IEC 62443-4-1:2018 Turvallisen tuotekehityksen elinkaari teollisuusautomaatiossa

Turvallisen kehittämisen elinkaari, kahdeksan käytäntöä

47 vaatimusta. Tämän standardin mukainen sertifiointi on mahdollista akkreditoidussa sertifiointielimessä. Versio 07/2026.

IEC 62443-4-1 on sertifioitavissa, mutta kohde on epätavallinen: sertifioidaan nimetyn kehitysorganisaation kehitysprosessi, eli yksi konkreettinen dokumentoitu versio turvallisen kehittämisen elinkaaresta. Tuotetta tai henkilöä ei sertifioida. Reitit ovat ISASecure SDLA ja IECEE CB Scheme. Nykytilanteen mukaan tällainen sertifikaatti ei luo vaatimustenmukaisuusolettamaa EU:n Cyber Resilience Act -asetuksen suhteen. Tämä on eri asia kuin IEC 62443-4-2, joka asettaa vaatimuksia itse komponentille. Tämä lista on työkalu itsearviointiin, ei osoitus vaatimustenmukaisuudesta.

Yritys	Päivämäärä	Täyttäjä

5 Käytäntö 1: Turvallisuuden hallinta (SM) 13

SM-1 Asiakirja

Määritelty tuotekehityksen elinkaari on olemassa ja se kuljettaa turvallisuutta mukana kaikissa vaiheissa ensimmäisestä ideasta tuotteen käytöstä poistoon, ja tämän elinkaaren mukaan myös todellisuudessa työskennellään.

Mistä sen tunnistaa: Prosessikuvaus tai työohje, jossa luetellaan vaiheet, kunkin vaiheen tuotokset ja luovutuspisteet, ja lisäksi näyttö käynnissä olevasta hankkeesta siitä, että vaiheet todella käytiin läpi. Pieni yritys pärjää yhdellä sivulla vaihetta kohden ja tikettijärjestelmässä olevalla tarkistuslistalla; olennaista on, että dokumentoitu prosessi ja arjen käytäntö vastaavat toisiaan.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SM-2 Asiakirja

Jokaiselle turvallisen kehittämisen elinkaaren tehtävälle on määritelty vastuuhenkilö, ja tämä jako on osallisten tiedossa.

Mistä sen tunnistaa: Roolien ja vastuiden matriisi, jossa jokainen prosessin vaihe on liitetty nimettyyn rooliin, täydennettynä roolien nykyisellä miehityksellä. Muutaman hengen yrityksessä riittää taulukko, jossa on rooli, tehtävä ja henkilö; tärkeintä on sijaisjärjestely loman ja sairauden varalle.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SM-3 Asiakirja

Jäljitettävällä tavalla on määritelty, mitkä tuotteet, variantit, julkaisut ja komponentit kuuluvat turvallisen kehittämisen elinkaaren piiriin ja mitkä eivät.

Mistä sen tunnistaa: Luettelo soveltamisalaan kuuluvista tuotteista ja versiotiloista perusteluineen sille, mitä sisällytetään ja mitä rajataan ulos, ylläpidettynä jokaisen uuden julkaisun yhteydessä. Käytännössä toimii hyvin tuoteyhteenvedon sarake, jossa on rivikohtaisesti kyllä tai ei ja yksi lause perusteluksi.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SM-4

Turvallisuustehtäviä hoitavilla henkilöillä on niihin tarvittava tekninen pätevyys, ja tätä pätevyyttä kartutetaan ja päivitetään suunnitelmallisesti.

Mistä sen tunnistaa: Pätevyysprofiili kutakin turvallisuusroolia kohden, pätevyystallenteet, koulutussuunnitelma ja osallistumistallenteet, täydennettynä yhteenvedolla puutteista. Pienet yritykset osoittavat tämän todistuksilla, osallistumisilla konferensseihin tai webinaareihin ja lyhyellä vuosittaisella läpikäynnillä siitä, kuka sulkee minkä puutteen ja mihin mennessä, tarvittaessa ostamalla asiantuntemusta ulkopuolelta.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SM-5 Asiakirja

Turvallisen kehittämisen elinkaaren soveltamisala on rajattu ja siinä nimetään mukana olevat toimipaikat, organisaatioyksiköt, toimittajien osuudet ja kehitysympäristöt sekä tämän alueen rajat.

Mistä sen tunnistaa: Soveltamisalan kuvaus, jossa ovat toimipaikat, tiimit, ulkoistetut osuudet ja järjestelmät, sekä luonnos ulkoisista rajapinnoista. Yhdellä toimipaikalla kehittävä yritys kirjaa tämän muutamaan lauseeseen ja nimeää nimenomaisesti sen, mikä jää ulkopuolelle, esimerkiksi muualla kehitetyt kokoonpanot tai kolmannen osapuolen tarjoama palvelinpalvelu.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SM-6 **Jokaisen käyttäjille toimitettavan osan, ohjelmiston, laiteohjelmiston, konfiguraatioiden ja mukana tulevien tiedostojen eheys on tarkistettavissa, jolloin vastaanottaja havaitsee huomaamatta tehdyt muutokset.**

Mistä sen tunnistaa: Allekirjoitukset tai julkaistut tarkistussummat kutakin toimituspakettia kohden, menetelmän kuvaus ja yksi esimerkki todellisesta julkaisusta yhdessä asiakkaalle tarkoitetun ohjeen kanssa siitä, miten tarkistus tehdään. Pienelle tiimille riittää allekirjoitettu tarkistussummatiedosto latauksen vieressä ja yksi kappale julkaisutiedotteessa.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SM-7 **Ympäristöt, joissa kehitetään, käännetään ja testataan, on suojattu luvattomalta pääsyltä sekä lähdekoodin, käännöstyökalujen ja artefaktien manipuloinnilta.**

Mistä sen tunnistaa: Pääsynhallinnan periaatteet versionhallinnalle, käännöspalvelimelle ja testijärjestelmille, käyttöoikeuslistat viimeisimmän katselmoinnin päiväyksellä, tallenteet turvallisuuden kannalta merkityksellisistä muutoksista ja näyttö tuotantokäyttöoikeuksien ja kehityskäyttöoikeuksien erottamisesta. Ilman omaa tietohallintoa riittävät kaksivaiheinen kirjautuminen, suojattu päähaara pakollisine katselmointeineen ja puolivuosittainen läpikäynti siitä, kenellä on yhä pääsy.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SM-8 **Yksityiset avaimet, joilla toimitukset allekirjoitetaan, on suojattu paljastumiselta ja väärinkäytöltä, ja niiden käyttö on rajattu valtuutettuihin henkilöihin ja järjestelmiin.**

Mistä sen tunnistaa: Kuvaus avainten säilytyksestä, käytöstä, uusimisesta ja sulkemisesta, näyttö suojatusta säilytyksestä, esimerkiksi laitepohjainen suojausavain tai avaintenhallintapalvelu, sekä tallenteet allekirjoitustapahtumista. Pieni yritys säilyttää allekirjoitusavaimen laitepohjaisella suojausavaimella, dokumentoi ne kaksi henkilöä, joilla on pääsy, ja sillä on valmiina menettely katoamistilanteen varalle.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SM-9 **Ostetuille tai käyttöön otetuille komponenteille, avoimen lähdekoodin ohjelmistot mukaan lukien, on määritelty toimittajaan kohdistuvat turvallisuusodotukset, ja niitä sovelletaan valinnassa.** Asiakirja

Mistä sen tunnistaa: Turvallisuusvaatimukset toimittajamäärittelyissä tai sopimuksissa, valintakriteerit kolmannen osapuolen komponenteille, luettelo kaikista kolmannen osapuolen komponenteista versioineen ja lähteineen sekä arvio siitä, täyttääkö toimittaja odotukset. Ilman hankintaosastoa riittää ylläpidetty komponenttiluettelo, jossa on sarake sille, onko toimittajan turvapäivitykset ja ilmoituskanavat tarkastettu.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SM-10 **Kolmannen osapuolen tilauksesta kehittämiä komponentteja koskevat samat turvallisuusvaatimukset kuin omaa kehitystä, ja noudattaminen todennetaan.**

Mistä sen tunnistaa: Ostotilaus tai sopimusasiakirjat, joissa vaaditut turvallisuusvelvoitteet ilmenevät, palveluntarjoajan näyttö sovelletuista käytännöistä, hyväksymistallenteet ja omien tarkastusten tulokset toimitetusta työstä. Ilman auditointibudjettia riittävät sopimuksessa annettu vakuutus, palveluntarjoajan testitulosten toimittaminen ja yksi oma pistokoe ennen hyväksymistä.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SM-11 **Turvallisuuteen liittyvät havainnot kaikista lähteistä, testeistä, katselmoinneista, käyttäjäilmoituksista ja kolmansien osapuolten tiedotteista, kirjataan, niiden vaikutus arvioidaan, niille osoitetaan vastuuhenkilö ja määräaika, ja niitä seurataan sulkemiseen asti.** Asiakirja

Mistä sen tunnistaa: Vikajärjestelmä tai tikettijärjestelmä, jossa on oma merkintä turvallisuusaiheille, ja kussakin merkinnässä vaikutusarvio, vastuuhenkilö, määräaika ja sulkemismerkintä, sekä raportti avoimista kohdista. Pieni tiimi käyttää olemassa olevan tikettijärjestelmän tunnistetta ja viikkopalaverin vakioaihetta.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SM-12 **Ennen tuotteen julkaisua todennetaan ja osoitetaan, että turvallisen kehittämisen elinkaaren suunnitellut vaiheet on todella tehty ja että niihin liittyvät tallenteet on laadittu.** Asiakirja

Mistä sen tunnistaa: Julkaisukatselmointi kutakin julkaisua kohden prosessin vaiheita vasten, viittaukset kyseisiin tallenteisiin ja dokumentoitu julkaisupäätös päiväyksineen ja allekirjoituksineen. Käytännössä toimii hyvin julkaisun tarkistuslista, joka ei salli toimitusta ilman täysiä merkintöjä; avoimet kohdat perustellaan ja niille annetaan päivämäärä.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SM-13 **Turvallisen kehittämisen elinkaarta itseään haastetaan ja parannetaan säännöllisesti hyödyntäen havaintoja tapahtumista, testituloksista, asiakaspalautteesta ja uhkakuvan kehityksestä.**

Mistä sen tunnistaa: Tallenteet prosessin katselmoinnista, esimerkiksi johdon katselmuksesta tai retrospektiivistä, käynnistetyt prosessimuutokset, niiden toteutustilanne ja viittaus juurisyyhyn. Standardin kypsyystasoja käyttävä yritys kirjaa nykytilan ja tavoitteen kutakin käytäntöä kohden; kypsyystaso 4 edellyttää juuri tätä näyttöä jatkuvasta parantamisesta. Pienelle yritykselle riittää yksi kokous vuodessa pöytäkirjoineen ja kolme konkreettista parannusta.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

6 Käytäntö 2: Turvallisuusvaatimusten määrittely (SR) 5

SR-1 **Tuotteen aiottu toimintayhteys on kuvattu: odotettu käyttöympäristö, ympäristön oletetusti tarjoamat turvatoimet, aiotut käyttäjäryhmät ja roolit, oletetut luottamusrajat sekä ne käyttötavat, joihin tuotetta ei nimenomaisesti ole tarkoitettu.** Asiakirja

Mistä sen tunnistaa: Kuvaus tuotteen turvallisuusyhteydestä joko omana asiakirjanaan tai tuotemäärittelyn kiinteänä osana, sisältäen verkkoympäristön, oletetut ulkoiset suojaukset, esimerkiksi palomuurin tai fyysisen pääsynhallinnan, roolien luettelon ja nimenomaisen luettelon soveltamisalan ulkopuolisista käyttötavoista. Pienellä yrityksellä tämä on kahden sivun mittainen, mukana yksinkertainen luonnos laitosympäristöstä, ja tuotevastaava päivää ja hyväksyy sen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR-2 **Tuotteelle on olemassa uhkamalli, joka kuvaa tietovirrat, rajapinnat, luottamusrajat ja hyökkäyspolut, nimeää niistä seuraavat uhkat ja niiden mahdollisen vaikutuksen sekä osoittaa vastatoimet. Se katselmoidaan ja päivitetään merkityksellisten muutosten yhteydessä ja vähintään kerran tuotejulkaisua kohden, ja avoimia kohtia seurataan siihen asti, kunnes ne on suljettu.** Asiakirja

Mistä sen tunnistaa: Uhkamalli tietovirtakaavioineen, uhkaluettelo kutakin rajapintaa kohden, osoitetut vastatoimet ja avoimien kohtien tila sekä muutoshistoria päiväyksineen ja tekijöineen. Pieni yritys pärjää yhdellä taulukolla rajapintaa kohden, sarakkeina se, mikä siinä voi mennä pieleen, kuinka paha se olisi, mitä sille tehdään ja kuka sen katselmoi.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR-3 **Tuotteen turvallisuusvaatimukset on määritelty ja dokumentoitu. Ne kattavat uhkamallin tulokset, kuvatun tuotteen turvallisuusyhteyden, sovellettavat lakisääteiset ja sopimusperusteiset velvoitteet sekä tavoitellun turvallisuustason, ja niihin sisältyvät turvallisuustoiminnot, jotka tuote itse tarjoaa.** Asiakirja

Mistä sen tunnistaa: Vaatimusluettelo tai vaatimustenhallinnan työkalu, jossa on yksilöivä tunniste kutakin vaatimusta kohden, kunkin merkinnän lähde, esimerkiksi uhka, asiakassopimus tai lakisääteinen velvoite, ja tavoiteltu turvallisuustaso. Pieni yritys hoitaa tämän yhtenä taulukkona, jossa on kiinteä tunnistesarake, johon todentaminen ja testaus myöhemmin kiinnittyvät.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR-4 **Jokainen yksittäinen turvallisuusvaatimus on muotoiltu yksiselitteiseksi, ristiriidattomaksi, testattavaksi ja jäljitettäväksi tiettyyn tuotteen toimintoon tai rajapintaan, ja se sisältää tiedon, jolla se voidaan myöhemmin todentaa ilman lisäselvityksiä.**

Mistä sen tunnistaa: Otos vaatimusluettelosta, jossa kutakin vaatimusta kohden näkyvät mitattava hyväksymiskriteeri ja kyseinen toiminto tai rajapinta, sekä vaatimusten ja testitapausten välinen vastaavuus. Pieni yritys varmistuu tästä kiinteällä muotoilupohjalla ja kontrollikysymyksellä siitä, voiko vaatimuksesta kirjoittaa testitapauksen ilman lisäkysymyksiä.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR-5 **Turvallisuusvaatimukset katselmoidaan ennen kuin niitä käytetään suunnittelussa ja toteutuksessa, ja mukana ovat asianosaiset, kuten kehitys, testaus, tuotevastuu ja tarvittaessa myynti tai asiakas. Katselmoinnissa tarkastellaan täydellisyyttä uhkamalliin ja tuotteen turvallisuusyhteyteen nähden, oikeellisuutta ja testattavuutta. Havainnot kirjataan ja niitä seurataan sulkemiseen asti.**

Mistä sen tunnistaa: Katselmointitallenne päiväyksineen, osallistujineen ja heidän rooleineen, katselmoitu vaatimusten versio, luettelo havainnoista vastuuhenkilöineen ja sulkemistiloineen sekä hyväksymismerkintä. Pieni yritys hoitaa tämän kahden henkilön katselmointina kehityksen ja testauksen välillä, lyhyellä tallenteella ja hyväksymisrivillä vaatimusluettelossa.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7 Käytäntö 3: Turvallinen suunnittelu (SD) 4

SD-1 **Jokaisella tuotteella on suunnittelukuvaus, joka kattaa arkkitehtuurin turvallisuuden kannalta merkitykselliset osat: mitä komponentteja on, miten ne viestivät keskenään, missä luottamusrajat kulkevat, mitkä ulkoiset rajapinnat ovat avoinna ja millä mekanismeilla aiemmin määritellyt turvallisuusvaatimukset toteutuvat suunnittelussa.** Asiakirja

Mistä sen tunnistaa: Arkkitehtuuriasiakirja tai suunnittelumäärittely, jossa on kaavio komponenteista, tietovirroista ja luottamusrajoista, sekä vastaavuustaulukko kustakin turvallisuusvaatimuksesta siihen suunnittelun osaan, joka sen toteuttaa. Pieni toimittaja pärjää yhdellä ylläpidetyllä kaaviolla ja kahdella tai kolmella sivulla selitystä; olennaista on, että se on versionhallinnassa ja päivittyy aina, kun arkkitehtuuri muuttuu.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SD-2 **Suunnittelu analysoidaan järjestelmällisesti uhkien varalta. Analyysi nimeää hyökkääjän tavoitteet, kyseiset luottamusrajat ja rajapinnat, niistä seuraavat uhkat luokituksineen sekä suunnittelussa tehdyt vastatoimet. Se toistetaan aina, kun arkkitehtuuri tai ympäristö muuttuu olennaisesti, ja tunnistettuja uhkia seurataan siihen asti, kunnes kustakin niistä on tehty päätös.** Asiakirja

Mistä sen tunnistaa: Uhkamalli tuotetta tai pääjulkaisua kohden, esimerkiksi taulukko, jonka sarakkeina ovat uhka, kyseinen rajapinta, luokitus, vastatoimi ja tila, sekä mallinnustilaisuuden muistio, jossa ovat osallistujat ja päiväys. Pieni tiimi mallintaa käytännönläheisesti kahden tai kolmen tunnin työpajassa arkkitehtuurikaavion mukaisesti ja kirjaa avoimet kohdat tiketeiksi, jolloin näyttö seurannasta syntyy ilman lisätyötä.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SD-3 **Suunnittelu noudattaa osoitettavasti tunnustettuja turvallisen suunnittelun periaatteita, muun muassa vähimpien oikeuksien periaatetta, mahdollisimman pientä hyökkäyspintaa, syvyyssuuntaista puolustusta, turvallisia oletusasetuksia, turvalliseen tilaan päätyvää vikakäyttäytymistä ja mahdollisimman yksinkertaisia ja todennettavia turvamekanismeja. Näiden periaatteiden soveltaminen näkyy suunnittelussa ja on perusteltu.**

Mistä sen tunnistaa: Suunnittelukuvauksen luku tai oma suunnitteluohje, jossa periaatteet nimetään, sekä konkreettinen näyttö kustakin periaatteesta tuotteessa, esimerkiksi palveluiden oikeusmatriisi, luettelo avoimista porteista perusteluineen, toimitettavat oletusasetukset tai dokumentoitu virheenkäsittelyn toiminta. Pieni toimittaja käyttää näistä periaatteista lyhyttä tarkistuslistaa suunnittelukatselmoinnin vakiokohtana ja arkistoi täytetyn lomakkeen suunnittelun mukana.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SD-4 **Suunnittelun katselmoivat pätevät kollegat ennen toteutuksen alkua. Katselmoinnissa tarkastellaan täydellisyyttä turvallisuusvaatimuksiin nähden, turvamekanismien oikeellisuutta ja vaikuttavuutta sekä uhka-analyysin tuloksia. Mukana on henkilöitä, joilla on riittävä turvallisuuspätevyys, havainnot kirjataan ja niitä seurataan sulkemiseen asti.** Asiakirja

Mistä sen tunnistaa: Katselmointitallenne päiväyksineen, katselmoitava kohde versioineen, osallistujat rooleineen, luettelo havainnoista tiloineen ja hyväksymispäätös. Pieni tiimi liittää katselmoinnin suunnitteluasiakirjojen muutospyyntöön ja jättää havainnot kommenteiksi sulkemismerkintöineen, mikä osoittaa seurannan ilman lisätyökaluja. Jos turvallisuuspätevyyttä ei ole omasta takaa, käytännöllinen reitti on ulkopuolinen katselmoija tuntiperusteisesti kriittisiä suunnitelmia varten.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

8 Käytäntö 4: Turvallinen toteutus (SI) 2

SI-1 **Toteutuksen todentamiseen turvallista suunnittelua vasten on olemassa määritelty prosessi: katselmoinnissa vahvistetaan, että suunnittelussa ennakoidut suojaustoimet ovat todella olemassa ja vaikuttavia koodissa, että syvyyssuuntainen puolustus säilyy ja että toteutuksen aikana ei ole syntynyt uusia haavoittuvuuksia. Katselmoinnin tekee tehtävään pätevä henkilöstö, ja löytyneet poikkeamat kirjataan ja niitä seurataan sulkemiseen asti.**

Mistä sen tunnistaa: Kirjallinen menettely toteutuksen katselmointiin sekä katselmointitallenteet komponenttia tai julkaisua kohden: katselmoitu moduuli, viittaus suunnitteluasiakirjaan, päiväys, katselmoija, havainnot ja niiden ratkaisutila. Näytöksi käyvät muutospyyntöjen katselmoinnit pakollisine turvallisuustarkistuslistoineen, staattisen koodianalyysin tulokset kunkin osuman dokumentoituine arvioineen ja katselmointitilaisuuksien muistiot. Pieni tiimi kattaa tämän neljän silmän periaatteella, arkistossa olevalla katselmointipohjalla, jossa jokainen suunnittelun toimenpide kuitataan erikseen, ja yhdellä tiketillä avointa havaintoa kohden. Olennaista on, että koodin kirjoittaja ei koskaan ole saman koodin katselmoija.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SI-2 **Sitovat turvallisen ohjelmoinnin säännöt koskevat kaikkea turvallisuuteen liittyvää kehitystyötä ja kattavat vähintään tunnettujen turvattomien rakenteiden ja funktioiden välttämisen, syötteiden ja virheiden käsittelyn, muistin ja resurssien hallinnan sekä tarkastetun turvakoodin käytön itse kirjoitettujen toteutusten sijaan. Säännöt koskevat kutakin käytössä olevaa ohjelmointikieltä, ovat kaikkien kehittäjien tiedossa ja päivittyvät tarvittaessa, esimerkiksi uusien hyökkäystapojen tai uusien työkalujen ilmaantuessa.** Asiakirja

Mistä sen tunnistaa: Hyväksytty turvallisen ohjelmoinnin standardi versiotietoineen, kielikohtaisine soveltamisaloineen ja hyväksymispäiväyksineen, täydennettynä näytöllä siitä, että se vaikuttaa arjen työssä: koodintarkastus- ja analysointityökalujen asetukset versionhallinnassa, käännössääntö, joka nostaa rikkomukset esiin, ja perehdytyksen osallistujaluettelo. Pienet yritykset eivät kirjoita standardia tyhjästä; ne julistavat vakiintuneen julkisen säännöstön sitovaksi, lisäävät lyhyen luettelon omista täydentävistä säännöistään ja ankkuroivat tarkastuksen käännösputkeen, jolloin noudattaminen näkyy automaattisesti.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

9 Käytäntö 5: Turvallisuuden todentava ja kelpuuttava testaus (SVV) 5

SVV-1 **Jokaiselle turvallisuuteen liittyvälle tuotevaatimukselle on osoitettu vähintään yksi testitapaus, joka osoittaa, että suojaava toiminto toimii tarkoitetusti normaalikäytössä, että se käyttäytyy määritellysti virheellisellä syötteellä tai väärinkäytön kohteena ja että tuotteen mukana toimitettavat oletusasetukset vastaavat turvallista tilaa. Suoritus ja tulos kirjataan kustakin testatusta ohjelmistoversiosta.** Asiakirja

Mistä sen tunnistaa: Jäljitettävyysmatriisi, joka yhdistää vaatimuksen testitapaukseen ja tulokseen, sekä testitallenteet, joista näkyvät päiväys, testattu versio tai käännös ja testin tekijän nimi. Pieni toimittaja lisää vaatimusluetteloonsa yksinkertaisesti testitapauksen tunnistesarakkeen ja arkistoi käännösputken automaattisen testiajon lokin tiedostona kyseisen version yhteyteen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SVV-2 **Uhkamallista johdetut vastatoimet testataan nimenomaisesti sen varmistamiseksi, että ne todella sulkevat oletetun hyökkäyspolun. Testaus tehdään tunnistettuja uhkia vastaan, ei pelkkää sääntöjenmukaista käyttöä vasten, ja avoimet kohdat viedään vikojen käsittelyprosessiin.**

Mistä sen tunnistaa: Testitapaukset, jotka viittaavat suoraan uhkamallin merkintöihin, esimerkiksi yksi väärinkäyttötapaus uhkatunnistetta kohden odotettuine puolustautumiskäyttäytymisineen, sekä näiden ajojen tallenteet. Ilman raskasta koneistoa riittää lisätä uhkamalliin sarake, joka viittaa testitapaukseen ja viimeisimmän onnistuneen tarkastuksen päiväykseen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SVV-3 **Tuote tutkitaan järjestelmällisesti haavoittuvuuksien varalta ennen julkaisua. Laajuus kattaa vähintään: ulkoa saavutettavien rajapintojen ja palveluiden tutkimisen, testauksen virheellisellä ja satunnaisesti muunnellulla syötteellä, käytettyjen kolmannen osapuolen komponenttien vertaamisen tunnettuihin ilmoitettuihin haavoittuvuuksiin ja toimittajan oman koodin tarkastamisen tunnettujen heikkousluokkien varalta. Havainnot kirjataan arvioineen.** Asiakirja

Mistä sen tunnistaa: Käytettyjen työkalujen raportit, joissa ilmoitetaan työkalun nimi, versio ja haavoittuvuustietokannan ajantasaisuus, satunnaissyötetestauksen tallenteet, luettelo kolmannen osapuolen komponenteista viimeisimmän vertailun päiväyksellä ja havaintoluettelo arvioineen ja päätöksineen. Pieni toimittaja yhdistää maksuttomat vakiotyökalut, riippuvuuksien skannauksen sekä porttien ja palveluiden skannauksen asennettua tuotetta vastaan ja arkistoi tulosteet julkaisua kohden yhteen kansioon.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SVV-4 **Julkaisuehdokas altistetaan todenmukaisissa oloissa hyökkäysyritykselle, joka aktiivisesti pyrkii ohittamaan suojamekanismit eikä vain tiedustele niiden tilaa. Testin laajuus, reunaehdot ja rajat sovitaan etukäteen, ja löytyneitä heikkouksia käsitellään ja seurataan kuten vikoja.**

Mistä sen tunnistaa: Toimeksianto tai testitilaus, jossa ilmenevät laajuus ja testiympäristö, raportti lähestymistavasta, hyödynnetyistä heikkouksista ja niiden arvioinnista sekä merkinnät vikajärjestelmässä tai tikettijärjestelmässä näyttöineen korjauksesta tai perustellusta riskin hyväksymisestä. Pienet toimittajat ostavat tämän testin tyypillisesti ulkoa rajattuna aikabudjettina tai teettävät sen henkilöllä, joka ei ole kehittänyt tuotetta.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SVV-5 **Testaavan henkilöstön riippumattomuus on määritelty ja se vastaa tavoiteltua kypsyystasoa. Komponentin kehittänyt henkilö ei julkaise sitä pelkästään oman testauksensa perusteella, ja kypsyystason noustessa testauksesta vastaa organisatorisesti erillinen yksikkö tai ulkopuolinen taho. Todellinen vastuunjako on jäljitettävissä kunkin testin osalta.**

Mistä sen tunnistaa: Roolien määrittely kehitysprosessissa siten, että tekeminen ja testaus ovat erillään, sekä kustakin testiajosta tai testiraportista kirjattu testin tekijän nimi ja rooli. Kahden hengen yritys hoitaa tämän keskinäisellä katselmoinnilla ja dokumentoidulla neljän silmän merkinnällä ja ottaa syvälliseen turvallisuustestaukseen mukaan ulkopuolisen henkilön.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

10 Käytäntö 6: Turvallisuusvikojen käsittely (DM) 6

DM-1 **On olemassa määritelty kanava, jonka kautta ilmoitukset tuotteen turvallisuusheikkouksista otetaan vastaan ja kirjataan kaikista suunnista: kehitystiimiltä itseltään, testauksesta ja katselmoinneista, asiakkailta ja integroijilta, ulkopuolisilta ilmoittajilta sekä käytössä olevia kolmannen osapuolen ja avoimen lähdekoodin komponentteja koskevista tiedotteista. Ilmoituskanava on ulkopuolisten löydettävissä, ja jokainen ilmoitus kirjataan vastaanottopäivineen ja lähteineen.** Asiakirja

Mistä sen tunnistaa: Kuvaus ilmoituskanavasta, julkisesti tavoitettava yhteyspiste (turvallisuussivu, security.txt-tiedosto tai postilaatikko, esimerkiksi security@), ja vastaanottorekisteri, jossa on kustakin ilmoituksesta päiväys, lähde ja lyhyt kuvaus. Pieni yritys pärjää yhteisellä postilaatikolla ja yhdellä taulukolla tai tiketin tunnisteella, kunhan jokainen ilmoitus päätyy sinne, myös sisäisessä kehittäjäkeskustelussa esiin nostetut.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

DM-2 **Jokainen saapuva ilmoitus lajitellaan ja tutkitaan sen selvittämiseksi, onko se turvallisuuden kannalta merkityksellinen ja mihin tuotteisiin, versioihin ja komponentteihin se vaikuttaa. Myös ilmoitukset, jotka osoittautuvat turvallisuuden kannalta merkityksettömiksi tai aiheettomiksi, suljetaan perusteluineen eikä niitä hylätä hiljaisesti.**

Mistä sen tunnistaa: Lajittelumerkintä kustakin ilmoituksesta, jossa ilmenevät lopputulos (turvallisuuden kannalta merkityksellinen kyllä tai ei), kyseiset versiot ja tarvittaessa hylkäyksen peruste, näkyvissä tiketissä tai vastaanottoluettelossa. Tiimit, joilla ilmoituksia on vähän, hoitavat lajittelun lyhyessä toistuvassa tilaisuudessa ja kirjaavat lopputuloksen kahdella lauseella merkintää kohden.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

DM-3 **Vahvistetut turvallisuusviat arvioidaan yhtenäisellä menetelmällä: juurisyy, kyseiset versiot ja konfiguraatiot, mahdollinen vaikutus toimintaan ja turvallisuuteen, hyödynnettävyys sekä vakavuus määriteltyä asteikkoa vasten. Arvioinnin tulos kirjataan ja se on jäljitettävissä.** Asiakirja

Mistä sen tunnistaa: Arviointitallenne tai joukko tikettikenttiä kustakin viasta kattaen juurisyyn, vakavuuden ja sovelletun asteikon (esimerkiksi yleisesti käytetty vakavuuden luokittelujärjestelmä dokumentoituine vektoreineen) sekä luettelo kyseisistä versioista. Pienet tiimit nojaavat kiinteään kenttäpohjaan tikettijärjestelmässä ja puoleen sivuun, jossa kuvataan asteikko ja ne rajat, jotka käynnistävät välittömän toiminnan.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

DM-4 **Jokaisesta arvioidusta turvallisuusviasta tehdään päätös sen käsittelystä: korjaus, korvaava toimenpide tai perusteltu riskin hyväksyminen. Päätös seuraa vakavuudesta, sille osoitetaan vastuuhenkilö ja määräaika, ja vikaa seurataan sulkemiseen asti.** Asiakirja

Mistä sen tunnistaa: Toimenpideluettelo tai tikettitila, josta näkyvät vastuuhenkilö, tavoitepäivä, toimenpiteen laji ja sulkemismerkintä, kytkettynä siihen koodiversioon tai julkaisuun, jossa korjaus astuu voimaan. Hyväksytyt jäännösriskit edellyttävät lyhyttä kirjallista perustelua, jonka tuotevastuu hyväksyy. Pienellä yrityksellä tämä on tikettitaulussa määräaikoineen ilman lisätyökaluja.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

DM-5 **Kyseisille käyttäjille, integroijille ja muille sidosryhmille kerrotaan turvallisuusvioista heti, kun arviointi sitä edellyttää, ilmoittaen kyseiset versiot, vaikutuksen ja saatavilla olevan korjauksen tai korvaavan toimenpiteen. Julkistuksen aikataulut ja vastaanottajajoukko on määritelty etukäteen, samoin toimintatapa kolmansien osapuolten ilmoituksiin, joilla on oma julkistusmääräaikansa.**

Mistä sen tunnistaa: Julkaistut turvallisuustiedotteet päiväyksineen ja versioviittauksineen, jakelulista tai tilaajakanava sekä kirjallinen sääntö aikatauluista ja koordinoidusta julkistuksesta. Toimittajat, joilla on vähän asiakkaita, käyttävät yhtä postitusta ylläpidetylle asiakaslistalle sekä päivättyä tiedotesivua, jonka muutokset versioidaan.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

DM-6 **Turvallisuusvikojen käsittely katselmoidaan määräajoin. Katselmoinnissa tarkastellaan avoimia ja myöhässä olevia tapauksia, ilmoituksesta korjaukseen kulunutta aikaa, toistuvia juurisyitä ja tehtyjen toimenpiteiden vaikuttavuutta. Katselmoinnista seuraavat prosessin parannukset toteutetaan ja niiden toteutumista seurataan.** Asiakirja

Mistä sen tunnistaa: Toistuvan katselmoinnin muistio päiväyksineen ja osallistujineen, luvut avoimista ja myöhässä olevista tapauksista sekä luettelo sovituista parannuksista vastuuhenkilöineen ja määräaikoineen. Pieni yritys liittää tämän kohdan olemassa olevaan neljännesvuosikokoukseen ja kokoaa luvut ja päätökset yhdelle sivulle.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

11 Käytäntö 7: Turvapäivitysten hallinta (SUM) 5

SUM-1 **Jokainen tuotteen turvapäivitys todennetaan tuettuja tuoteversioita ja käyttöympäristöjä vasten ennen kuin se julkaistaan asiakkaille, ja olemassa on tallenne siitä, että päivitys sulkee haavoittuvuuden häiritsemättä tuotteen tarkoitettua toimintaa.** Asiakirja

Mistä sen tunnistaa: Testitallenne kutakin korjauspäivitystä kohden kattaen testatun tuoteversion, alustan, testitapaukset (vaikuttavuus haavoittuvuutta vastaan sekä ydintoimintojen regressio) ja julkaisuhyväksynnän. Pieni toimittaja pärjää lyhyellä korjauspäivityksen hyväksymismerkinnällä tiketissä: tiketin tunniste, todentaja, todennuspäivä, tulos, ja liitteenä automaattisen testiajon loki.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SUM-2 **Kaikkien niiden tuotteen komponenttien osalta, joita ei ole kehitetty itse (kolmannen osapuolen kirjastot, käyttöjärjestelmä, ajoympäristöt), on määritelty ja osoitettu, miten niiden turvapäivitykset arvioidaan ja joko otetaan tuotteeseen tai hylätään dokumentoiduin perustein.** Asiakirja

Mistä sen tunnistaa: Komponenttiluettelo kolmannen osapuolen osista versioineen ja lähteineen sekä yksi arviointimerkintä kutakin ilmoitettua kolmannen osapuolen haavoittuvuutta kohden, jossa ilmenevät päätös (otetaan käyttöön, ei koske tuotetta, katetaan korvaavalla toimenpiteellä) ja perustelu. Pienet tiimit ajavat automaattisen riippuvuusskannauksen käännöksessä ja kirjaavat päätökset kommentteina skannauksen tulokseen tai kevyeen poikkeusluetteloon.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SUM-3 **Jokaisen toimitettavan turvapäivityksen mukana käyttäjät saavat ymmärrettävät oheistiedot: mitä tuoteversioita asia koskee, mikä haavoittuvuus korjataan, kuinka vakava se on, onko sivuvaikutuksia tai korvaavia toimenpiteitä huomioitavana ja miten päivitys asennetaan.** Asiakirja

Mistä sen tunnistaa: Julkaistut turvallisuustiedotteet tai julkaisutiedotteet, joissa ilmoitetaan haavoittuvuuden tunniste, kyseiset versiot, vakavuusluokitus, asennusvaiheet ja ohje paluusta edelliseen tilaan. Pienillä toimittajilla on yksi julkinen sivu, jolla turvallisuustiedotteet ovat aikajärjestyksessä, ja he linkittävät siihen tuotteen sisältä.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SUM-4 **On olemassa määritelty ja manipuloinnilta suojattu reitti, jonka kautta käyttäjät saavat turvapäivitykset, ja päivityksen aitous ja eheys on todennettavissa käyttäjän puolella ennen asennusta.**

Mistä sen tunnistaa: Kuvaus toimituskanavasta (latausalue, päivityspalvelin, fyysinen tietoväline) suojaustoimineen sekä digitaalinen allekirjoitus tai tarkistussumma pakettia kohden ja ohje käyttäjälle siitä, miten sen todentaa. Pienet toimittajat toteuttavat tämän allekirjoittamalla käännöspalvelimella, julkaisemalla tarkistussumman latauksen vieressä ja nimeämällä yhden selkeän paikan, jossa julkinen avain on.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SUM-5 **Turvapäivitysten saataville saattamiselle on määritellyt aikatavoitteet, jotka on porrastettu haavoittuvuuden vakavuuden mukaan; toteutuneita aikoja seurataan, ja ylittynyt tavoite perustellaan ja sen tueksi annetaan käyttäjille väliaikainen toimenpide.** Asiakirja

Mistä sen tunnistaa: Sisäinen määrittely, jossa on aikaikkuna kutakin vakavuusluokkaa kohden (esimerkiksi kriittinen <= 30 päivää, korkea <= 90 päivää), ja arviointi kutakin haavoittuvuutta kohden: ilmoituspäivä, korjauspäivityksen julkaisupäivä, kuluneet päivät, poikkeaman syy. Pienillä toimittajilla tämä on kahtena päivämääräkenttänä haavoittuvuustiketissä, ja he käyvät listan läpi kerran neljännesvuodessa oman mittarijärjestelmän pystyttämisen sijaan.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

12 Käytäntö 8: Turvallisuusohjeet tuotteen käyttöönottoon ja käyttöön (SG) 7

SG-1 **Jokaisen tuotteen mukana on kuvaus sen syvyyssuuntaisen puolustuksen strategiasta: siinä nimetään tuotteeseen itseensä rakennetut suojauskerrokset, liitetään ne niihin uhkiin, joita vastaan ne toimivat, ja osoitetaan, mikä suojausvaikutus syntyy vasta useamman kerroksen yhteispelistä.** Asiakirja

Mistä sen tunnistaa: Luku toimitettavassa tuotedokumentaatiossa tai erillinen turvallisuuskonsepti, jossa kustakin suojauskerroksesta ilmenevät mekanismi, katettu uhka ja sen vaikutuksen rajat. Pienelle yritykselle riittää kahden sivun taulukko: sarake suojauskerros, sarake uhka omasta uhkamallista, sarake jäännösriski. Ristiviittaus kohdan SR-2 uhkamalliin riittää, sisältöä ei ylläpidetä kahteen kertaan.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SG-2 **Dokumentaatiossa nimetään ne turvatoimet, joita tuote ei itse tarjoa vaan odottaa käyttöympäristöltä, esimerkiksi verkon segmentointi, edessä olevat palomuurit, fyysinen pääsynhallinta tai ulkoinen aikapalvelu, ja siinä tehdään selväksi, että luvattua turvallisuustasoa ei saavuteta ilman näitä toimia.** Asiakirja

Mistä sen tunnistaa: Käyttöönoton edellytyksiä käsittelevä luku käyttöohjeessa tai viitearkkitehtuurin piirros vyöhykkeineen ja yhdyskäytävineen, jossa käyttäjäorganisaation toimitettaviksi jäävät toimet on nimenomaisesti merkitty. Käytännössä hyväksi on osoittautunut luettelo ympäristöä koskevista oletuksista, joka johdetaan suoraan tuotteen turvallisuusyhteydestä ja luetaan uudelleen jokaisen tuoteversion kohdalla.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SG-3 **On olemassa turvallisen perusasetuksen ohje, jossa luetellaan kaikki turvallisuuden kannalta merkitykselliset asetukset, palvelut, portit ja rajapinnat, ilmoitetaan suositeltu toimitustila ja kuvataan, miten suosituksesta poikkeaminen vaikuttaa.** Asiakirja

Mistä sen tunnistaa: Kovennusohje asetustaulukkoineen: parametri, suositeltu arvo, vaikutus, sivuvaikutus poikettaessa. Lisäksi luettelo oletuskonfiguraatiossa aktiivisista palveluista ja porteista perusteluineen sille, miksi ne pysyvät päällä. Pieni tiimi säilyttää tätä taulukkoa arkistossa suoraan konfiguraatiotiedoston vieressä ja vie sen toimitusdokumentaatioon, jolloin se pysyy tuotteen mukaisena.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SG-4 **Jatkuvaa käyttöä varten on ohje, jossa kuvataan, miten tuotetta käytetään turvallisesti, miten sitä seurataan ja miten se säilyy turvallisessa tilassa, mukaan lukien varmuuskopio ja palautus, lokitus sekä turvallisuuden kannalta merkityksellisten tapahtumaviestien käsittely.** Asiakirja

Mistä sen tunnistaa: Käyttöohje, jossa on luvut lokituksesta, varmuuskopioista, uudelleenkäynnistyksestä ja tapahtumaviesteistä. Lisänäyttönä luettelo turvallisuuden kannalta merkityksellisistä viesteistä, joita tuote antaa, kunkin yhteydessä lyhyt suositeltu toimenpide, jolloin käyttäjäorganisaatio ei jää tulkitsemaan niitä yksin.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SG-5 **Dokumentaatiossa selitetään, miten tuotteen käyttäjätilit, roolit ja oikeudet perustetaan ja miten niitä ylläpidetään, erityisesti roolien erottaminen, oletustunnusten vaihtaminen ja tarpeettomiksi käyneiden tilien poistaminen.** Asiakirja

Mistä sen tunnistaa: Käyttäjätilien hallintaa käsittelevä luku, jossa on yhteenveto rooleista ja kullekin roolille annetuista oikeuksista, sekä nimenomainen huomautus oletustunnuksista ja niiden vaihtamisesta käyttöönotossa. Käytännössä toimii hyvin lyhyt käyttöönoton tarkistuslista käyttöohjeessa, jonka käyttäjäorganisaatio voi kuitata ja arkistoida.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SG-6 **On olemassa ohje turvalliseen käytöstä poistoon, jossa kuvataan arkaluonteisten tietojen, kuten tunnusten, avainten, konfiguraatiotietojen ja lokien, täydellinen poistaminen tuotteesta ennen kuin laite luovutetaan eteenpäin, otetaan uudelleen käyttöön tai hävitetään.** Asiakirja

Mistä sen tunnistaa: Käytöstä poistoa käsittelevä luku, jossa luetellaan tuotteen sisällä jokainen arkaluonteisten tietojen tallennuspaikka ja vastaava poistomenettely, mukaan lukien ne tapaukset, joissa poistaminen on teknisesti mahdotonta ja laitteisto hävitetään fyysisesti. Tässä auttaa arkkitehtuurikuvauksesta poimittu luettelo pysyvistä tallennuspaikoista, se estää tallennuspaikan unohtumisen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SG-7 **Käyttäjille toimitettava turvallisuusdokumentaatio katselmoidaan ennen julkaisua: se on teknisesti oikea, yhdenmukainen toimitettavan tuoteversion kanssa, kattava suunniteltuun sisältöön nähden ja ymmärrettävä kohdeyleisölle, ja se päivittyy aina, kun tuote muuttuu.**

Mistä sen tunnistaa: Katselmointitallenne kutakin asiakirjaa ja tuoteversiota kohden katselmoijineen, päiväyksineen, havaintoineen ja niiden sulkemisineen, kytkettynä julkaisuhyväksyntään. Pieni yritys ratkaisee tämän neljän silmän periaatteella dokumentaation muutospyynnössä: yksi kehittäjä tarkastaa teknisen sisällön, toinen henkilö ymmärrettävyyden, ja hyväksyntä kirjataan tikettiin. Versio on toimitettavissa vasta, kun katselmointi on dokumentoitu.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

IEC 62443-3-3:2013 Teollisuusautomaation järjestelmien tietoturvavaatimukset

Seitsemän perusvaatimusta, 51 järjestelmävaatimusta

100 vaatimusta. Tämän standardin mukainen sertifiointi on mahdollista akkreditoidussa sertifiointielimessä. Versio 07/2026.

IEC 62443-3-3 on sertifioitavissa, ja sertifioinnin kohteena on järjestelmä, ei organisaatio eikä henkilö. Reitit ovat ISASecure SSA ja IECEE CB Scheme. Organisaation sertifiointiin tarvitaan 62443-2-1 tai 2-4, komponentin sertifiointiin 62443-4-2. Tämä lista sisältää 51 järjestelmävaatimusta ja 49 vaatimuksen laajennusta. Se, mitkä niistä koskevat kohdetta, riippuu tavoitellusta turvallisuustasosta: SL 1 alkaen niitä on 38, SL 2 alkaen 60, SL 3 alkaen 90 ja tasolla SL 4 kaikki 100. Yksikään laajennus ei koske jo tasoa SL 1. Tämä lista on työkalu itsearviointiin, ei osoitus vaatimustenmukaisuudesta.

Yritys	Päivämäärä	Täyttäjä

5 FR 1: Kuka tai mikä pyytää pääsyä, ja onko se todella se, joka se väittää olevansa 24

SR 1.1 Henkilökäyttäjät tunnistetaan ja heidän henkilöllisyytensä todennetaan ennen pääsyn saamista jokaisessa kohdassa, jossa automaatiojärjestelmää voi käyttää tai konfiguroida. Tähän kuuluvat koneen käyttöpaneelit, suunnittelupääsy ja verkkopalvelut.

Mistä sen tunnistaa: Luettelo järjestelmän kaikista kirjautumiskohdista, eli HMI, valvomo, PLC-ohjelmointipääsy, kytkin, VPN ja etähuollon työasema, kunkin kohdalla siinä käytetty todentamistapa. Lisäksi konfiguraatioote tai näyttökuva kirjautumisnäkymästä jokaisesta laiteluokasta. Pieni yritys aloittaa yhdellä taulukolla laitetta kohden, sarakkeina laite, liityntä, todentaminen kyllä tai ei, sekä perustelu jos ei. Vaaditaan tasosta SL 1 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 1.1 RE 1 Jokainen henkilökäyttäjä toimii henkilökohtaisella tunnisteella, joka on annettu vain hänelle. Yhteiskäyttöiset ja vuorokohtaiset tilit ovat poissa käytöstä, ja jäljelle jäävät poikkeukset perustellaan tapauskohtaisesti ja tuetaan lisätoimenpitein.

Mistä sen tunnistaa: Tilivienti järjestelmittäin, jossa tunniste yhdistyy henkilöön, poikkeuslista perusteluineen ja korvaavine toimenpiteineen, esimerkiksi kamera tai läsnäololista käyttöpaikalla. Tämä rivi on vaatimuksen laajennus eikä siksi ole koskaan pakollinen tasolla SL 1, se vaaditaan tasosta SL 2 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 1.1 RE 2 Ei-luotetusta verkosta kirjautuva, esimerkiksi internetistä tai etähuoltoyhteyden kautta, osoittaa henkilöllisyytensä vähintään kahdella toisistaan riippumattomalla tekijällä.

Mistä sen tunnistaa: Etäyhteyden konfiguraatio, jossa toinen tekijä on käytössä, esimerkkitallenne kirjautumisesta molempine tekijöineen sekä luettelo jaetuista tunnistevälineistä tai sovellusrekisteröinneistä. Pieni yritys käyttää olemassa olevan VPN-välityslaitteen toista tekijää tai todentamissovellusta, mikä ei maksa muuta kuin käyttöönottoon kuluvan ajan. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen, ei tasolla SL 1.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 1.1 RE 3 Kahden riippumattoman tekijän käyttö koskee ulkopuolelta tulevan pääsyn lisäksi jokaista henkilökäyttäjän kirjautumista, myös kirjautumisia luotetuksi luokitellun verkon sisällä.

Mistä sen tunnistaa: Keskitetyn todentamispalvelun politiikkaote, joka osoittaa toisen tekijän pakottamisen ilman verkkokohtaisia poikkeuksia, sekä esimerkkitallenteet kirjautumisista valvomosta ja käyttöpaneelilta. Vaatimuksen laajennus, vaaditaan vasta tasosta SL 4 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 1.2 **Ihmisten lisäksi myös ohjelmistoprosessit ja laitteet todentavat itsensä järjestelmälle ennen kuin ne saavat vaihtaa tietoa tai käyttää palveluja. Tähän kuuluvat ohjainten väliset kytkennät, tiedonsiirtoyhteydet ylemmän tason järjestelmiin ja diagnostiikkatyökalut.**

Mistä sen tunnistaa: Luettelo laitteiden välisistä yhteyksistä, joissa mainitaan lähde, kohde, protokolla ja kussakin käytetty tunnistautumistieto, esimerkiksi varmenne, palvelutili tai ennalta jaettu avain. Lisäksi konfiguraatioote yhdestä kytkennästä, josta todentaminen näkyy. Vaaditaan tasosta SL 2 alkaen, ei vaadita tasolla SL 1.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 1.2 RE 1 **Jokainen ohjelmistoprosessi ja jokainen laite esittää oman yksilöllisen tunnisteensa. Yhteiskäyttöiset palvelutilit tai yksi järjestelmänlaajuinen avain monelle laitteelle eivät ole sallittuja.** Asiakirja

Mistä sen tunnistaa: Laitteiden ja tunnisteiden tai varmenteiden sarjanumeroiden vastaavuustaulukko, josta näkyy, ettei yksikään tunniste esiinny kahdesti. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen eikä siksi kuulu tasoon SL 1.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 1.3 **Tilejä hallitaan koko elinkaaren ajan: luonti, oikeuksien muutos, sulkeminen lähdön yhteydessä ja poisto ovat sääntöjen ohjaamia ja järjestelmien tukemia. Tämä koskee käyttäjätilejä, palvelutilejä ja hätätilejä.** Asiakirja

Mistä sen tunnistaa: Tilirekisteri, jossa on tyyppi, omistaja, käyttötarkoitus ja tila, sekä näyttö tulijoista ja lähtijöistä, esimerkiksi allekirjoitettu luovutus tai tiketti, josta sulkeminen ja sen päiväys näkyvät. Toistuva tilien katselmointi on suositeltavaa, ja pienessä yrityksessä riittää tililistan vuosittainen täsmäytys henkilöstölistaan. Vaaditaan tasosta SL 1 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 1.3 RE 1 **Tilien hallinta on yhtenäinen kaikissa järjestelmän komponenteissa, jolloin yhdessä paikassa tehty tilin sulkeminen ei jää vaikutuksettomaksi yksittäisissä laitteissa.**

Mistä sen tunnistaa: Näyttö keskitetystä hakemistointegraatiosta, esimerkiksi hakemistopalvelu tai RADIUS, luettelo liitetyistä komponenteista sekä nimenomainen luettelo laitteista, joita ei voi liittää, ja niiden vaihtoehtoinen menettely. Testitallenne sulkemisesta, joka vaikuttaa kaikkiin liitettyihin järjestelmiin. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 1.4 **Tunnisteet annetaan kiinteiden sääntöjen mukaan, ne kohdistuvat yksiselitteisesti henkilöön, laitteeseen tai rooliin, ne poistetaan käytöstä kun niitä ei enää käytetä, eikä niitä anneta myöhemmin uudelleen toiselle haltijalle.**

Mistä sen tunnistaa: Tunnisteiden nimeämissääntö, esimerkiksi sukunimi ja etunimen alkukirjain tai laitostunnus ja numero, sekä käytöstä poistettujen tunnisteiden historia, joka osoittaa, ettei niitä käytetä uudelleen. Pienessä yrityksessä riittää yksi juokseva lista, jossa on antopäivä ja käytöstä poiston päivä. Vaaditaan tasosta SL 1 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 1.5 **Todentamisvälineet kuten salasanat, avaimet, varmenteet ja tunnistevälineet annetaan hallitusti, vaihdetaan kun paljastumista epäillään ja peruutetaan tarvittaessa. Toimitustilan oletustilit ja tehdassalasanat vaihdetaan ennen käyttöönottoa.**

Mistä sen tunnistaa: Luettelo annetuista tunnistevälineistä ja varmenteista vastaanottajineen ja päiväyksineen, näyttö vaihdoista ja peruutuksista sekä laitekohtainen käyttöönoton tarkistuslista, jossa kohta tehdassalasana vaihdettu on kuitattu. Vaaditaan tasosta SL 1 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 1.5 RE 1 **Ohjelmistoprosessien tunnistautumistietoja ei säilytetä luettavana tiedostona tallennusvälineellä, vaan laitepohjaisessa säilössä, joka estää salaisen osan lukemisen ulos.**

Mistä sen tunnistaa: Käytetyn turvakomponentin tyyppinäyttö, esimerkiksi TPM, secure element tai HSM, sekä konfiguraatioote, joka osoittaa avaimen säilyvän komponentin sisällä. Tyyppinäytöksi riittää hankintatallenne tai tietolehti. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen, ei vaadita tasoilla SL 1 ja SL 2.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 1.6 **Langaton pääsy järjestelmään, esimerkiksi WLAN, radio-ohjaimet tai Bluetooth-diagnostiikka, on käytettävissä vasta käyttäjän ja laitteen tunnistamisen ja todentamisen jälkeen, ja sitä hallitaan tietoisesti.**

Mistä sen tunnistaa: Luettelo kaikista langattomista yhteyksistä käyttötarkoituksineen, kantamineen ja salausmenetelmineen, tukiaseman konfiguraatioote sekä luettelo hyväksytyistä päätelaitteista. Pieni yritys kirjaa lisäksi, mitkä laitteiden langattomat liitynnät on tietoisesti kytketty pois. Vaaditaan tasosta SL 1 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 1.6 RE 1 **Jokainen langaton pääsy on kohdistettavissa yhteen tiettyyn käyttäjään tai yhteen tiettyyn laitteeseen, eikä kaikille osapuolille yhteinen verkkoavain riitä.**

Mistä sen tunnistaa: Näyttö menetelmästä, jossa on henkilökohtaiset tunnistautumistiedot, esimerkiksi yritystason WLAN-todentaminen hakemistoa vastaan tai laitekohtaiset varmenteet, sekä yhteysloki, josta yksilöllinen tunniste näkyy. Vaatimuksen laajennus, vaaditaan tasosta SL 2 alkaen eikä siksi tasolla SL 1.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 1.7 **Siellä missä salasanoja käytetään, niiden vähimmäisvahvuus on asetettavissa, esimerkiksi vähimmäispituus ja vaaditut merkkityypit, ja asetetut arvot vaikuttavat kaikkiin kyseisiin tileihin.**

Mistä sen tunnistaa: Järjestelmäkohtainen konfiguraatioote salasanapolitiikasta todella asetettuine arvoineen, esimerkiksi pituus >= 10 merkkiä ja vähintään kolme merkkityyppiä, sekä luettelo järjestelmistä, jotka eivät teknisesti tue tätä asetusta, ja niiden korvaava toimenpide. Vaaditaan tasosta SL 1 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 1.7 RE 1 **Henkilökäyttäjillä salasanojen muodostamista ja voimassaoloa ohjaavat lisäsäännöt: aiempien salasanojen uudelleenkäyttö estetään ja voimassaoloa rajataan ajallisesti.**

Mistä sen tunnistaa: Konfiguraatioote salasanahistoriasta, esimerkiksi viiden viimeisen salasanan uudelleenkäyttö estetty, sekä asetettu enimmäisvoimassaoloaika. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 1.7 RE 2 **Salasanan voimassaolon rajoitus koskee ihmisten lisäksi kaikkia tilejä, mukaan lukien palvelu-, huolto- ja laitetilit.**

Mistä sen tunnistaa: Teknisten tilien vaihtosuunnitelma, jossa on tilikohtaisesti viimeisin ja seuraava vaihtopäivä, sekä näyttö vaihdoista, esimerkiksi muutostallenne tai tiketti. Vaatimuksen laajennus, vaaditaan vasta tasosta SL 4 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 1.8 **Siellä missä varmenteita käytetään, ne tulevat hallitusta varmenteiden hallinnasta, jossa on määritellyt säännöt hakemiselle, myöntämiselle, voimassaoloajalle, uusimiselle ja peruuttamiselle.** Asiakirja

Mistä sen tunnistaa: Varmennepolitiikka tai lyhyt kirjallinen sääntö, jossa todetaan vastuu, voimassaoloajat ja peruuttamisen reitti, sekä luettelo myönnetyistä varmenteista päättymispäivineen. Pienelle yritykselle riittää taulukko, jossa on varmenne, laite, päättymispäivä ja muistutuspäivä, mikä estää vanhentuneista varmenteista johtuvat huomaamattomat laitoksen seisokit. Vaaditaan tasosta SL 2 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 1.9 **Kun todentamiseen käytetään avainpareja, järjestelmä tarkastaa varmenteen kokonaan: luottamusketju, voimassaoloaika, peruutustila ja osoitus siitä, että vastapuolella todella on yksityinen avain. Varmenteen ja tilin välinen yhteys on yksiselitteinen.**

Mistä sen tunnistaa: Konfiguraatioote, jossa peruutustarkistus on käytössä, esimerkiksi CRL tai OCSP, testitallenne hylätystä kirjautumisesta vanhentuneella tai peruutetulla varmenteella sekä varmenteiden ja tilien vastaavuustaulukko. Vaaditaan tasosta SL 3 alkaen, ei vaadita tasoilla SL 1 ja SL 2.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 1.9 RE 1 **Yksityiset avaimet sijaitsevat yksinomaan laitepohjaisessa säilössä, josta niitä ei voi lukea ulos, ja niitä myös käytetään tämän säilön sisällä.**

Mistä sen tunnistaa: Käytetyn turvakomponentin tietolehti tai sertifiointinäyttö sekä konfiguraatioote, josta näkyy avaimen syntyvän komponentin sisällä, jolloin yksityinen avain ei koskaan poistu siitä. Vaatimuksen laajennus, vaaditaan vasta tasosta SL 4 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 1.10 **Kirjautumisen aikana järjestelmä ei paljasta tietoa, jota voisi käyttää hyväksi. Syötetyt salasanat peitetään, eivätkä virheilmoitukset kerro, oliko väärin tunnus vai salasana.**

Mistä sen tunnistaa: Näyttökuva kirjautumisnäkymästä peitettyine syötteineen ja näyttökuva virheilmoituksesta epäonnistuneen yrityksen jälkeen. Laitteista, jotka eivät tähän teknisesti kykene, esimerkiksi vanhemmista käyttöpaneeleista, lisätään lyhyt merkintä korvaavasta toimenpiteestä, esimerkiksi rajoitettu fyysinen pääsy asennuspaikkaan. Vaaditaan tasosta SL 1 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 1.11 **Peräkkäisten epäonnistuneiden kirjautumisyritysten määrä on rajoitettu ja siihen annettava vaste on asetettavissa, esimerkiksi määräaikainen lukitus. Valittu vaste ei haittaa laitoksen turvallisuuteen liittyvää käyttöä.**

Mistä sen tunnistaa: Konfiguraatioote raja-arvosta, esimerkiksi lukitus <= 5 epäonnistuneen yrityksen jälkeen, ja lukituksen kesto, sekä lyhyt arvio siitä, miksi lukitus ei estä hätäkäyttöä tai laitoksen turvallista alasajoa. Turvallisuustoiminnon sisältävillä käyttöpaikoilla määräaikainen lukitus on parempi kuin tilin pysyvä lukitseminen. Vaaditaan tasosta SL 1 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 1.12 **Ennen kirjautumista on näytettävissä käyttöilmoitus, joka viittaa järjestelmän käytön ja seurannan sääntöihin. Teksti ja näyttötapa ovat suojattavan kohteen haltijan asetettavissa.**

Mistä sen tunnistaa: Näyttökuva näytetystä ilmoitustekstistä ja hyväksytty sanamuoto hyväksymispäivineen. Pienet yritykset sopivat sanamuodon lyhyesti henkilöstön edustajan tai johdon kanssa, yksi kappale riittää. Vaaditaan tasosta SL 1 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 1.13 **Pääsy ei-luotetuista verkoista, esimerkiksi toimittajien etähuolto, on rajattu määriteltyihin reitteihin, sitä seurataan ja se on katkaistavissa milloin tahansa.**

Mistä sen tunnistaa: Luettelo etäyhteysreiteistä käyttötarkoituksineen, vastapuolineen, yhteyshenkilöineen ja käytettyine reitteineen, sekä yhteyslokit ja näyttö katkaisumahdollisuudesta, esimerkiksi avainkytkin, palomuurisääntö tai etähuoltoreititin, jonka voi kytkeä pois. Vaaditaan tasosta SL 1 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 1.13 RE 1 **Vastuuhenkilö hyväksyy nimenomaisesti jokaisen yksittäisen istunnon ei-luotetusta verkosta ennen yhteyden muodostamista, eikä pysyvästi auki oleva yhteys riitä.**

Mistä sen tunnistaa: Hyväksyntätallenteet etähuoltoistunnoittain, joissa on aika, syy, hyväksyvä henkilö ja kesto, teknisesti esimerkiksi pääsyreitittimen avainkytkimellä tai hyväksyntäportaalilla. Pienessä yrityksessä riittää ohjauskaapilla oleva etähuoltopäiväkirja, jonka huoltoteknikko kuittaa jokaisesta istunnosta. Vaatimuksen laajennus, vaaditaan tasosta SL 2 alkaen eikä siksi koskaan tasolla SL 1.

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

6 FR 2: Käytön hallinta (oikeudet, istunnot, lokitallenteet) 24

SR 2.1 **Järjestelmä pakottaa myönnetyt oikeudet teknisesti: jokainen kirjautunut henkilö, jokainen laite ja jokainen ohjelmistoprosessi saa täsmälleen sille määritellyn pääsyn, ja tämän ylittävä yritys hylätään.**

Mistä sen tunnistaa: Oikeusmalli, joka yhdistää tilit käyttöoikeuksiin, sekä näyttökuva tai konfiguraatioote ohjausjärjestelmästä, HMI:stä ja suunnitteluasemasta aktiivisine oikeuksineen. Lisäksi testitallenne, jossa vähäisin oikeuksin varustettu tili yrittää estettyä toimintoa ja hylätään. Vaaditaan tasosta SL 1 alkaen. Pieni yritys pärjää kahdella tai kolmella roolilla, esimerkiksi käyttö, kunnossapito ja suunnittelu, ja kuvaa ne yhdelle sivulle.

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

SR 2.1 RE 1 **Oikeuksien pakottaminen koskee henkilökäyttäjien lisäksi yhtä lailla ohjelmistoprosesseja ja laitteita, jotka käyttävät järjestelmää omatoimisesti.**

Mistä sen tunnistaa: Luettelo teknisistä tileistä ja palvelutileistä, esimerkiksi OPC UA -asiakkaat, historiatietokannan yhteydet ja varmuuskopiointipalvelut, kunkin kohdalla sille annetut oikeudet. Ote oikeuksien hallinnasta, josta näkyy, etteivät nämä tilit toimi pääkäyttäjän oikeuksin. Vaatimuksen laajennus, vaaditaan tasosta SL 2 alkaen, ei tasolla SL 1.

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

SR 2.1 RE 2 **Oikeuksia ei anneta yksittäisille henkilöille erikseen vaan roolien kautta, ja roolin ja sallittujen toimintojen välinen vastaavuus on kirjattu jäljitettävästi.** Asiakirja

Mistä sen tunnistaa: Rooli- ja oikeusmatriisi taulukkona: riveinä roolit, sarakkeina toiminnot kuten asetusarvon muutos, ohjelman lataus, hälytyksen kuittaus ja tilin luonti. Lisäksi luettelo, joka yhdistää henkilön rooliin. Vaatimuksen laajennus, vaaditaan tasosta SL 2 alkaen. Ylläpidetty taulukkolaskentatiedosto, jossa on muutospäivä, riittää näytöksi täysin.

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

SR 2.1 RE 3 **Tiukasti rajatuissa poikkeustapauksissa valtuutettu esimies voi poistaa oikeusrajoituksen määräajaksi, ja jokainen tällainen ohitus kirjataan lokitallenteisiin.**

Mistä sen tunnistaa: Menettelykuvaus poikkeusluvasta, jossa todetaan, kuka sen voi myöntää ja kuinka kauan se on voimassa, sekä lokitallenteet jo myönnetyistä ohituksista järjestelmälokista. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

SR 2.1 RE 4 **Erityisen kriittiset toimenpiteet edellyttävät kahden toisistaan riippumattoman valtuutetun henkilön hyväksynnän ennen toiminnon suorittamista.**

Mistä sen tunnistaa: Luettelo kaksoishyväksyntää vaativista toiminnoista, esimerkiksi turvaparametrien muutos tai uuden ohjausohjelman lataus, sekä konfiguraatiosta saatava näyttö ja lokitallenteet, joissa molemmat hyväksyjät on nimetty. Vaatimuksen laajennus, vaaditaan vasta tasosta SL 4 alkaen.

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

SR 2.2 **Langattomien yhteyksien käyttö automaatioverkossa on sidottu nimenomaiseen valtuutukseen, ja vain hyväksytyt osapuolet saavat vaihtaa tietoa tai puuttua toimintaan langattomasti.**

Mistä sen tunnistaa: Luettelo kaikista langattomista yhteyksistä, esimerkiksi WLAN-tukiasemat, Bluetooth-parit ja mobiilireitittimet, kunkin kohdalla käyttötarkoitus ja hyväksytyt osapuolet. Lisäksi tukiaseman pääsynhallinnan konfiguraatio. Vaaditaan tasosta SL 1 alkaen. Jos prosessiverkossa ei ole yhtään langatonta yhteyttä, se todetaan kirjallisesti juuri niin ja tueksi liitetään konfiguraationäkymä, jossa langaton toiminto on pois käytöstä.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.2 RE 1 **Automaatioverkon läheisyydessä olevat luvattomat langattomat laitteet havaitaan ja niistä ilmoitetaan.**

Mistä sen tunnistaa: Tallenne langattomasta seurannasta tai toistuvasta langattomasta kartoituksesta päiväyksineen, tuloslistoineen ja merkintöineen jokaisesta tuntemattomasta laitteesta. Ilmoitusreitti vastuulliselle taholle on nimetty. Vaatimuksen laajennus, vaaditaan tasosta SL 2 alkaen, ei tasolla SL 1. Pieni yritys voi tehdä kartoituksen neljännesvuosittain kannettavalla tietokoneella ja arkistoida tuloksen tallenteena.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.3 **Kannettavien ja liikuteltavien laitteiden käyttö järjestelmässä, esimerkiksi huoltokannettavat, USB-muistit tai tabletit, on sääntöjen ohjaamaa ja teknisesti rajattu nimenomaisesti hyväksyttyihin laitteisiin.**

Mistä sen tunnistaa: Laitteiden käyttöä koskeva säännöstö, luettelo hyväksytyistä huoltolaitteista tunnisteineen sekä näyttö teknisestä rajoituksesta, esimerkiksi HMI:n ja suunnitteluaseman USB-portit poissa käytöstä tai rajattu tiettyihin laitteisiin. Vaaditaan tasosta SL 1 alkaen. Pieni yritys käyttää kahta merkittyä huoltotikkua, joille kirjoitetaan vain yhdellä siirtoasemalla.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.3 RE 1 **Ennen liittämistä kannettavan tai liikuteltavan laitteen tietoturvatila tarkastetaan, ja vaatimukset täyttämättömät laitteet estetään pääsemästä järjestelmään.**

Mistä sen tunnistaa: Laitteen tilan tarkastuskriteerit, esimerkiksi ajantasainen haittaohjelmasuojaus ja korjauspäivitysten taso, sekä huoltolaitekohtaiset tarkastustallenteet ja näyttö teknisestä pakottamisesta, esimerkiksi siirtoaseman tai verkon pääsynhallinnan kautta. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.4 **Järjestelmässä suoritettavasta ladattavasta koodista, esimerkiksi käyttöliittymien skripteistä tai raporttien aktiivisesta sisällöstä, on määritelty, mitkä tyypit ovat sallittuja, ja muiden kuin sallittujen tyyppien suoritus estetään.** Asiakirja

Mistä sen tunnistaa: Määrittely siitä, mikä ladattava koodi on sallittua millä järjestelmillä, sekä konfiguraatioote rajoituksesta, esimerkiksi skriptien suoritus HMI-selaimessa poissa käytöstä ja makrot analyysitiedostoissa estetty. Vaaditaan tasosta SL 1 alkaen. Riittää yhden sivun määrittely, joka kattaa ne kolme tai neljä tapausta, jotka todella ovat olemassa.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.4 RE 1 **Ennen ladattavan koodin suoritusta todennetaan, että se on peräisin odotetusta lähteestä eikä sitä ole muutettu.**

Mistä sen tunnistaa: Konfiguraatioote allekirjoituksen tarkistuksesta tai tarkistussummien valvonnasta sekä testitallenne, jossa muunneltu tai allekirjoittamaton koodi hylätään. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.5 **Istunto lukitaan, kun käyttäjä ei ole toiminut määriteltyyn aikaan, ja avataan uudelleen vasta uuden todentamisen jälkeen, ilman että turvallisuuden kannalta olennaisten prosessitietojen näyttö katoaa.**

Mistä sen tunnistaa: Konfiguraatioote työasemakohtaisesta lukitusajasta sekä perustelu niille työasemille jatkuvasti miehitetyissä valvomoissa, joissa lukitus on tietoisesti asetettu toisin. Vaaditaan tasosta SL 1 alkaen. Visuaalinen näyttö: näyttökuva lukitusnäkymästä, jossa hälytysrivi näkyy edelleen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.6 **Etäistunnot päätetään määritellyn toimettoman ajan jälkeen tai käyttäjän vaatimuksesta, jotta yksikään avoin etäyhteys ei jää valvomatta.**

Mistä sen tunnistaa: Etäyhteyden konfiguraatio toimettomuuden aikarajoineen, lokitallenteet päätetyistä etäistunnoista sekä kuvaus siitä, miten käyttäjä voi katkaista käynnissä olevan etähuoltoistunnon välittömästi, esimerkiksi avainkytkimellä tai istuntokohtaisella vapautuksella. Vaaditaan tasosta SL 2 alkaen, ei tasolla SL 1.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.7 **Samanaikaisten istuntojen määrä tiliä tai roolia kohden on rajoitettu, ja tämän rajan ylittävät kirjautumisyritykset hylätään.**

Mistä sen tunnistaa: Konfiguraatioote roolikohtaisesta ylärajasta, esimerkiksi <= 1 samanaikainen istunto suunnittelutileillä, sekä testitallenne hylätystä toisesta kirjautumisyrityksestä. Vaaditaan tasosta SL 3 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.8 **Tietoturvan kannalta olennaiset tapahtumat kirjataan, ja jokainen merkintä nimeää vähintään ajankohdan, lähteen, käynnistäneen tilin, tapahtuman lajin ja lopputuloksen.** Asiakirja

Mistä sen tunnistaa: Määrittely kirjattavista tapahtumalajeista, esimerkiksi kirjautuminen, epäonnistunut kirjautuminen, oikeuksien muutos, ohjelman muutos ja konfiguraation muutos, sekä aito ote lokitiedostosta, josta mainitut kentät näkyvät. Vaaditaan tasosta SL 1 alkaen. Pieni yritys kerää ohjausjärjestelmän, HMI:n ja palomuurin lokit yhteen kansioon, jolla on kiinteä säilytysaika.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.8 RE 1 **Yksittäisten komponenttien lokitallenteet kootaan yhteen keskitettyyn paikkaan, jossa ne muodostavat yhden järjestelmänlaajuisen tallenteen, joka on arvioitavissa kokonaisuutena.**

Mistä sen tunnistaa: Arkkitehtuurikaavio lokien keruusta kaikkine liitettyine lähteineen sekä analyysi, joka asettaa vähintään kahden komponentin tapahtumat samalle aikajanalle. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.9 **Lokitallenteille on varattu riittävä tallennustila, jotta tapahtumat säilyvät määritellyn säilytysajan eivätkä korvaudu tahattomasti.**

Mistä sen tunnistaa: Laskelma tai arvio tallennustilan tarpeesta päivittäisen lokimäärän ja säilytysajan tulona, sekä asetettu tallennustilan koko ja arkistointisääntö. Vaaditaan tasosta SL 1 alkaen. Käytännössä riittää päivittäinen kopiointi erilliseen sijaintiin, jolla on dokumentoitu säilytysaika.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.9 RE 1 **Kun lokitallennustilan käytölle määritelty raja saavutetaan, vastuulliselle taholle annetaan varoitus ennen kuin tila on kokonaan käytetty.**

Mistä sen tunnistaa: Konfiguraatioote raja-arvosta, esimerkiksi varoitus >= 80 prosentin käytöstä alkaen, sekä esimerkki laukaistusta ilmoituksesta ja vastaanottajalista. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.10 **Jos lokitus epäonnistuu tai lokitallennustila täyttyy, järjestelmä toimii ennalta määritellyllä tavalla ja vastuullinen taho saa tiedon, ilman että laitoksen turvallinen käyttö vaarantuu.**

Mistä sen tunnistaa: Määritelty toiminta kussakin häiriötapauksessa, esimerkiksi vanhempien merkintöjen korvaaminen ja ilmoituksen antaminen laitoksen pysäyttämisen sijaan, perusteluineen prosessin näkökulmasta. Näyttönä on laukaistu testi-ilmoitus ja sitä vastaava lokimerkintä. Vaaditaan tasosta SL 1 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.11 **Jokaisessa lokitallenteessa on aikaleima nimetystä aikalähteestä, jotta eri komponenttien tapahtumat ovat asetettavissa keskinäiseen järjestykseen.**

Mistä sen tunnistaa: Ilmoitus komponenttikohtaisesti käytetystä aikalähteestä ja lokiote, jossa aikaleima aikavyöhykkeineen näkyy. Vaaditaan tasosta SL 2 alkaen, ei tasolla SL 1.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.11 RE 1 **Kaikkien mukana olevien komponenttien kellot tahdistetaan yhteiseen aikalähteeseen niin, että poikkeama pysyy määritellyissä rajoissa.**

Mistä sen tunnistaa: Ajan tahdistuksen konfiguraatio, esimerkiksi NTP-palvelin ja tahdistusväli, sekä tarkastustallenne komponenttikohtaisesti mitatusta poikkeamasta suhteessa määriteltyyn rajaan, esimerkiksi <= 1 sekunti. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.11 RE 2 **Aikalähde itse on suojattu muuntelulta, ja epäuskottava tai muutettu aikaviite havaitaan ja siitä ilmoitetaan.**

Mistä sen tunnistaa: Kuvaus aikalähteen suojauksesta, esimerkiksi todennettu ajan tahdistus, rajaus sisäiseen lähteeseen ja aikahyppyjen seuranta, sekä ilmoitukset tai lokitallenteet havaitusta poikkeamasta. Vaatimuksen laajennus, vaaditaan vasta tasosta SL 4 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.12 **Määritellyistä kriittisistä toiminnoista on jälkikäteen todettavissa kiistattomasti, kuka ne käynnisti, jolloin toiminut henkilö ei voi uskottavasti kiistää tekoaan.** Asiakirja

Mistä sen tunnistaa: Luettelo toiminnoista, joita tämä näyttö koskee, esimerkiksi reseptin muutos, erän vapautus ja raja-arvojen muutos, sekä vastaavat tallenteet yksilöllisine henkilötunnisteineen ja näyttö siitä, että ryhmätilit on suljettu pois näistä toiminnoista. Vaaditaan tasosta SL 3 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 2.12 RE 1 **Kiistämätön kohdistaminen toimineeseen henkilöön koskee valittujen kriittisten toimintojen lisäksi kaikkia käyttäjiä ja kaikkia heidän käynnistämiään toimintoja.**

Mistä sen tunnistaa: Näyttö siitä, että jokainen tili on sidottu yhteen henkilöön eikä yhteiskäyttöisiä kirjautumisia ole jäljellä, sekä lokiote satunnaisista toiminnoista, joissa yksilöllinen henkilötunniste esiintyy läpi koko otteen. Vaatimuksen laajennus, vaaditaan vasta tasosta SL 4 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

7 FR 3: Järjestelmän eheys, tietojen, ohjelmistojen ja istuntojen suojaaminen luvattomalta muuttamiselta 19

SR 3.1 **Ohjausjärjestelmä havaitsee, kun tietoa on muutettu siirron aikana tietoliikennekanavassa, ja tämä koskee yhtä lailla ohjaustietoja, konfiguraatiotietoja ja hallintaliikennettä. Suojaus kattaa myös yhteydet, jotka poistuvat järjestelmästä tai kulkevat ei-luotettujen verkkosegmenttien läpi.**

Mistä sen tunnistaa: Verkko- ja protokollakatsaus, jossa todetaan, mikä kanava käyttää mitäkin eheysmekanismia (tarkistussumma, viestin todennuskoodi, allekirjoitetut sanomat), konfiguraatioote kenttäväylän tai OPC UA:n turva-asetuksista sekä testitallenne, joka osoittaa, että muunneltu sanoma hylättiin todistetusti. Pieni yritys kokoaa tämän yhteyskohtaiseen taulukkoon, jonka sarakkeina ovat lähde, kohde, protokolla ja eheysmekanismi, ja osoittaa vaikuttavuuden kerran liikennekaappauksella. Vaaditaan tasosta SL 1 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 3.1 RE 1 **Siirron aikainen eheyden suojaus perustuu salausmekanismeihin, jolloin hyökkääjän omin keinoin tekemä tahallinen muuntelu ei jää havaitsematta. Pelkkä siirtovirheitä vastaan tarkoitettu tarkistussumma ei tässä riitä.**

Mistä sen tunnistaa: Luettelo kanavakohtaisesti käytössä olevista salausmekanismeista ja avainpituuksista, viittaus taustalla olevaan avainten hallintaan sekä konfiguraatiootteet (esimerkiksi TLS-salausvalikoimat, OPC UA SecurityPolicy, IPsec-profiilit). Pienet yritykset luottavat ohjaintensa turvallisiin oletusprofiileihin ja arkistoivat näyttökuvan voimassa olevasta asetuksesta. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 3.2 **Haittakoodia vastaan on olemassa suojausmekanismit, jotka estävät ei-toivotun ohjelmakoodin suorituksen järjestelmän komponenteissa ja ilmoittavat jokaisesta havainnosta. Mekanismit on valittu niin, etteivät ne häiritse laitoksen tarkoitettua toimintaa, ja ne pidetään ajan tasalla.**

Mistä sen tunnistaa: Komponenttikohtainen katsaus siitä, mikä mekanismi on käytössä (virustorjunta, sovellusten sallimislista, kovennettu käyttöjärjestelmä ilman suoritusoikeuksia), näyttö tunnisteiden tai sallimislistojen päivittämisestä sekä suojausjärjestelmän hälytykset. Siellä missä virustorjunta ei ole mahdollinen, esimerkiksi ohjaimessa, korvaava toimenpide kirjataan perusteluineen. Pienet yritykset pärjäävät hyvin käyttöpäätteen sallimislistalla ja kirjallisella säännöllä USB-medioista. Vaaditaan tasosta SL 1 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 3.2 RE 1 **Haittakoodilta suojaaminen vaikuttaa lisäksi laitoksen sisään- ja ulostulopisteissä, joissa tieto saapuu tai poistuu, eikä vain päätelaitteissa itsessään.**

Mistä sen tunnistaa: Luettelo kaikista sisään- ja ulostulopisteistä (etähuoltoyhteys, tiedonsiirron välityslaite, siirrettävät tallennusvälineet, luovutus toimistoverkkoon, sähköpostireitti ohjelmaversioille) ja kussakin vaikuttava tarkistusmekanismi, sekä tallenteet tarkastetuista luovutuksista. Pienet yritykset perustavat yhden luovutustietokoneen virustarkistuksineen välityspisteeksi ja kirjaavat tämän työohjeeseen. Vaatimuksen laajennus, vaaditaan tasosta SL 2 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 3.2 RE 2 **Haittakoodin suojausmekanismeja hallitaan keskitetysti, päivitykset jaetaan keskitetysti ja havainnot kerätään yhteen paikkaan arviointia varten.**

Mistä sen tunnistaa: Keskitetyn hallintakonsolin konfiguraatio, raportti kaikkien liitettyjen komponenttien päivitystilasta sekä analyysi ilmoitetuista havainnoista tietyltä ajanjaksolta. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 3.3 **Järjestelmän turvatoiminnot todennetaan suunnitelluin välein ja muutosten jälkeen sen varmistamiseksi, että ne todella toimivat. Testit ajoitetaan niin, etteivät ne vaaranna laitoksen käyttöä, ja tulokset kirjataan.** Asiakirja

Mistä sen tunnistaa: Testaussuunnitelma, jossa todetaan testauskohde, testausväli ja aikaikkuna, sekä testitallenteet, joista näkyvät päiväys, testaaja, odotettu käyttäytyminen ja havaittu käyttäytyminen. Hyödyllisiä yksittäisiä testejä ovat: kirjautuminen suljetulla tilillä epäonnistuu, virustorjunta reagoi testitiedostoon, etähuoltoyhteys ei ole tavoitettavissa ilman vapautusta. Pienet yritykset liittävät testauksen jo muutenkin suunniteltuun kunnossapitoseisokkiin ja käyvät läpi kiinteän tarkistuslistan. Vaaditaan tasosta SL 1 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 3.3 RE 1 **Turvatoimintojen todentaminen tapahtuu automatisoiduin keinoin, jolloin se on toistettavissa ilman käsityötä ja tuottaa yhdenmukaisen tuloksen.**

Mistä sen tunnistaa: Skriptit tai testityökalut aikatauluineen, niiden tulostiedostot sekä useamman ajon vertailu, joka osoittaa, että poikkeamat havaitaan. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 3.3 RE 2 **Turvatoimintojen todentaminen on mahdollista myös normaalin käytön aikana, ilman laitoksen pysäyttämistä tai erityistilaan asettamista.**

Mistä sen tunnistaa: Kuvaus testausmenettelystä ja näyttö siitä, ettei sillä ole haitallista vaikutusta prosessiin, esimerkiksi analyysi vaikutuksesta kiertoaikoihin ja verkkokuormaan, sekä testitallenteet tuotantokäytöstä. Vaatimuksen laajennus, vaaditaan tasosta SL 4 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 3.4 **Ohjelmistoihin, laiteohjelmistoihin ja levossa olevaan tietoon tehdyt luvattomat muutokset havaitaan. Tämä koskee yhtä lailla ohjausohjelmia, parametrijoukkoja, reseptejä ja konfiguraatiotiedostoja.**

Mistä sen tunnistaa: Luettelo suojattavista versioista tallennettuine tarkistusarvoineen tai allekirjoituksineen, eheysvertailujen tulokset sekä dokumentoitu täsmäytys versionhallinnassa olevaan versioon. Pienet yritykset tallentavat julkaistun ohjelmaversion tarkistussummineen kirjoitussuojattuun sijaintiin ja vertaavat epäilyn herätessä tai kunnossapidon jälkeen. Vaaditaan tasosta SL 1 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 3.4 RE 1 **Jos ohjelmiston tai tiedon eheyden loukkaus havaitaan, järjestelmä ilmoittaa siitä automaattisesti vastuulliselle taholle, ilman että kenenkään tarvitsee etsiä sitä aktiivisesti.**

Mistä sen tunnistaa: Ilmoitusreittien konfiguraatio (hälytys valvomossa, sähköposti, viesti valvontajärjestelmään), vastaanottajalista sijaisjärjestelyineen sekä vähintään yksi testihälytys dokumentoituine vasteaikoineen. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 3.5 **Syötteet, jotka järjestelmä ottaa vastaan prosessitiedoista, liitynnöistä tai käyttöliittymistä, tarkastetaan sallitun syntaksin, sallitun arvoalueen ja sallitun pituuden osalta ennen käsittelyä. Virheelliset syötteet eivät johda hallitsemattomaan käyttäytymiseen.**

Mistä sen tunnistaa: Määrittely syötekohtaisista rajoista ja muodoista, otteet ohjaimen tai sovelluksen tarkastuslogiikasta sekä testitapaukset tahallisesti virheellisillä syötteillä (liian suuri arvo, väärä tietotyyppi, ylipitkä merkkijono) ja järjestelmän dokumentoitu käyttäytyminen niissä. Pienet yritykset kirjaavat mittauspistekohtaiset uskottavuusrajat taulukkoon ja todentavat ne käyttöönoton yhteydessä. Vaaditaan tasosta SL 1 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 3.6 **Häiriötilanteen varalta on määritelty, minkä tilan laitokselle menevät lähdöt ottavat, ja järjestelmä ottaa täsmälleen tuon tilan. Määritelty tila on sovitettu yhteen laitoksen toiminnallisen turvallisuuden kanssa.**

Mistä sen tunnistaa: Määrittely lähdöittäin tai lähtöryhmittäin (arvon pito, määritelty korvaava arvo, turvallinen alasajotila) perusteluineen riskin arvioinnista, ohjaimen konfiguraatioote sekä näyttö vikatestistä, esimerkiksi kaapelikatkosta tai tietoliikenteen menetyksestä, joka osoittaa odotetun käyttäytymisen. Vaaditaan tasosta SL 1 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 3.7 **Järjestelmä käsittelee virhetilanteet niin, että käyttö pysyy hallinnassa eikä hyökkääjää auttavaa tietoa paljastu. Käyttäjille näytettävät virheilmoitukset pysyvät lyhyinä, ja tekniset yksityiskohdat menevät vain sisäisiin tallenteisiin.**

Mistä sen tunnistaa: Katsaus virheluokkiin ja kullekin ennakoituun järjestelmän käyttäytymiseen, esimerkkejä näytetyistä ilmoituksista verrattuina vastaaviin sisäisiin lokimerkintöihin sekä testinäyttö siitä, ettei käyttöliittymässä näy tiedostopolkuja, tilien nimiä, tietokannan tulosteita eikä versiotietoja. Vaaditaan tasosta SL 1 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 3.8 **Aktiiviset istunnot on suojattu kaappaukselta ja vieraiden viestien syöttämiseltä. Istunto päättyy uloskirjautumiseen tai määritellyn toimettoman ajan jälkeen, eikä sitä sen jälkeen voi käyttää uudelleen.**

Mistä sen tunnistaa: Istunnonhallinnan konfiguraatio asetettuine raja-arvoineen toimettomuusajalle ja enimmäiskestolle, näyttö mekanismista, joka suojaa viestien uudelleentoistolta, sekä testitallenne, jossa kaapattu istunto ei enää toimi uloskirjautumisen jälkeen. Vaaditaan tasosta SL 2 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 3.8 RE 1 **Istuntotunnisteet menettävät voimassaolonsa istunnon päättyessä, eikä järjestelmä hyväksy niitä enää, ei myöskään silloin kun ne esitetään uudelleen ulkopuolelta.**

Mistä sen tunnistaa: Konfiguraatioote istunnonhallinnasta mitätöinnin osalta sekä testitallenne, jossa aiemmin voimassa ollut tunniste lähetetään uudelleen uloskirjautumisen jälkeen ja järjestelmä hylkää sen. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 3.8 RE 2 **Jokaiselle uudelle istunnolle luodaan oma kertakäyttöinen tunniste. Tunnisteita ei käytetä uudelleen istuntojen, käyttäjien tai laitteiden välillä.**

Mistä sen tunnistaa: Kuvaus luontimenettelystä ja näyttö lokista tai liikennekaappauksesta siitä, että useat peräkkäiset kirjautumiset saavat eri tunnisteet. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 3.8 RE 3 **Istuntotunnisteet luodaan tunnustetuilla satunnaismekanismeilla, jolloin niitä ei voi arvata eikä johtaa edeltävistä tunnisteista.**

Mistä sen tunnistaa: Ilmoitus käytetystä satunnaislukugeneraattorista ja sen entropialähteestä, toimittajan vakuutus tai testiraportti siitä sekä tilastollinen analyysi luotujen tunnisteiden otoksesta. Vaatimuksen laajennus, vaaditaan tasosta SL 4 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 3.9 **Tietoturvan kannalta olennaiset tallenteet ja niiden arviointiin käytettävät työkalut on suojattu luvattomalta pääsyltä, muuttamiselta ja poistamiselta. Niiden henkilöiden joukko, jotka saavat muuttaa tai poistaa tallenteita, on suppea ja nimetty.** Asiakirja

Mistä sen tunnistaa: Lokitietojen käyttöoikeusmalli nimettyine kohdistuksineen, edelleenlähetyksen konfiguraatio erilliseen lokijärjestelmään, säilytysajat sekä testinäyttö siitä, ettei tavallinen käyttäjä voi poistaa merkintöjä. Pienet yritykset lähettävät lokit erilliselle laitteelle, johon laitoksen käyttäjillä ei ole kirjoitusoikeutta. Vaaditaan tasosta SL 2 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 3.9 RE 1 **Tietoturvan kannalta olennaiset tallenteet säilytetään lisäksi välineellä, joka sulkee pois jälkikäteisen ylikirjoituksen, jolloin kertaalleen kirjoitettua merkintää ei voi enää muuttaa, ei edes pääkäyttäjän oikeuksin.** Asiakirja

Mistä sen tunnistaa: Kuvaus käytetystä säilytystavasta (kertakirjoitusväline, muuntelunkestävä arkisto, jatkuvasti täydentyvä allekirjoitusketju), näyttö epäonnistuneesta yrityksestä muuttaa merkintää sekä sääntö siitä, miten välineitä säilytetään ja haetaan. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

8 FR 4: Tietojen luottamuksellisuus 6

SR 4.1 **Automaatiojärjestelmä suojaa luottamuksellisen tiedon luvattomalta paljastumiselta sekä siirron aikana että levossa. On määritelty, mikä tieto on luottamuksellista, esimerkiksi reseptit, parametrijoukot, tunnistautumistiedot, konfiguraatiotiedostot tai henkilöön viittaavat diagnostiikkatiedot.** Asiakirja

Mistä sen tunnistaa: Luettelo suojattavista tietolajeista, jossa todetaan, missä niitä säilytetään ja miten niitä siirretään, sekä kunkin kohdalla nimenomainen suojaustoimenpide, esimerkiksi salattu yhteys, salattu tallennusväline tai rajattu jakoresurssi. Pieni yritys pärjää yhden sivun taulukolla: tietolaji, sijainti, kuka saa nähdä sen, mikä suojaa sitä. Vaaditaan tasosta SL 1 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 4.1 RE 1 **Tiedon, joka kulkee ei-luotettujen verkkojen läpi tai jota säilytetään suojatun ympäristön ulkopuolella, luottamuksellisuus varmistetaan teknisin keinoin eikä pelkästään luvata organisatorisessa säännössä.**

Mistä sen tunnistaa: Konfiguraatioote käytössä olevasta siirron salauksesta tai tallennuksen salauksesta, esimerkiksi etähuollon VPN-profiili, ohjausjärjestelmän liitynnän TLS-asetukset tai varmuuskopiovälineiden salaus. Näytöksi riittää päivätty näyttökuva voimassa olevasta asetuksesta. Vaaditaan tasosta SL 2 alkaen, ei tasosta SL 1, koska kyseessä on vaatimuksen laajennus.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 4.1 RE 2 **Luottamuksellisuus varmistetaan myös vyöhykkeiden välisillä rajoilla, jottei tieto tule näkyviin selväkielisenä siirtyessään vyöhykkeeltä toiselle.**

Mistä sen tunnistaa: Vyöhyke- ja yhdyskäytäväsuunnitelma, johon on merkitty, mitkä ylitykset ovat salattuja, sekä rajakomponentin konfiguraatio, esimerkiksi välityslaite, palomuuri tai datadiodi. Liikennekaappaus tai testitallenne, joka osoittaa, ettei rajalla esiinny selväkielistä tietoa. Vaaditaan tasosta SL 4 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 4.2 **On määritelty, miten luottamuksellinen tieto poistetaan luotettavasti, kun laitteita poistetaan käytöstä, ne vaihtavat omistajaa, lähtevät korjattavaksi tai otetaan uudelleen käyttöön, jottei luettavaa jäännöstietoa jää jäljelle.** Asiakirja

Mistä sen tunnistaa: Kirjallinen käytöstä poiston menettely laitetyypeittäisine puhdistusmenetelmineen sekä poistotallenteet, joissa on laitteen tunnistetiedot, päiväys ja suorittanut henkilö. Pieni yritys kirjaa tämän yhtenä rivinä laitetta kohden yhteiseen listaan ja arkistoi ulkoisten hävityspalvelujen todistukset sen rinnalle. Vaaditaan tasosta SL 2 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 4.2 RE 1 **Yhteiskäyttöiset muistialueet tyhjennetään ennen kuin ne osoitetaan uudelleen toiselle käyttäjälle tai prosessille, jottei edellisen käyttäjän sisältöä voi lukea.**

Mistä sen tunnistaa: Valmistajan ilmoitus tai konfiguraatiotallenne uudelleen käytettävien muisti- ja puskurialueiden tyhjennyksestä, täydennettynä testitallenteella vastaanottotarkastuksesta tai kunnossapidosta. Siellä missä komponentti ei tähän kykene, näyttönä on dokumentoitu korvaava toimenpide, esimerkiksi laitteen jakamatta jättäminen eri roolien kesken. Vaaditaan tasosta SL 3 alkaen, ei tasosta SL 1, koska kyseessä on vaatimuksen laajennus.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 4.3 **Siellä missä salausta käytetään, algoritmit, avainpituudet ja avainten käsittely noudattavat tunnustettua hyvää käytäntöä, ja on määritelty, miten avaimet luodaan, jaetaan, säilytetään, vaihdetaan ja peruutetaan.** Asiakirja

Mistä sen tunnistaa: Katsaus järjestelmäkohtaisesti käytettyihin mekanismeihin algoritmeineen, avainpituuksineen ja voimassaoloaikoineen, sekä avainten hallinnan säännöt ja tallenteet avainten vaihdoista ja varmenteiden uusimisista. Mittapuuna toimivat julkiset suositukset, esimerkiksi Saksan BSI:n tekniset ohjeet. Pienessä yrityksessä on varmennelista päättymispäivineen ja muistutuksineen >= 30 päivää ennen päättymistä. Vaaditaan tasosta SL 1 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

9 FR 5: Rajoitettu tiedonkulku, vyöhykkeet ja yhdyskäytävät 11

SR 5.1 **Ohjausjärjestelmä on jaettavissa erillisiin vyöhykkeisiin, ja liikenne näiden vyöhykkeiden välillä kulkee vain määriteltyjen yhdyskäytävien kautta. Jako noudattaa perustetta, joka on selitettävissä, esimerkiksi suojaustarve, omistajuus tai kyseisten laitososien toiminta.** Asiakirja

Mistä sen tunnistaa: Verkkokaavio, jossa näkyvät vyöhykkeet ja niiden väliset yhdyskäytävät, vyöhykeluettelo, jossa on peruste jokaiselle rajalle, sekä erottavien komponenttien konfiguraatio, esimerkiksi VLAN-määrittelyt tai palomuurin liitynnät. Pieni yritys pärjää yhden sivun luonnoksella, jossa toimisto, koneverkko ja etäyhteys ovat kolmena laatikkona keskinäisine yhteyksineen, sekä näyttökuvalla kytkimen VLAN-konfiguraatiosta.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 5.1 RE 1 **Vyöhykkeiden erottelu on toteutettu fyysisesti, eli omilla verkkokomponenteilla ja omalla kaapeloinnilla, eikä se perustu pelkästään yhteiskäyttöisten laitteiden sisäiseen loogiseen konfiguraatioon. Kohta 9.1 tässä listassa, vaaditaan tasosta SL 2 alkaen. Tämän standardin vaatimusten laajennukset eivät ole koskaan pakollisia jo tasolla SL 1.**

Mistä sen tunnistaa: Luettelo verkkokomponenteista, jossa todetaan, mikä kytkin tai reititin palvelee mitäkin vyöhykettä, valokuvat tai kaappikuva erotelluista jakeluista sekä kaapelimerkinnät. Pienet yritykset osoittavat tämän kahdella erillisellä, selvästi merkityllä kytkimellä yhden yhteisen laitteen sijaan ja valokuvalla ohjauskaapista laitosdokumentaatiossa.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 5.1 RE 2 **Automaatioverkkoa voi käyttää riippumatta automaation ulkopuolisista verkoista. Jos toimiston tietotekniikka tai ulkoinen yhteys pettää, laitoksen ohjaus ja valvonta jatkuvat. Vaaditaan tasosta SL 3 alkaen.**

Mistä sen tunnistaa: Riippuvuusluettelo automaatioverkon sisällä käytetyistä palveluista, kuten aikapalvelin, nimipalvelu, hakemistopalvelu tai lisenssipalvelin, ja tieto siitä, missä kukin niistä sijaitsee, sekä testitallenne irrotuskokeesta, jossa yhteys toimiston tietotekniikkaan katkaistiin. Pieni yritys kirjaa tällaisen kokeen tuloksen kunnossapitopäiväkirjaan: runkoyhteys irrotettiin, laitos jatkoi käyntiä, vain toimiston raportit puuttuivat.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 5.1 RE 3 **Vyöhykkeet, joilla on erityisen kriittisiä toimintoja, esimerkiksi turva- tai suojaustoimintoja, on erotettu muista vyöhykkeistä sekä loogisesti että fyysisesti. Vaaditaan tasosta SL 4 alkaen.**

Mistä sen tunnistaa: Kriittisten vyöhykkeiden merkintä vyöhykekaavioon luokittelun perusteineen, näyttö näiden vyöhykkeiden omista verkkokomponenteista ja omasta kaapeloinnista sekä yhdyskäytävien konfiguraatio ja näyttö siitä, ettei yhteistä reittiä ole.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 5.2 **Vyöhykerajoilla liikennettä hallitaan, seurataan ja joko sallitaan tai estetään määriteltyjen sääntöjen mukaan. Kahden vyöhykkeen välillä ei ole reittiä, joka ohittaisi tämän valvontapisteen.**

Mistä sen tunnistaa: Palomuurin tai rajalaitteen viety sääntöjoukko, lokit estetyistä ja sallituista yhteyksistä sekä näyttö siitä, ettei sivureittejä ole, esimerkiksi tarkastus laitostietokoneiden lisäverkkokorteista, modeemeista tai mobiilireitittimistä. Pieni yritys osoittaa tämän yhden palomuurinsa sääntöviennillä ja lyhyellä kierrosmuistiolla, joka vahvistaa, ettei yhdessäkään ohjauskaapissa ole suunnittelematonta reititintä.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 5.2 RE 1 **Vyöhykerajan sääntöjoukko toimii periaatteella, jossa kaikki estetään ellei sitä ole nimenomaisesti sallittu. Jokainen salliva sääntö on perusteltu erikseen ja sidottu käyttötarkoitukseen. Vaaditaan tasosta SL 2 alkaen.**

Mistä sen tunnistaa: Sääntöjoukko, jossa näkyy loppusääntö, joka pudottaa loput, sekä sallimislista, jossa on jokaisesta säännöstä lähde, kohde, palvelu, käyttötarkoitus ja vastuuhenkilö. Pienissä yrityksissä tämä lista on viisisarakkeisena taulukkona palomuurin viennin rinnalla, ja se käydään kerran vuodessa läpi sellaisten sääntöjen löytämiseksi, joita kukaan ei enää tarvitse.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 5.2 RE 2 **Automaatioverkon voi tietoisesti katkaista kaikista ulkoisista yhteyksistä, jolloin se jatkaa toimintaansa saarekekäytössä. Toimenpide on käynnistettävissä ilman laitoksen pysäyttämistä. Vaaditaan tasosta SL 3 alkaen.**

Mistä sen tunnistaa: Kuvaus erotusmenettelystä, jossa todetaan, kuka sen saa käynnistää ja miten, näyttö teknisestä toteutuksesta, esimerkiksi hätäsääntöjoukko tai merkitty erotuskytkin, sekä tallenne harjoituksesta, jossa erotus todella tehtiin. Pieni yritys tekee harjoituksen kerran vuodessa kunnossapidon yhteydessä ja kirjaa päiväyksen, keston ja mahdolliset poikkeavuudet.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 5.2 RE 3 **Jos vyöhykerajan laite vikaantuu tai menettää sääntönsä, se estää liikenteen sen sijaan, että päästäisi sen läpi. Vika ei jätä jälkeensä avointa yhteyttä. Vaaditaan tasosta SL 4 alkaen.**

Mistä sen tunnistaa: Toimittajan ilmoitus tai konfiguraatiosta saatava näyttö siitä, miten komponentti toimii vikaantuessaan ja uudelleenkäynnistyksessä, testitallenne tahallisesti aiheutetusta viasta havaittuine tuloksineen sekä yhteensovitus laitoksen riskin arvioinnin kanssa, koska liikenteen estävällä rajalla voi prosessista riippuen olla itsessään seurauksia.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 5.3 **Yleiset henkilöiden väliset viestintäpalvelut, kuten sähköposti, pikaviestit tai videopuhelut, ovat estettävissä automaatiolaitteissa ja automaatioverkoissa. Eston laajuus on määritelty ja perusteltu.**

Mistä sen tunnistaa: Määrittely siitä, mitkä palvelut eivät ole sallittuja automaatioverkossa, sekä tekninen toteutus: estetyt portit ja kohteet sääntöjoukossa, poistetut tai estetyt sovellukset käyttöasemilla ja näyttö laitteiden ohjelmistoluettelosta. Pieni yritys hoitaa tämän HMI-aseman sovellusestolla ja säännöllä, jonka mukaan koneverkosta ulos suuntautuva sähköposti- ja verkkoliikenne estetään.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 5.3 RE 1 **Tällaiset henkilöiden väliset viestintäpalvelut estetään koko automaatioverkossa, eikä niitä vain osittain rajoiteta tai rajata yksittäisiin laitteisiin. Vaaditaan tasosta SL 2 alkaen.**

Mistä sen tunnistaa: Näyttö siitä, että esto koskee jokaista vyöhykkeen laitetta, esimerkiksi katselmointi vyöhykkeen jokaisen tietokoneen asennetuista ohjelmistoista ja yhteystesti satunnaiselta laitostietokoneelta. Pienet yritykset osoittavat tämän laitelistalla, jonka jokainen rivi on kuitattu tarkastuspäivällä, ja näyttökuvalla epäonnistuneesta yhteysyrityksestä.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 5.4 **Sovellusten tiedot ja toiminnot on jaettu niin, etteivät prosessit, joilla on eri suojaustarve tai eri oikeudet, ylety samoille alueille. Erottelu on suunniteltu järjestelmäarkkitehtuuriin eikä jää asennuksen sattuman varaan.**

Mistä sen tunnistaa: Katsaus sovelluksiin, jossa todetaan, mitä tietoja ja palveluja ne käyttävät ja mitkä tilit niiden takana ovat, erillisten instanssien, tietokantojen, hakemistojen tai virtuaalikoneiden konfiguraatio sekä aluekohtainen oikeuslista. Pieni yritys ratkaisee tämän erillisillä käyttäjätileillä ja erillisillä datakansioilla suunnittelulle ja käytölle sekä merkinnällä siitä, mikä sovellus käyttää mitäkin kansiota.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

10 FR 6: Oikea-aikainen reagointi tapahtumiin 3

SR 6.1 **Järjestelmään kerätyt lokitallenteet ovat siihen valtuutettujen henkilöiden ja roolien luettavissa ja arvioitavissa häiritsemättä laitoksen käynnissä olevaa toimintaa, ja pääsy näihin tallenteisiin on itsessään rajattu valtuutettuihin käyttäjiin.**

Mistä sen tunnistaa: Rooli- ja oikeusmatriisi siitä, kuka saa katsoa lokitietoja, sekä näyttökuva tai vienti todella haetusta lokinäkymästä aikaleimoineen. Lisäksi lyhyt merkintä haussa käytetystä reitistä, esimerkiksi ohjaimen käyttöliittymä, lokipalvelin tai tiedostovienti. Pienet yritykset pärjäävät yhden sivun katsauksella laitosta kohden: missä loki sijaitsee, kenellä on lukuoikeus ja miten se haetaan. Kerran vuodessa tehty testihaku, kirjattuna kunnossapitopäiväkirjaan, osoittaa reitin toimivan. Koskee tasosta SL 1 alkaen kaikkia turvallisuustasoja.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 6.1 RE 1 **Lokitallenteet ovat haettavissa koneliitynnän kautta, jolloin analyysityökalut voivat käsitellä niitä edelleen ilman käsin kirjoittamista, ja tieto tarjotaan dokumentoidussa, yleisesti käytetyssä muodossa.**

Mistä sen tunnistaa: Kuvaus käytössä olevasta liitynnästä muotoineen, esimerkiksi syslog, OPC UA Alarms and Conditions, REST-kysely tai CSV-vienti, sekä esimerkkitallenne ja vastaanottavan järjestelmän konfiguraatio. Näyttönä voi olla ote SIEM-järjestelmän tai lokinkerääjän konfiguraatiosta yhdessä todisteen kanssa saapuneista tallenteista. Ilman SIEM-järjestelmää riittää lokinkerääjä yksinkertaisella palvelimella, joka hakee lokit yön aikana skriptillä ja tallentaa ne; näyttönä on itse skripti ja hakemistolistaus kerätyistä tiedostoista. Laajennuksena tämä vaaditaan vasta tasosta SL 3 alkaen, ei tasosta SL 1.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 6.2 **Järjestelmän tietoturvan kannalta olennaista toimintaa seurataan jatkuvasti, seuranta havaitsee hyökkäysyritykset ja väärinkäytön ja ilmoittaa niistä viipymättä nimetylle yhteyspisteelle, ja tähän käytetyt työkalut, ilmoitusreitit ja vastuut on määritelty.**

Mistä sen tunnistaa: Katsaus vyöhykekohtaisiin seurantatyökaluihin, esimerkiksi verkkoanturi, virustorjunnan hälytykset, palomuurin hälytykset tai eheystarkistus, ja tieto siitä, kuka hälytyksen vastaanottaa ja missä ajassa reagointia odotetaan. Näyttönä toimivat hälytysten konfiguraatiot, luettelo viime kuukausina syntyneistä hälytyksistä ja niiden käsittelymerkinnät. Pienet yritykset eivät tarvitse ympärivuorokautista valvomoa: riittää yhteinen postilaatikko tai tikettijono, joka kokoaa olemassa olevien järjestelmien hälytykset, sekä kiinteä sääntö siitä, että nimetty henkilö käy sen läpi jokaisena työpäivänä, ja tämä osoitetaan postilaatikon historialla. Vaaditaan tasosta SL 2 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

11 FR 7: Resurssien saatavuus 13

SR 7.1 **Ylikuormituksessa tai tarkoituksellisissa tulvahyökkäyksissä järjestelmä pysyy määritellyssä käyttötilassa, olennaiset ohjaustoiminnot jatkavat toimintaansa, eikä yksittäisen palvelun vikaantuminen vedä laitosta mukanaan.**

Mistä sen tunnistaa: Suojausmekanismien konfiguraatio (nopeusrajoitus, yhteysrajat, yleislähetystulvan hallinta kytkimissä), valmistajan ilmoitukset käyttäytymisestä kuormituksessa sekä tallenne kuormitustestistä tai todellisesta ylikuormitustapahtumasta ohjaustoiminnon havainnointeineen. Vaaditaan tasosta SL 1 alkaen. Pieni yritys kattaa tämän näyttökuvilla kytkimen ja palomuurin asetuksista ja lyhyellä merkinnällä siitä, mikä toiminto pysyi käynnissä tärkeimmän solun testin aikana.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 7.1 RE 1 **Yksittäisten komponenttien verkkoon syöttämälle tietoliikennekuormalle on asetettu katto, jolloin viallinen tai vaarantunut komponentti ei voi tulvittaa verkkosegmenttiä.**

Mistä sen tunnistaa: Porttikohtaiset kaistanleveys- ja ryhmälähetysrajat verkkokomponenteissa, näyttö katosta jokaisen yhteyden osalta sekä mittaus laitekohtaisesta todellisesta peruskuormasta. Vaaditaan tasosta SL 2 alkaen, ei tasosta SL 1. Ilman hallittavia kytkimiä tätä riviä ei voi osoittaa, ja se on silloin avoin kohta.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 7.1 RE 2 **Tarkasteltavan järjestelmän sisäinen ylikuormitustilanne ei leviä viereisiin järjestelmiin tai verkkoihin; ulospäin kohdistuva vaikutus on teknisesti rajattu.**

Mistä sen tunnistaa: Segmentointi- ja suodatussäännöt rajoilla, näyttö ulos suuntautuvan liikenteen rajoittamisesta sekä testitallenne, joka osoittaa, ettei soluverkossa synnytetty kuorma heikentänyt toimisto- tai naapuriverkkoa. Vaaditaan tasosta SL 3 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 7.2 **Suoritinajan, muistin, tallennustilan ja verkon kaistanleveyden käyttö on rajattu niin, ettei yksittäinen prosessi tai palvelu voi kuluttaa ohjaukseen tarvittavia resursseja.**

Mistä sen tunnistaa: Resurssirajojen konfiguraatio (kiintiöt, prosessien prioriteetit, muistirajat), analyysi kuormituksen seurannasta edustavalta ajanjaksolta sekä raja-arvot, joissa varoitus annetaan. Vaaditaan tasosta SL 1 alkaen. Pienet yritykset käyttävät käyttöjärjestelmän omia keinoja ja yksinkertaista seurantaa, jossa levytilasta ja suorittimen kuormasta lähtee hälytys sähköpostiin.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 7.3 **Järjestelmäkonfiguraatioista, sovellusten tiedoista ja ohjelmaversioista on olemassa varmuuskopiot; ne ovat tehtävissä keskeyttämättä käynnissä olevaa toimintaa, ja ne on suojattu luvattomalta pääsyltä ja muuttamiselta.** Asiakirja

Mistä sen tunnistaa: Varmuuskopioinnin malli, joka kattaa laajuuden, tiheyden ja säilytysajan, viimeisimpien ajojen varmuuskopiolokit sekä näyttö varmuuskopiovälineiden pääsysuojauksesta (erillinen säilytys, salaus, omat käyttöoikeudet). Vaaditaan tasosta SL 1 alkaen. Pieni yritys varmuuskopioi PLC-projektit ja HMI-versiot salatulle välineelle, joka irrotetaan fyysisesti varmuuskopioinnin jälkeen, ja kirjaa päiväyksen ja version yksinkertaiseen listaan.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 7.3 RE 1 **Varmuuskopioiden käyttökelpoisuus on todennettu; on osoitettu, että niistä on todella palautettavissa toimiva tila.**

Mistä sen tunnistaa: Tallenne palautustestistä päiväyksineen, testattuine varmuuskopioversioineen, kohdejärjestelmineen ja tuloksineen, vähintään kriittisistä komponenteista. Vaaditaan tasosta SL 2 alkaen, ei tasosta SL 1. Pienet yritykset tarkastavat kerran vuodessa pistokokeena yhden PLC-ohjelman ja yhden HMI-vedoksen varalaitteella ja kirjaavat tuloksen kahdella lauseella.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 7.3 RE 2 **Varmuuskopiointi ajetaan automaattisesti määritellyn aikataulun mukaan; epäonnistunut ajo havaitaan ja siitä ilmoitetaan.**

Mistä sen tunnistaa: Varmuuskopiotyön aikataulu, aukottomat suorituslokit sekä näyttö vikailmoituksesta ajosta, joka ei onnistunut (hälytys, tiketti, sähköposti). Vaaditaan tasosta SL 3 alkaen.

◯ Avoin ◯ Kesken ◯ Täytetty ◯ Ei koske

Näyttö / perustelu

SR 7.4 **Häiriön, vikaantumisen tai hyökkäyksen jälkeen järjestelmä on palautettavissa tunnettuun, turvalliseen tilaan; palautus on harjoiteltu ja vastuut on nimetty.** Asiakirja

Mistä sen tunnistaa: Uudelleenkäynnistyksen suunnitelma jokaiselle kriittiselle komponentille järjestyksineen, tarvittavine tallennusvälineineen, yhteystietoineen ja tavoiteaikoineen, sekä tallenne viimeisimmästä palautusharjoituksesta. Vaaditaan tasosta SL 1 alkaen. Pieni yritys pärjää yhden sivun käynnistyskortilla linjaa kohden, ohjauskaapissa säilytettynä ja aina varaosan vaihdon yhteydessä tarkastettuna.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 7.5 **Jos tavanomainen sähkönsyöttö pettää, järjestelmä siirtyy määriteltyyn tilaan: joko syöttö jatkuu varalähteestä tai tapahtuu hallittu alasajo turvallista tilaa menettämättä.**

Mistä sen tunnistaa: Mitoitus- ja kunnossapitonäyttö keskeytymättömästä sähkönsyötöstä tai varavoimakoneesta, testitallenne viimeisimmästä akku- tai kuormitustestistä sekä kuvaus käyttäytymisestä vaihdon hetkellä ja verkkosähkön palatessa. Vaaditaan tasosta SL 1 alkaen. Pienet yritykset testaavat UPS-laitteen kuormalla kerran vuodessa ja kirjaavat testipäivän, siltausajan ja akun iän.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 7.6 **Järjestelmän verkko- ja tietoturva-asetukset on kiinnitetty hyväksyttyyn tavoitetilaan, poikkeamat tavoitetilasta ovat havaittavissa, ja nykytila on haettavissa milloin tahansa.** Asiakirja

Mistä sen tunnistaa: Hyväksytty tavoitekonfiguraatio laiteluokittain (kovennusmäärittely), laitteiden nykyiset konfiguraatiotilat sekä tavoitteen ja toteuman vertailun tulos poikkeamaluetteloineen ja kunkin poikkeaman syineen. Vaaditaan tasosta SL 1 alkaen. Pieni yritys tallentaa konfiguraatioviennit versionhallintaan ja vertaa niitä ennen jokaista muutosta ja sen jälkeen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 7.6 RE 1 **Tietoturva-asetusten nykytila on tulostettavissa koneluettavassa muodossa, jolloin sen voi tarkastaa automaattisesti tavoitetilaa vastaan.**

Mistä sen tunnistaa: Esimerkkituloste koneluettavassa muodossa (konfiguraatiovienti, rakenteinen tiedosto, liityntäkysely) ja skripti tai työkalu, joka tekee vertailun tavoitetilaan, sekä yhden ajon tulosraportti. Vaaditaan tasosta SL 3 alkaen.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 7.7 **Järjestelmä on rajattu toimintaan tarvittaviin toimintoihin; tarpeettomat palvelut, portit, protokollat ja liitynnät on poistettu käytöstä tai poistettu kokonaan.**

Mistä sen tunnistaa: Luettelo komponenttikohtaisista aktiivisista palveluista ja avoimista porteista tarpeen perusteluineen, näyttö siitä, että loput on poistettu käytöstä (konfiguraatio, porttiskannauksen tulos), sekä sääntö USB- ja huoltoliitynnöistä. Vaaditaan tasosta SL 1 alkaen. Pienet yritykset ajavat yksinkertaisen porttiskannauksen segmenttiä kohden ja perustelevat jokaisen avoimen kohdan yhdellä rivillä.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu

SR 7.8 **Ajantasainen luettelo kaikista järjestelmän komponenteista valmistajineen, tyyppeineen, laiteohjelmisto- tai ohjelmistoversioineen ja verkko-osoitteineen on saatavilla, ja se päivitetään muutosten yhteydessä.** Asiakirja

Mistä sen tunnistaa: Komponenttiluettelo tarkistuspäivineen ja omistajineen, näyttö ylläpidosta muutoshistorian kautta sekä vertailu verkkokartoitukseen kirjaamattomien laitteiden löytämiseksi. Vaaditaan tasosta SL 2 alkaen, ei tasosta SL 1. Pienessä yrityksessä luettelo on taulukkona ja se päivitetään kiinteänä sääntönä aina kun laite vaihdetaan ja aina kun laiteohjelmisto päivitetään.

○ Avoin ○ Kesken ○ Täytetty ○ Ei koske

Näyttö / perustelu