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 Asiakirja

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.

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 Asiakirja

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.

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