

IEC 62443-3-3:2013 Teollisuusautomaation järjestelmien tietoturva vaatimukset

Seitsemän perusvaatimusta, 51 järjestelmävaatimusta

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

IEC 62443-3-3 on sertifiointivissa, ja sertifiointin kohteena on järjestelmä, ei organisaatio eikä henkilö. Reitit ovat ISASecure SSA ja IEC 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 kirjautumisnäkyvästä 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.

Avoim	Kesken	Täytetty	Ei koske
-------	--------	----------	----------

Näyttö / perustelu

SR 1.1 RE 1 Jokainen henkilökäyttäjä toimii henkilökohtaisella tunnisteella, joka on annettu vain hänelle. Yhteiskäyttöiset ja vuorokohdaiset 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.

Avoim	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, esimerkiksi tallenne 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 kuluva ajan. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen, ei tasolla SL 1.

Avoim	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 esimerkkitalenteet kirjautumisista valvomosta ja käyttöpaneelilta. Vaatimuksen laajennus, vaaditaan vasta tasosta SL 4 alkaen.

Avoim	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 salasana, avaimet, varmenteet ja tunnistevälineet annetaan hallitusti, vaihdetaan kun paljastumista epäillään ja peruutetaan tarvittaessa. Toimitustilan oletustilit ja tehdassalasana vaihdetaan ennen käyttöönottoa.

Mistä sen tunnistaa: Luettelo annetuista tunnistevälineistä ja varmenteista vastaanottajineen ja päiväyksineen, näyttö vaihdoista ja peruutuksista sekä laitekohtainen käyttöönoton tarkistuslista, jossa kohta tehdassalasanana 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 säilytyksessä, 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 tasolla 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, kantamieineen ja salausmenetelmieineen, tukiaseman konfiguraatioote sekä luettelo hyväksytyistä päätelaitteista. Pieni yritys kirjaa lisäksi, mitkä laitteiden langattomat liittymät 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 tunnistus 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 salasanauudelleenkäyttö estetty, sekä asetettu enimmäisvoimassaoloaika. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

Avoin	Kesken	Täytetty	Ei koske
-------	--------	----------	----------

Näyttö / perustelu

SR 1.7 RE 2 Salasanauudelleenkäytön 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 myönnettyistä 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, testitalenne 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 kirjautumisnäkömästä 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 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 etäyhteyksireiteistä 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 myönnettyt 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 määrääjäksi, 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 myönnettyistä 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.

Avoim 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, tulostistoinen 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.

Avoim 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 hyväksytyihin laitteisiin.

Mistä sen tunnistaa: Laitteiden käyttöä koskeva säännöstö, luettelo hyväksytyistä huoltolaitteista tunnistuneen 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 merkittävää huoltotikkua, joille kirjoitetaan vain yhdellä siirtoasemalla.

Avoim 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 haittaohjelasuojaus ja korjauspäivitysten taso, sekä huoltolaittekohtaiset tarkastustallenteet ja näyttö teknisestä pakottamisesta, esimerkiksi siirtoaseman tai verkon pääsynhallinnan kautta. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

Avoim 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 konfiguraatioite rajoituksesta, esimerkiksi skriptien suoritus HMI-selaimessa poissa käytöstä ja makrot analyysitiedoissa estetty. Vaaditaan tasosta SL 1 alkaen. Riittää yhden sivun määrittely, joka kattaa ne kolme tai neljä tapausta, jotka todella ovat olemassa.

Avoim 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: Konfiguraatioite allekirjoituksen tarkistuksesta tai tarkistussummien valvonnasta sekä testitallenne, jossa muunneltu tai allekirjoittamaton koodi hylätään. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

Avoim Kesken Täytetty Ei koske

Näyttö / perustelu

SR 2.5 Istunto lukitaan, kun käyttäjä ei ole toiminut määritettyyn 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 lukitusnäkyvästä, jossa hälytysrivi näkyy edelleen.

Avoin Kesken Täytetty Ei koske

Näyttö / perustelu

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

Mistä sen tunnistaa: Etäyhteyden konfiguraatio toimeettomuuden aikarajoiheen, 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 kirjautumisyriitykset hylätään.

Mistä sen tunnistaa: Konfiguraatioote roolikohtaisesta ylärajasta, esimerkiksi ≤ 1 samanaikainen istunto suunnittelutileillä, sekä testitallenne hyläystä toisesta kirjautumisyriityksestä. 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, käynnistyneen 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 liitettynä lähteineen sekä analyysi, joka asettaa vähintään kahden komponentin tapahtumat samalle aikajalalle. 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 korvaukseen 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: Määritely 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 aikälähteestä, jotta eri komponenttien tapahtumat ovat asetettavissa keskinäiseen järjestykseen.

Mistä sen tunnistaa: Ilmoitus komponenttikohtaisesti käytetystä aikälähteestä 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 aikälähteeseen 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 aikälähteen suojauksesta, esimerkiksi todennettu ajan tahdistus, rajausta 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, konfiguraatietietoja 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 mitään eheysmekanismeja (tarkistussumma, viestin todennuskoodi, allekirjoitetut sanomat), konfiguraatioite 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.

Avoim	Kesken	Täytetty	Ei koske
-------	--------	----------	----------

Näyttö / perustelu

SR 3.1 RE 1 Siirron aikainen eheyden suojaus perustuu salausrakenteisiin, 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 salausrakenteista ja avainpituuksista, viittaus taustalla olevaan avainten hallintaan sekä konfiguraatioiteet (esimerkiksi TLS-salausvalikoimat, OPC UA SecurityPolicy, IPsec-profiilit). Pienet yritykset luottavat ohjaintensa turvallisiin oletusprofiileihin ja arkistivat näyttökuvan voimassa olevasta asetuksesta. Vaatimuksen laajennus, vaaditaan tasosta SL 3 alkaen.

Avoim	Kesken	Täytetty	Ei koske
-------	--------	----------	----------

Näyttö / perustelu

SR 3.2 Haittakoodia vastaan on olemassa suojausmekanismi, 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 tunnistajien 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.

Avoim	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 virustarkistukseen välityspisteeksi ja kirjaavat tämän työohjeeseen. Vaatimuksen laajennus, vaaditaan tasosta SL 2 alkaen.

Avoim	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.

Avoim	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 konfiguraatietiedostoja.

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 alarajotila) perusteluineen riskin arvioinnista, ohjaimen konfiguraatioote sekä näyttö vikatestistä, esimerkiksi kaapelikatkoksta 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 verrattuna 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 toimetoman 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 testitalenne, 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 testitalenne, 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 pääsylvä, 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, muuntelukestävä 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, konfiguraatiodokumentit 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: Konfiguraatioite 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, palomuuuri 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 laitetyyppittäisine 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.

Avoim 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.

Avoim 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 liittynät. Pieni yritys pärjää yhden sivun luonnoksella, jossa toimisto, koneverkko ja etäyhteys ovat kolmena laatikkona keskinäisine yhteyksineen, sekä näyttökuvalla kytkimen VLAN-konfiguraatiosta.

Avoim 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 mitään vyöhykettä, valokuvat tai kaappikuva erotelluista jakeluista sekä kaapelimerkinnot. Pienet yritykset osoittavat tämän kahdella erillisellä, selvästi merkityllä kytkimellä yhden yhteisen laitteen sijaan ja valokuvalla ohjauskaapista laitosdokumentaatioissa.

Avoim 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.

Avoim 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.

Avoim 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 laitos tietokoneiden 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 laitos tietokoneelta. 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.

Avoim 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 lokinäköymästä aikaleimoinen. Lisäksi lyhyt merkintä haussa käytetyistä 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.

Avoim Kesken Täytetty Ei koske

Näyttö / perustelu

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

Mistä sen tunnistaa: Kuvaus käytössä olevasta liittynästä muotoineen, esimerkiksi syslog, OPC UA Alarms and Conditions, REST-kysely tai CSV-vienti, sekä esimerkkitalenne 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.

Avoim 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 nimetyille 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.

Avoim 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.

Avoim 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 pääsylvä ja muuttamiselta.[Asiakirja](#)

Mistä sen tunnistaa: Varmuuskopioinnin malli, joka kattaa laajuuden, tiheyden ja säilytysajan, viimeisimpien ajojen varmuuskopiolokit sekä näyttö varmuuskopiovälineiden pääsyysojauksesta (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 harjoitettu 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 määritellyyn tilaan: joko syöttö jatkuu varalähteestä tai tapahtuu hallittu alasajo turvallista tilaa menettämättä.

Mistä sen tunnistaa: Mitoitus- ja kunnossapitönäyttö keskeytymättömästä sähkönsyötöstä tai varavaimakoneesta, 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 poikkeamaluetteloihin 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 (konfiguraatioviennit, rakenteinen tiedosto, liityntäkysely) ja skripti tai työkalu, joka tekee vertailun tavoitetilaan, sekä yhden ajon tulostusraportti. 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, tyyppineen, 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