittyvät käyttämiinne ja toimittamiinne IoT-järjestelmiin
- Oletteko osallistunut tai osallistumassa *bug-bounty* -ohjelmiin tai vastaaviin?

[GP-OP-05 GP-OP-06 GP-OP-07 GP-OP-08]

IoT – TOIMITTAJIEN JA RATKAISUJEN ARVIOINTI

Tarkastuslista

Millaista tietoturvaan ja yksityisyyteen liittyvää koulutusta olette järjestäneet henkilöstöllenne?

- Kuinka usein koulutuksia järjestetään?
- Kuinka seuraatte ketkä henkilöstöstänne ovat käyneet tietoturvakoulutuksissa?

[GP-OP-10]

Kuka omistaa tarjoamanne IoT-järjestelmän tuottaman datan?

- Oletteko varmistaneet datan omistajuuden sopimuksilla?
- Käsitelläänkö toimittamanne IoT-järjestelmän dataa kolmannen osapuolen käyttämissä pilvipalvelussa?
    - Miten kolmas osapuoli suojaa käsittelemänsä datan?
    - Miten kolmas osapuoli ilmoittaa, jos heidän säilyttämänsä dataan kohdistuu tietoturvaloukkauksia?

[GP-OP-12 GP-OP-13]

Kuinka olette arvioineet käyttämienne laitteisto- ja ohjelmistotoimittajien kyberturvallisuuden?

- Onko käyttämillänne toimittajilla heidän johtonsa hyväksymä tietoturvapolitiikka joka ohjaa tietoturvan toteuttamista?
- Millaisia teknisiä kyberturvaratkaisuja käyttämänne toimittajat käyttävät?
- Miten käyttämänne toimittajat ilmoittavat havaitsemistaan haavoittuvuuksista ja tietoturvaloukkauksista teille?
    - Entä heidän käyttämänsä kolmannet osapuolet?

[GP-OP-14]

TEKNISEEN TOTEUTUKSEEN LIITTYVIÄ KYSYMYKSIÄ

Miten tarjoamassanne IoT-järjestelmässä on estetty se, ettei järjestelmän jonkin osan vikaantuessa aiheudu henkilö- tai ympäristövahinkoja?

- Osaavatko kriittiset IoT-järjestelmään kuuluvat osat, esimerkiksi pilvipalvelu tai IoT-yhdyskäytävä, tehdä itsenäistä vianmääritystä tai häiriötilanteesta elpymistä?
- Kykenevätkö järjestelmään kuuluvat IoT-päätelaitteet itsenäiseen toimintaan (ilman verkkoyhteyttä)?
- Miten IoT-päätelaitteet ja -yhdyskäytävät toimivat, jos ne menettävät yhteyden käyttämäänsä pilvipalveluun?
- Menevätkö järjestelmän eri osat, kuten IoT-päätelaitteet, sammuessaan tunnettuun turvalliseen tilaan?

[GP-TM-15 GP-TM-16 GP-TM-17 GP-TM-06]

Miten IoT-laitteiden todentaminen (*authentication*) on toteutettu tarjoamassanne IoT-järjestelmässä?

- Miten IoT-päätelaitteet ja -yhdyskäytävät liittyvät todennetusti muuhun järjestelmään?
- Miten laitteiden ja yhdyskäytävien salasana/tunniste voidaan vaihtaa)?

[GP-TM-21 GP-TM-22]

Miten IoT-järjestelmän käyttäjien todentaminen (*authentication*) on toteutettu tarjoamassanne IoT-järjestelmässä?

- Pakotetaanko järjestelmän oletuskäyttäjätilien ja salasanojen vaihtaminen?
- Miten varmistetaan salasanojen riittävä pituus?
  - Onko järjestelmässä mahdollista käyttää monivaiheista todennusta (MFA - *Multi-Factor Authentication*)
- Eihän salasanoja ole talletettu selväkielisenä IoT-järjestelmässä?
  - Miten salasanat on suojattu?
- Miten salasanojen palauttaminen on suojattu?

[GP-TM-23 GP-TM-24 GP-TM-26]

Miten todentaminen (*authentication*) käyttäytyy poikkeustilanteessa?

- Kuinka monta kertaa IoT-järjestelmä antaa käyttäjän yrittää virheellistä salasanaa?
  - Mitä sen jälkeen tapahtuu?
- Havaitseeko IoT-järjestelmä, jos siihen yritetään tunkeutua kokeilemalla salasanoja (*brute-force attack*)?
  - Miten järjestelmä toimii, kun se havaitsee salasanojen kokeilua?
- Palautuuko järjestelmä jossain tilanteissa oletustunnuksiin ja -salasanoihin?
  - Missä tapauksissa?
  - Miten näissä tapauksissa laite voidaan kytkeä uudestaan toimittajan palveluun – vai voidaanko?

[GP-TM-25]

Millaisia tietoturvaominaisuuksia tarjoamassanne IoT-järjestelmässä on?

- Ovatko tietoturvaominaisuudet ja turvalliset asetukset käytössä oletusarvoisesti?
  - Onko jokaisella toimitetulla järjestelmällä oma yksilöllinen oletussalasanansa joka ei ole laskettavissa joistakin sen ominaisuuksista?
  - Onko järjestelmästä oletusarvoisesti poistettu käytöstä tarpeettomat palvelut ja ohjelmistot sekä fyysiset liittimet kuten USB?

[GP-TM-08 GP-TM-09]

Miten toimittamanne IoT-järjestelmää päivitetään?

- Onko järjestelmään kuuluvien IoT-päätelaitteiden ja -yhdyskäytävien ohjelmistoja mahdollista päivittää turvallisesti langattoman yhteyden yli (OTA - *over-the-air*)?
- Miten päivityspakettien turvallisuus on varmistettu?
  - Onko päivityspaketit allekirjoitettu?
  - Kenen toimittamalla varmenteella?
- Onko päivitykset mahdollista automatisoida?
  - Onko automaattinen päivittäminen oletuksena päällä?
- Onko käyttäjillä mahdollisuus päättää, mitkä päivitykset asennetaan?
- Säilyvätkö käyttäjän laitteeseen tekemät asetukset päivityksen yhteydessä?
- Jos päivitys epäonnistuu, mihin tilaan IoT-laite käynnistyy?
  - Palaako IoT-laite oletustilaan, edelliseen versioon vai johonkin muuhun tilaan?

[GP-TM-05 GP-TM-18 GP-TM-19 GP-TM-20]

Miten tarjoamanne IoT-järjestelmän muuttumattomuus ja eheys (*integrity*) on suojattu?

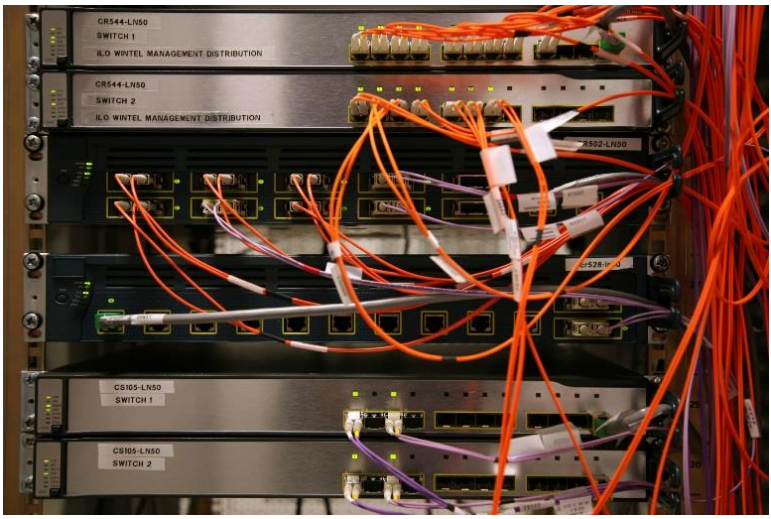
- Miten järjestelmän käynnistyminen luotettuun tilaan on varmistettu?
  - Suojataanko järjestelmää käyttämällä
    - luotettua suojattua käynnistystä (*trusted boot*, *TPM - Trusted Platform Module*), ja
    - laitteessa olevan käyttöjärjestelmän, ohjelmistojen ja asetusten allekirjoituksia?
  - Käynnistyykö järjestelmä turvalliseen tilaan myös virhetilanteen jälkeen?

[GP-TM-06]

Miten laitteen eheys (*integrity*) ja luottamuksellisuus (*confidentiality*) on suojattu pääsynvalvonnalla (*access control*)?

- Voidaanko laitteissa käyttää eri tilanteisiin ja ympäristöihin soveltuvia tietoturvatasoja?

[GP-TM-29 GP-TM-30]



Miten IoT-päätelaitteet ja -yhdyskäytävät ovat suojattu fyysisiä hyökkäyksiä vastaan?

- Voidaanko IoT-laitteen data tyhjentää etähallinnalla, jos se on varastettu?
- Havaitsevatko IoT-laitteet luvattoman muuttamisen (*tamper*) ja miten muuten ne on suojattu?
- Havaitsevat IoT-laitteet, jos niitä yritetään purkaa ja miten ne toimivat sellaisessa tilanteessa?
- Onko IoT-laitteiden tallennusjärjestelmät suojattu salauksella?
- Onko laitteen fyysiset portit, kuten USB, suojattu tai onko ne mahdollista ottaa pois käytöstä?

[GP-TM-31 GP-TM-32 GP-TM-33]

Miten tiedon siirto ja säilytys on suojattu tarjoamassanne IoT-järjestelmässä?

- Mitä salausmenetelmiä ja -protokollia järjestelmässä on käytettävissä?
  - Miksi ne on valittu?
  - Onko käytetyt salausalgoritmit toteutettu käyttäen luotettavia kirjastoja vai oletteko koodanneet ne itse?
  - Miten kirjautuminen ja siihen liittyvä dataliikenne mukaan lukien salasanat on suojattu?
- Kuinka järjestelmän eri osat mukaan lukien IoT-laitteet, IoT-yhdyskäytävät ja pilvipalvelussa olevat ohjelmistot todentavat (*authenticate*) toisensa?
  - Miten eri laitteet, mukaan lukien päätelaitteet ja yhdyskäytävät, toimivat havaitessaan luvattoman yhteydenoton?

[GP-TM-38 GP-TM-39 GP-TM-40 GP-TM-41 GP-TM-42 GP-TM-43 GP-TM-44]

Miten tarjoamanne IoT-järjestelmän käyttämä salaus ja avainten hallinta on toteutettu?

- Mitä salausalgoritmeja ja avainten pituuksia järjestelmässä käytetään?
- Miten avainten luominen, jakaminen, vaihtaminen ja säilyttäminen on toteutettu?
  - Miten riittävä satunnaisuus on varmistettu avaimia luotaessa?
- Miten järjestelmässä käytetty salaus ja avaintenhallinta skaalautuvat siihen kuuluviin IoT-päätelaitteisiin?
  - Miten salaus on toteutettu niissä järjestelmään kuuluvissa laitteissa, joissa on vain vähän laskentakapasiteettia ja tehoresursseja käytössä?
    - Miten salausavain jaetaan järjestelmässä esimerkiksi pieniin antureihin?

[GP-TM-34 GP-TM-35 GP-TM-36 GP-TM-37]

Miten valtuuttaminen (*authorization*) on toteutettu järjestelmässä?

- Käyttävätkö järjestelmässä olevat sovellukset esimerkiksi pienimmän valtuuden periaatetta (PoLP - *the Principle of least privilege*)?
- Onko järjestelmässänne etuoikeutettuja ohjelmia tai ohjelmakoodia (*privileged code*)?
- Miten järjestelmässä etuoikeutettu koodi, prosessit ja data on suojattu?

[GP-TM-27 GP-TM-28]

Miten tarjoamanne IoT-järjestelmä on suojattu verkkohyökkäyksiä vastaan?

- Miten järjestelmää on kovennettu tai miten sitä olisi mahdollista koventaa?
  - Voidaanko esimerkiksi tiettyjä tietoliikenneprotokollia tai portteja sulkea pois käytöstä?
- Onko laitteissa mahdollista rajoittaa tulevan ja lähtevän tietoliikenteen lähteitä ja -kohteita, sekä dataliikenteen määrää?
- Tukeeko IoT-järjestelmä siihen kuuluvien IoT-laitteiden ja yhdyskäytävien jakamista alueisiin?
- Suojaavatko järjestelmässä käytetyt tietoliikenneprotokollat tai muut tietoturvaratkaisut tilanteessa jossa yksi verkkoon kuuluvista laite on joutunut hyökkääjän haltuun?
  - Käyttävätkö kaikki saman tuoteperheen laitteet samaa salausavainta?
- Miten järjestelmä käyttäytyy, jos siihen kohdistetaan palvelunestohyökkäys?
  - Miten järjestelmä toipuu palvelunestohyökkäyksen jälkeen?
- Miten järjestelmälle (ja sen Web-rajapinnalle) annetut syötteet tarkastetaan ennen niiden prosessointia?

[GP-TM-45 GP-TM-46 GP-TM-50 GP-TM-47 GP-TM-48 GP-TM-49 GP-TM-51]

Miten järjestelmän Web-rajapinta on suojattu verkkohyökkäyksiä vastaan?

- Miten järjestelmän Web-rajapinta on suojattu ja kovennettu hyökkäyksiä vastaan?
  - Onko Web-rajapinta testattu esimerkiksi haavoittuvuusskannereilla tai käyttämällä eettisiä hakkereita?
- Missä tilanteissa järjestelmä ja sen Web-rajapinta tuottavat ulospäin näkyviä virheilmoituksia?
  - Miten järjestelmän tuottamat ilmoitukset ja sille annetut syötteet suodatetaan?
  - Onko virheilmoituksista mahdollista päätellä järjestelmän ominaisuuksia?

[GP-TM-52 GP-TM-53 GP-TM-54]

Onko järjestelmän toteutuksessa käytetty laitteistopohjaisia tietoturvamekanismeja?

- Käytetäänkö järjestelmässä esimerkiksi
  - luotettua suojattua käynnistystä (*trusted secure boot*),
  - luotettua ajoympäristöä (*trusted execution* environment),
  - kriittisten muistialueiden suojausta,
  - tallennusjärjestelmän salausta, tai
  - luvattoman järjestelmän muuttamisen (*tamper*) havainnointia.

[GP-TM-01 GP-TM-02 GP-TM-03]

Miten järjestelmä noudattaa tietosuojalakeja, kuten GDPR-asetus?

- Miten IoT-järjestelmän käyttäjät voivat vaikuttaa siihen mitä ja kuinka paljon järjestelmä kerää heistä tietoa?
    - (tai esimerkiksi henkilöt jotka ovat samassa tilassa missä IoT-päätelaite tekee mittauksia)
- Miten varmistetaan se, että kerättyä tietoa käytetään vain ilmoitettuun tarkoitukseen?
    - Miten käyttötarkoituksen muutos ilmoitetaan?
- Miten IoT-järjestelmän käyttäjät voivat tarkastaa, hakea, korjata ja poistaa IoT-järjestelmän heistä keräämää tietoa?
    - (tai esimerkiksi henkilöt jotka ovat samassa tilassa missä IoT-päätelaite tekee mittauksia)

[GP-TM-10 GP-TM-11 GP-TM-12 GP-TM-13 GP-TM-14]

Miten tarjoamassanne IoT-järjestelmässä monitoroidaan siihen kuuluvien laitteiden toimintaa ja häiriöitä?

- Havaitseeko monitorointi myös IoT-järjestelmään tai sen osiin kohdistuvia verkkohyökkäyksiä?
- Tehdäänkö tarjoamallenne IoT-järjestelmälle tietoturva-auditointeja ja/tai -testausta?

[GP-TM-56 GP-TM-57]

Miten tarjoamanne IoT-järjestelmän tapahtumat talletetaan lokeihin ja miten lokit on suojattu?

- Mitkä tapahtumat talletetaan ja kuinka pitkäksi aikaa?
    - Mihin lokit tallennetaan
    - Miten lokit on suojattu luvatonta muuttamista tai poistamista vastaan?
- Miten ja kuinka nopeasti lokit saadaan tutkittavaksi?
    - Voidaanko lokeja tutkia, jos IoT-järjestelmällä ei ole yhteyttä sen toteutuksessa käytettyyn pilvipalveluun?
    - Onko käyttäjällä mahdollisuus saada lokitiedot jotka koskevat hänen omaa toimintaansa tai omia laitteitansa?

[GP-TM-55]