

IEC 62443-4-1:2018 Turvaline tootearenduse olelusring tööstusautomaatikas

Turvalise arenduse olelusring, kaheksa praktikat

47 nõuet. Selle standardi järgi on võimalik sertifitseerida akrediteeritud sertifitseerimisasutuses. Versioon 07/2026.

IEC 62443-4-1 on sertifitseeritav, kuid objekt on ebatavaline: sertifitseeritakse nimetatud arendusorganisatsiooni arendusprotsess, see tähendab turvalise olelusringi üht konkreetset dokumenteeritud versiooni. Sertifitseeritud ei ole toode ega isik. Teed on ISASecure SDLA ja IEC CB Scheme. Praeguse seisuga ei loo selline sertifikaat vastavuseeldust EU Cyber Resilience Act suhtes. Seda ei aeta segi standardiga IEC 62443-4-2, mis esitab nõuded komponendile endale. See loend on töövahend enesehindamiseks, mitte tõend.

Ettevõtte

Kuupäev

Täitja

5 Praktika 1: Turvalisuse juhtimine (SM)

13

SM-1

Olemas on määratletud tootearenduse olelusring, mis kannab turvalisust läbi kõigi faaside alates esimesest ideest kuni toote kasutuselt kõrvaldamiseni, ja just selle järgi tegelikult töötatakse.

Dokument

Mille järgi seda näeb: Protsessikirjeldus või tööjuhend, kus on loetletud faasid, iga faasi tulemid ja üleandmispunktid, koos tõenditega käimasolevast projektist, mis näitavad, et faasid tõesti läbiti. Väike ettevõtte saab hakkama ühe leheküljega faasi kohta ja kontrollnimekirjaga piletisüsteemis; oluline on, et dokumenteeritud protsess ja igapäevane praktika kattuvad.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

SM-2

Igal turvalise arenduse olelusringi ülesandel on määratud vastutaja ja see jaotus on osalistele teada.

Dokument

Mille järgi seda näeb: Rollide ja vastutuse maatriks, mis seob iga protsessisammu nimetatud rolliga, täiendatuna nende rollide praeguse täitmisega. Vaid mõne inimese puhul piisab tabelist rolli, ülesande ja isikuga; oluline on asendamise kord puhkuse ja haiguse ajaks.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

SM-3

Jälgitavalt on määratletud, millised tooted, variandid, väljalasked ja komponendid kuuluvad turvalise arenduse olelusringi alla ja millised mitte.

Dokument

Mille järgi seda näeb: Käsitlusalaske kuuluvate toodete ja versiooniseisude loend koos põhjendusega kaasamise ja väljajätmise kohta, ajakohastatud iga uue väljalaskega. Praktikast toimib hästi veerg tooteülevaates, kus igal real on jah või ei ning üks lause põhjendust.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

SM-4

Turvaülesandeid täitvatel inimestel on selleks vajalik erialane pädevus ja seda pädevust arendatakse ning värskendatakse sihipäraselt.

Mille järgi seda näeb: Pädevusprofiil iga turvarolli kohta, kvalifikatsiooni kirjed, koolituskava ja osalemise kirjed, täiendatuna lünkade ülevaatega. Väikesed ettevõtted tõendavad seda tunnistuste, konverentsidel või veebiseminaridel osalemise ja kord aastas toimuva lühikese ülevaatusena, kus fikseeritakse, kes millise lünga mis ajaks sulgeb ja kus vaja, ostetakse väline pädevus sisse.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

SM-5

Turvalise arenduse olelusringi käsitlusala on piiritletud ja nimetab kaasatud asukohad, organisatsiooniüksused, tarnijate panused ja arenduskeskkonnad ning selle käsitlusala piirid.

Dokument

Mille järgi seda näeb: Käsitlusala kirjeldus, mis hõlmab asukohad, meeskonnad, sisseostetud osad ja süsteemid, lisaks väliste liideste visand. Kes arendab ühes asukohas, kirjeldab seda mõne lausega ja nimetab selgelt, mis jääb välja, näiteks väljaspool arendatud koostud või kolmanda osapoole majutus.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

SM-6 Iga kasutajatele tarnitava elemendi puhul, olgu tarkvara, püsivara, konfiguratsioon või kaasnev fail, on võimalik terviklust kontrollida, nii et saajad tuvastavad märkamatu muutmise.

Mille järgi seda näeb: Allkirjad või avaldatud kontrollsummad iga tarnepaketi kohta, meetodi kirjeldus ja üks näide tegelikust väljalaskest, koos juhiseiga kliendile, kuidas kontroll teha. Väikestele meeskondadele piisab allkirjastatud kontrollsummafailist allalaadimise kõrval ja ühest lõigust väljalaskemärkmetes.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SM-7 Arenduseks, koostamiseks ja testimiseks kasutatavad keskkonnad on kaitstud volitamata pääsu ning lähtekoodi, koostetööriistade ja artefaktide muutmise eest.

Mille järgi seda näeb: Pääsu ohjamise kontseptsioon hoidla, koosteserveri ja testsüsteemide jaoks, pääsuloendid koos viimase ülevaatuses kuupäevaga, turvalisust puudutavate muudatuste kirjed ja tõend, et tootmiskeskonna ja arenduskeskkonna pääs on lahutatud. Ilma majasisese infotehnoloogia osakonnata piisab kahefaktorilisest sisselogimisest, kaitstud peaharust kohustusliku ülevaatuses ja poolaastasest ülevaatuses, kellel on veel pääs.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SM-8 Tarnete allkirjastamiseks kasutatavad privaativõtmed on kaitstud avalikuks tuleku ja väärkasutuse eest ning nende kasutamine on piiratud volitatud inimeste ja süsteemidega.

Mille järgi seda näeb: Võtmete hoiustamise, pääsu, uuendamise ja tühistamise kirjeldus, tõend kaitstud hoiustamisest, näiteks riistvaraline turvavõti või võtmehaldusteenus, lisaks allkirjastamistoimingute kirjed. Väike ettevõtte hoiab allkirjastamisvõtit riistvaralisel turvavõtmel, dokumenteerib kaks pääsuõigusega inimest ja hoiab kaotuse juhiks korda valmis.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SM-9 Ostetud või üle võetud komponentide puhul, sealhulgas avatud lähtekoodiga tarkvara, on tarnijale esitatavad turvaootused määratletud ja neid rakendatakse valikul.[Dokument](#)

Mille järgi seda näeb: Turvanõuded tarnija spetsifikatsioonides või lepingutes, kolmanda osapoole komponentide valikukriteeriumid, kõigi kolmanda osapoole komponentide loetelu koos versiooni ja allikaga, lisaks hinnang, kas tarnija vastab ootustele. Ilma ostuosakonnata piisab ajakohasest komponentide loendist, kus veerg fikseerib, kas tarnija turvavärskendused ja teavituskanalid on üle vaadatud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SM-10 Kolmanda osapoole tellimustööna arendatud komponentidele kehtivad samad turvanõuded nagu majasisesele arendusele ja nende täitmist tõendatakse.

Mille järgi seda näeb: Ostutellimus või lepingudokumentid, milles on kirjas nõutud turvakohustused, teenusepakkuja tõendid rakendatud praktikate kohta, vastuvõtmise kirjed ja oma kontrollide tulemused tarnitud töö kohta. Ilma auditeerimise piisab lepingulisest kinnitusest, teenusepakkuja testitulemuste esitamisest ja ühest oma pistelisest kontrollist enne vastuvõtmist.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SM-11 Turvalisust puudutavad leiud kõigist allikatest, testidest, ülevaadustest, kasutajate teadetest ja kolmandate osapoolte teavitustest, registreeritakse, hinnatakse nende mõju, määratakse vastutaja ja tähtaeg ning neid jälgitakse kuni sulgemiseni.[Dokument](#)

Mille järgi seda näeb: Vigade ja piletite süsteem eraldi märgistusega turvateemade jaoks ning iga kande juures mõju hinnang, vastutaja, tähtaeg ja sulgemismärge, lisaks aruanne avatud punktide kohta. Väike meeskond kasutab olemasolevas piletisüsteemis silti ja püsivat päevakorrapunkti iganädalasel koosolekul.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SM-12

Enne toote väljalaske tõendatakse ja dokumenteeritakse, et turvalise arenduse olelusringi ettenähtud sammud tehti tegelikult läbi ja et vastavad kirjed valmisid.[Dokument](#)

Mille järgi seda näeb: Iga väljalaske kohta väljalaske ülevaatus võrdluses protsessisammudega, viited vastavatele kirjetele ja dokumenteeritud väljalaskeotsus koos kuupäeva ja allkirjaga. Praktikas toimib hästi väljalaske kontrollnimekiri, mis ei luba tarnet ilma kõigi linnukesteta; avatud punktid põhjendatakse ja neile antakse kuupäev.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SM-13

Turvalise arenduse olelusringi ennast seatakse korrapäraselt kahtluse alla ja parendatakse, tuginedes juhtumitest, testitulemustest, klientide tagasisidest ja ohupildist saadud teadmistele.

Mille järgi seda näeb: Protsessi ülevaatus kirjed, näiteks juhtkonnapoolne ülevaatus või retrospektiiv, koos käivitatud protsessimuudatuste, nende elluviimise seisuga ja viitega algpõhjusele. Kes kasutab standardi küpsustasemeid, fikseerib iga praktika praeguse seisuga ja sihi; küpsustase 4 nõuab just seda tõendit pideva parendamise kohta. Väikesele ettevõttele piisab ühest koosolekust aastas koos protokolliga ja kolmest konkreetsest parendusest.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6 Praktika 2: Turvanõuete spetsifitseerimine (SR)

5

SR-1

Toote kavandatud kontekst on kirjeldatud: eeldatav töökeskkond, turvameetmed, mida sellelt keskkonnalt eeldatakse, kavandatud kasutajarühmad ja rollid, eeldatavad usalduspiirid ning kasutusviisid, milleks toode selgelt ei ole mõeldud.[Dokument](#)

Mille järgi seda näeb: Toote turvakonteksti kirjeldus kas eraldi dokumendina või toote spetsifikatsiooni püsiva osana, mis hõlmab võrgukeskkonna, eeldatavad välised kaitsed nagu tulemüür või füüsiline pääsu ohjamine, rollide loetelu ja selge loetelu käsitlusala välja jäävatest kasutusviisidest. Väike ettevõtte piirneb kahe leheküljega, lisab lihtsa visandi käitiseskeskkonnast ja laseb toote omanikul selle kuupäeva ning kinnitusega varustada.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SR-2

Tootel on ohumudel, mis kaardistab andmevood, liidesed, usalduspiirid ja ründeteed, nimetab neist tulenevad ohud ja nende võimaliku mõju ning määrab vastumeetmed. Seda vaadatakse üle ja ajakohastatakse oluliste muutuste korral ning vähemalt kord iga toote väljalaske kohta ja avatud punkte jälgitakse kuni sulgemiseni.[Dokument](#)

Mille järgi seda näeb: Ohumudel koos andmevoo skeemiga, ohtude loend iga liidese kohta, määratud vastumeetmed ja avatud punktide seis, lisaks muutuste ajalugu koos kuupäeva ja autoriga. Väike ettevõtte saab hakkama ühe tabeliga liidese kohta, veergudega selle kohta, mis seal valesti minna võib, kui halb see oleks, mida selle vastu tehakse ja kes selle üle vaatab.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SR-3

Toote turvanõuded on määratletud ja dokumenteeritud. Need katavad ohumudeli tulemused, kirjeldatud toote turvakonteksti, kohalduvad õiguslikud ja lepingulised kohustused ning eesmärgiks seatud turvaseme ja need sisaldavad turvavõimekusi, mille toode ise annab.[Dokument](#)

Mille järgi seda näeb: Nõuete loend või nõuete halduse tööriist, kus igal nõudel on kordumatu tunnus, iga kande allikas, näiteks oht, kliendileping või õiguslik kohustus, ja eesmärgiks seatud kurtatase. Väike ettevõtte kasutab selleks üht tabelit, kus on püsiv tunnuse veerg, mille külge tõendamine ja testimine hiljem haakuvad.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SR-4

Iga üksik turvanõue on sõnastatud nii, et see on üheselt mõistetav, vastuoludeta, testitav ja jälgitav kindla tootefunktsiooni või liidese ning see kannab teavet, mida on hiljem tõendamiseks vaja ilma lisaküsimusteta.

Mille järgi seda näeb: Väljavõtte nõuete loendist, mis näitab iga nõude juures mõõdetavat vastuvõtukriteeriumi ja puudutatud funktsiooni või liidest, koos nõude ja testijuhtumi seosega. Väike ettevõtte kontrollib seda kindla sõnastusmalliga ja kontrollküsimusega, kas nõude põhjal saab testijuhtumi kirjutada ilma järele küsimata.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SR-5 Turvanõuded vaadatakse üle enne nende kasutamist disainis ja teostuses, kaasates puudutatud osalised, näiteks arenduse, testimise, toote omaniku ja kus kasulik ka müügi või kliendi. Ülevaatus katab täielikkuse ohumudeli ja toote turvakonteksti suhtes, õigsuse ja testitavuse. Leiud registreeritakse ja neid jälgitakse kuni sulgemiseni.

Mille järgi seda näeb: Ülevaatus kirje koos kuupäeva, osalejate ja nende rollidega, nõuete ülevaadatud versiooniga, leidude loendiga koos vastutaja ja sulgemise seisuga ning kinnitusemärgiga. Väike ettevõtte teeb seda kahe inimese ülevaatusena arenduse ja testimise vahel, lühikese kirje ja kinnitusreaga nõuete loendis.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

7 Praktika 3: Turvaline disain (SD)

4

SD-1 Igal tootel on disainikirjeldus, mis kajastab arhitektuuri turvalisust puudutavaid aspekte: millised komponendid on olemas, kuidas nad omavahel suhtlevad, kus kulgevad usalduspiirid, millised välised liidesed on avatud ja milliste mehhanismidega varem määratletud turvanõuded disainis teostatakse.

Dokument

Mille järgi seda näeb: Arhitektuuridokument või disaini spetsifikatsioon, mis sisaldab skeemi komponentide, andmevoogude ja usalduspiiridega, lisaks seostetabel igast turvanõudest seda teostava disainielemendini. Väike tarnija saab hakkama ühe ajakohase skeemi ja kahe või kolme lehekülje selgitusega; oluline on, et see on hoidlas versioonihalduses ja seda ajakohastatakse iga arhitektuurimuudatuse korral.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

SD-2 Disaini analüüsitakse süstemaatiliselt ohtude suhtes. Analüüs nimetab ründaja eesmärgid, puudutatud usalduspiirid ja liidesed, neist tulenevad ohud koos hinnanguga ning disainis võetud vastumeetmed. Seda korratakse iga kord, kui arhitektuur või keskkond oluliselt muutub, ja tuvastatud ohtusid jälgitakse, kuni iga ohu kohta on otsus tehtud.

Dokument

Mille järgi seda näeb: Ohumudel iga toote või iga suurema väljalaske kohta, näiteks tabel veergudega oht, puudutatud liides, hinnang, vastumeetmed ja seis, koos modelleerimise koosoleku protokolliga, kus on osalejad ja kuupäev. Väike meeskond modelleerib pragmaatiliselt kahe kuni kolme tunni pikkuses töötoas arhitektuuriskeemi järgi ja kirjutab avatud punktid piletiteks, nii et jälgimise tõend tekib ilma lisatööta.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

SD-3 Disain järgib tõendatavalt tunnustatud turvalise disaini põhimõtteid, nende hulgas vähima õiguse põhimõte, minimaalne ründepind, mitmekihiline kaitse, turvalised vaikeseaded, tõrke korral turvaline käitumine ja võimalikult lihtsad ning kontrollitavad turvamehhanismid. Nende põhimõtete rakendamine on disainis nähtav ja põhjendatud.

Mille järgi seda näeb: Jaotis disainikirjelduses või majasisene disainijuhend, mis nimetab põhimõtteid, lisaks konkreetne tõend iga põhimõtte kohta tootes, näiteks teenuste õiguste maatriks, avatud portide loend koos põhjendusega, tarnimisel kehtivad vaikeseaded või dokumenteeritud veakäsitluse käitumine. Väike tarnija kasutab nende põhimõtete lühikest kontrollnimekirja disaini ülevaatuses püsiva punktina ja säilitab täidetud lehe koos disainiga.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

SD-4 Disaini vaatavad enne teostuse algust üle pädevad kolleegid. Ülevaatus katab täielikkuse turvanõuete suhtes, turvamehhanismide õigsuse ja tulemuslikkuse ning ohtude analüüsi tulemused. Osalevad piisava turvapädevusega inimesed, leiud registreeritakse ja neid jälgitakse kuni sulgemiseni.

Dokument

Mille järgi seda näeb: Ülevaatus kirje koos kuupäeva, ülevaadatava objekti ja selle versiooni, osalejate ja nende rollide, leidude loendi koos seisuga ning väljalaskeotsusega. Väike meeskond seob ülevaatus disainidokumentide muudatustaotlusega ja jätab leiud kommentaaridena koos sulgemismärgiga, mis tõendab jälgimist ilma lisatööriistadeta. Kui majasisest turvapädevust napib, on praktiline tee väline ülevaataja, keda kaasatakse tunnitasu alusel kriitiliste disainide jaoks.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

8 Praktika 4: Turvaline teostus (SI)

2

SI-1 Olemas on määratletud protsess tegeliku teostuse tõendamiseks turvalise disaini suhtes: ülevaatus kinnitab, et disainis ette nähtud kaitsemeetmed on koodis tõesti olemas ja tulemuslikud, et mitmekihiline kaitse säilib ja et teostuse käigus ei ole tekkinud uusi haavatavusi. Ülevaatus teevad sobiva pädevusega inimesed ning leitud kõrvalekalded registreeritakse ja neid jälgitakse kuni sulgemiseni.

Mille järgi seda näeb: Kirjalik kord teostuse ülevaatuses koos ülevaatus kirjetega iga komponendi või väljalaske kohta: ülevaadatud moodul, viide disainidokumendile, kuupäev, ülevaataja, leiud ja nende lahendamise seis. Sobiv tõend on näiteks muudatustaotluste ülevaatused kohustusliku turvalisuse kontrollnimekirjaga, staatilise koodianalüüsi tulemused koos iga tabamuse dokumenteeritud hinnanguga ja ülevaatuskoosolekute protokollid. Väike meeskond katab selle nelja silma põhimõttega, hoidlas hoitava ülevaatusmalliga, kus iga disainimeede saab eraldi linnukese, ja ühe piletiga iga avatud leiu kohta. Oluline on, et koodi autor ei ole kunagi sama koodi ülevaataja.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SI-2 Kogu turvalisust puudutava arendustöö kohta kehtivad siduvad turvalise programmeerimise reeglid, mis katavad vähemalt teadaolevate ebaturvaliste konstruktsioonide ja funktsioonide vältimise, sisendite ja vigade käsitlemise, mälu ja ressursside halduse ning kontrollitud turvakoodi kasutamise ise kirjutatud teostuste asemel. Reeglid kehtivad iga kasutatava programmeerimiskeele kohta, on kõigile arendajatele teada ja neid ajakohastatakse vajaduse korral, näiteks uute ründemustrite või uute tööriistade ilmunisel.

Dokument

Mille järgi seda näeb: Kinnitatud turvalise programmeerimise standard koos versiooniseisu, keelepõhise käsitusala ja kinnitamise kuupäevaga, täiendatuna tõenditega, et see mõjub igapäevatöös: koodikontrolli ja analüüsi tööriistade seadistus hoidlas, koostereegel, mis toob rikkumised nähtavale, ja teavituskoooleku osalejate loend. Väikesed ettevõtted ei kirjuta standardit nullist; nad kuulutavad siduvaks mõne väljakujunenud avaliku reeglustiku, lisavad lühikese loendi oma täiendavatest reeglitest ja kinnistavad kontrolli koostetorusse, nii et reeglite järgimine tõendatakse automaatselt.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

9 Praktika 5: Turvalisuse tõendamise ja valideerimise testimine (SVV)

5

SVV-1 Igale turvalisust puudutavale tootenõudele on määratud vähemalt üks testijuhtum, mis näitab, et kaitsefunktsioon töötab tavatöös ettenähtud viisil, et see käitub spetsifikatsiooni kohaselt vigase sisendi või väärkasutuse korral ja et tootega kaasa antavad vaikeseaded vastavad turvalisele seisundile. Iga testitud tarkvaraversiooni kohta registreeritakse läbiviimine ja tulemus.

Dokument

Mille järgi seda näeb: Jälgitavuse maatriks, mis seob nõude testijuhtumi ja tulemusega, lisaks testikirjed, kus on kuupäev, testitav versioon või kooste ning testi tegija nimi. Väike tarnija lisab oma nõuete loendisse lihtsalt testijuhtumi tunnuse veeru ja arhiveerib koostetoru automaatselt testikäivituse väljundlogi failina vastava versiooni juurde.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SVV-2 Ohumudelitest tuletatud vastumeetmeid testitakse sihipäraselt, et kinnitada, et need tegelikult sulgevad eeldatud ründetee. Testitakse tuvastatud ohtude vastu, mitte üksnes korrapärase kasutuse suhtes ja avatud punktid suunatakse vigade käsitlemise protsessi.

Mille järgi seda näeb: Testijuhtumid, mis viitavad otse ohumudeli kannetele, näiteks üks väärkasutuse juhtum iga ohu tunnuse kohta koos oodatava kaitsekäitumisega, koos nende käivituste kirjetega. Ilma raske masinavärgita piisab ohumudelile veeru lisamisest, mis viitab testijuhtumile ja viimase eduka kontrolli kuupäevale.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SVV-3

Toodet uuritakse enne väljalaset süstemaatilisel haavatavuste suhtes. Käsitlusala katab vähemalt: väljastpoolt kättesaadavate liidest ja teenuste uurimise, testimise vigase ja juhuslikult muudetud sisendiga, kasutatud kolmanda osapoole komponentide võrdlemise teadaolevate teatatud haavatavustega ning tarnija enda koodis teadaolevate nõrkuseklasside kontrolli. Leiud registreeritakse koos hinnanguga.

[Dokument](#)

Mille järgi seda näeb: Kasutatud tööriistade aruanded, kus on tööriista nimi, versioon ja haavatavuste andmebaasi andmeseis, hāgustestimise kirjed, kolmanda osapoole komponentide loend koos viimase võrdluse kuupäevaga ning leidude loend koos hinnangu ja otsusega. Väike tarnija ühendab tasuta standardtööriistad, sõltuvuste skaneerimise ning portide ja teenuste skaneerimise paigaldatud toote vastu ja koondab väljundid iga väljalaske kohta ühte kausta.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SVV-4

Väljalaskekandidaat läbib realistlikes tingimustes ründekatse, mis pūūab aktiivselt kaitsemehhanismidest mööda minna, mitte üksnes neid pärida. Testi käsitlusala, ääritingimused ja piirid lepatakse eelnevalt kokku ning leitud nõrkusi käsitletakse ja jälgitakse nagu vigu.

Mille järgi seda näeb: Tellimus või testikorraldus, kus on käsitlusala ja testkeskkond, aruanne, mis katab lähenemise, ārakasutatud nõrkused ja nende hinnangu, lisaks kanded vigade ja pileтите süsteemis koos tõendiga kõrvaldamise või põhjendatud riski aktsepteerimise kohta. Väikesed tarnijad ostavad selle testi tavaliselt väljast piiratud ajamahunā või lasevad selle teha inimesel, kes toodet ei arendanud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SVV-5

Testijate sõltumatus on määratletud ja vastab kavandatud küpsustasemele. Kes komponendi arendas, ei anna seda välja üksnes oma testimise põhjal ja küpsustaseme tõustes vastutab testimise eest organisatsiooniliselt eraldi üksus või väline osapool. Tegelik jaotus on iga testi puhul jälgitav.

Mille järgi seda näeb: Rollide määratlus arendusprotsessis, mis näitab loomise ja testimise lahusust, lisaks iga testikäivituse või testiaruande juures registreeritud testi tegija nimi ja roll. Kahe inimesega ettevõtte lahendab selle vastastikuse ülevaatusega koos dokumenteeritud nelja silma märkega ja kaasab süvitsi mineva turvatestimise jaoks välise inimese.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

10 Praktika 6: Turvavigade haldus (DM)

6

DM-1

Olemas on määratletud kanal, mille kaudu võetakse vastu ja registreeritakse teated toote turvanõrkustest igast suunast: arendusmeeskonnalt endalt, testimisest ja ülevaatustest, klientidelt ja integreerijatelt, välistelt teatajatelt ning kasutatavate kolmanda osapoole ja avatud lähtekoodiga komponentide turvateadetest. Teatamiskanal on välistele osapooltele leitav ja iga teade registreeritakse koos saabumise kuupäeva ja allikaga.

[Dokument](#)

Mille järgi seda näeb: Teatamiskanalī kirjeldus, avalikult kättesaadav kontaktpunkt (turvalisuse leht, security.txt fail või postkast nagu security@) ja vastuvõturegister, kus on iga teate kohta kuupäev, allikas ja lühikirjeldus. Väike ettevõtte saab hakkama ühise postkasti ja ühe tabeli või piletisildiga, kui iga teade jõuab sinna, sealhulgas need, mis tõstatatakse sisemises arendajate vestluses.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

DM-2

Iga saabuv teade sorteeritakse ja uuritakse, et selgitada, kas see puudutab turvalisust ja milliseid tooteid, versioone ja komponente see mõjutab. Ka teated, mis osutuvad turvalisust mittepuudutavaks või mittekohalduvaks, suletakse põhjust nimetades, mitte vaikides kõrvale heites.

Mille järgi seda näeb: Iga teate kohta sortimismärke, kus on tulemus (turvalisust puudutav jah või ei), puudutatud versioonid ja vajaduse korral tagasilükkamise põhjus, nähtav piletil või vastuvõtuloendis. Väikese teatemahuga meeskonnad teevad sortimise lühikesel korduval koosolekul ja kirjutavad tulemuse kahe lausega iga kande kohta.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

DM-3

Kinnitatud turvavigu hinnatakse ühtse meetodiga: algpõhjus, puudutatud versioonid ja konfiguratsioonid, võimalik mõju talitlusele ja turvalisusele, ära kasutatavus ning raskusaste kindlaksmääratud skaalal. Hindamise tulemus registreeritakse ja on jälgitav.

[Dokument](#)

Mille järgi seda näeb: Hindamise kirje või piletiväljade kogum iga vea kohta, mis katab algpõhjust, raskusastme ja rakendatud skaala (näiteks levinud hindamissüsteem koos dokumenteeritud vektoriga), koos puudutatud versioonide loendiga. Väikesed meeskonnad tuginevad piletisüsteemi kindlale väljamallile ja pooleleheküljelisele kirjeldusele skaalast ning lävenditest, mis käivitavad kohese tegutsemise.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

DM-4

Iga hinnatud turvavea kohta tehakse otsus, kuidas seda käsitletakse: kõrvaldamine, kompenseeriv meede või põhjendatud riski aktsepteerimine. Otsus lähtub raskusastmest, sellele määratakse vastutav isik ja tähtaeg ning viga jälgitakse kuni sulgemiseni.

[Dokument](#)

Mille järgi seda näeb: Tegevusloend või pileтите seis, kus on vastutaja, sihtkuupäev, meetme liik ja sulgemismärge, seotud koodi lähtetasemega või väljalaskega, milles parandus jõustub. Aktsepteeritud jääkriskidel on lühike kirjalik põhjendus, mille kinnitab toote omanik. Väike ettevõtte hoiab seda piletitahvilil koos tähtaegadega, ilma lisatööriistadeta.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

DM-5

Puudutatud kasutajaid, integreerijaid ja teisi huvipooli teavitatakse turvavigadest niipea, kui hinnang seda nõuab, nimetades puudutatud versioonid, mõju ning olemasoleva paranduse või kompenseeriva meetme. Sellise avalikustamise tähtajad ja saajate ring on eelnevalt määratletud, samuti lähenemine kolmandate osapoolte teadetele, millel on oma avalikustamistähtaeg.

Mille järgi seda näeb: Avaldatud turvateated koos kuupäeva ja versiooniviitega, jaotusloend või tellijate kanal ning kirjalik reegel tähtaegade ja kooskõlastatud avalikustamise kohta. Väheste klientidega tarnijad kasutavad üht kirjasaadetist ajakohase kliendiloendi põhjal ja kuupäevastatud turvateadete lehte, mille muudatused on versioonitud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

DM-6

Turvavigade käsitlemine vaadatakse üle kindlaksmääratud sagedusega. Ülevaatus vaatleb avatud ja tähtaja ületanud juhtumeid, teatest kõrvaldamiseni kuluvat aega, korduvaid algpõhjusteid ja võetud meetmete tulemuslikkust. Ülevaatusel tulenevad protsessi parendused viiakse ellu ja nende elluviimist jälgitakse.

[Dokument](#)

Mille järgi seda näeb: Korduva ülevaatus protokoll koos kuupäeva, osalejate, avatud ja tähtaja ületanud juhtumite arvudega ning kokkulepitud parenduste loendiga koos vastutaja ja tähtajaga. Väike ettevõtte lisab selle punkti olemasolevale kvartalikoosolekule ja hoiab arvud ning otsused ühel leheküljel.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

11 Praktika 7: Turvavärskenduste haldus (SUM)

5

SUM-1

Iga toote turvavärskendus tõendatakse toetatud tooteversioonide ja töökeskkondade suhtes enne klientidele väljastamist ja olemas on kirje, mis näitab, et värskendus sulgeb haavatavuse ilma toote ettenähtud talitlust häirimata.

[Dokument](#)

Mille järgi seda näeb: Testikirje iga paiga kohta, mis katab testitud tooteversiooni, platvormi, testijuhtumid (tulemuslikkus haavatavuse vastu ja põhifunktsioonide regressioon) ja väljalaske kinnituse. Väike tarnija saab hakkama lühikese paiga kinnitamise kandega piletil: pileti tunnus, tõendaja, tõendamise kuupäev, tulemus, koos automaatse testikäivituse logiga.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SUM-2

Kõigi toote komponentide kohta, mida ei arendatud majasiseselt (kolmanda osapoole teegid, operatsioonisüsteem, käituskeskkonnad), on määratletud ja tõendatud, kuidas nende turvavärskendusi hinnatakse ja kas need võetakse tootesse üle või lükatakse tagasi koos dokumenteeritud põhjendusega.

[Dokument](#)

Mille järgi seda näeb: Kolmanda osapoole komponentide loetelu koos versiooni ja allikaga, lisaks üks hindamise kanne iga teatatud kolmanda osapoole haavatavuse kohta, kus on otsus (võetakse üle, ei puuduta, kaetud kompenseeriva meetmega) ja põhjendus. Väikesed meeskonnad käivitavad koostes automaatse sõltuvuste skaneerimise ja hoiavad otsuseid skaneerimise tulemuse kommentaaridena või lühikeses erandite loendis.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SUM-3

Iga väljastatava turvavärskendusega saavad kasutajad arusaadava saateteabe: millised tooteversioonid on puudutatud, milline haavatavus on parandatud, kui raske see on, kas kõrvalmõjude või kompenseerivate meetmetega on vaja arvestada ja kuidas värskendus paigaldatakse.

[Dokument](#)

Mille järgi seda näeb: Avaldatud turvateated või väljalaskemärkmed, kus on haavatavuse tunnus, puudutatud versioonid, raskusastme hinnang, paigaldamise sammud ja juhis eelmisses seisus tagasipöördumiseks. Väikesed tarnijad hoiavad üht avalikku lehte turvateadete ajalise loendiga ja viitavad sellele tootest endast.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SUM-4

Olemas on määratletud ja võltsimise eest kaitstud tee, mille kaudu kasutajad saavad turvavärskendusi, ja värskenduse ehtsust ning terviklust saab kasutaja poolel kontrollida enne paigaldamist.

Mille järgi seda näeb: Tarnekanali kirjeldus (allalaadimisala, värskendusserver, füüsiline andmekandja) koos selle kaitsemeetmetega, lisaks digitaalallkiri või kontrollsumma iga paketi kohta ja juhis kasutajale, kuidas seda kontrollida. Väikesed tarnijad saavutavad selle koosteserveril allkirjastamisega, kontrollsumma avaldamisega allalaadimise kõrval ja ühe selge koha nimetamisega, kus avalikku võtit hoitakse.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SUM-5

Turvavärskenduste kättesaadavaks tegemiseks on määratletud ajasihid, mis on astmestatud haavatavuse raskusastme järgi; tegelikult saavutatud aegu jälgitakse ning iga ületatud tähtaeg põhjendatakse ja kaetakse kasutajatele mõeldud vahemeetmega.

[Dokument](#)

Mille järgi seda näeb: Sisemine spetsifikatsioon ajaaknaga iga raskusastme kategooria kohta (näiteks kriitiline ≤ 30 päeva, kõrge ≤ 90 päeva) ja hinnang iga haavatavuse kohta: teate kuupäev, paiga väljalaske kuupäev, möödunud päevad, kõrvalekalde põhjus. Väikesed tarnijad hoiavad seda kahe kuupäevaväljana haavatavuse piletil ja vaatavad loendi kord kvartalis üle, selle asemel et seada üles eraldi mõõdukusüsteem.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

12 Praktika 8: Turvajuhised toote kasutuselevõtuks ja käitamiseks (SG)

7

SG-1

Iga tootega on kaasas selle mitmekihilise kaitse strateegia kirjeldus: see nimetab tootesse endasse ehitatud kaitsekihid, seob need ohtudega, mille vastu nad toimivad, ja näitab, milline kaitsetoime tekib alles mitme kihi koostoimes.

[Dokument](#)

Mille järgi seda näeb: Jaotis tarnitavas tootedokumentatsioonis või eraldi turvakontseptsioonis, kus on iga kaitsekihi kohta mehhanism, kaetud oht ja toime piirid. Väike ettevõtte hoiab seda kaheleheküljelise tabelina: veerg kaitsekiht, veerg oht oma ohumudelist, veerg jääkrisk. Piisab ristviitest SR-2 ohumudelile, sisu ei ole vaja kaks korda hallata.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SG-2

Dokument

Dokumentatsioon nimetab turvameetmed, mida toode ise ei anna, vaid eeldab kasutuskeskkonnalt, näiteks võrgu segmentimine, eesasetsevad tulemüürid, füüsiline pääsu ohjamine või väline ajateenus, ja teeb selgeks, et ilma nende meetmeteta tagatud turvataset ei saavutata.

Mille järgi seda näeb: Kasutuselevõtu eeltingimuste peatükk käsiraamatus või võrdlusarhitektuuri joonis tsoonide ja ühendusteedega, kus vara omaniku tagatavad meetmed on selgelt märgitud. Praktikas on kasulikuks osutunud keskkonda puudutavate eelduste loend, mis on tuletatud otse toote turvakontekstist ja mis loetakse iga tooteversiooni juures uuesti läbi.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SG-3

Dokument

Olemas on turvalise lähtekonfiguratsiooni juhend, mis loetleb kõik turvalisust puudutavad seaded, teenused, pordid ja liidesed, esitab soovitatava tarneseisundi ja kirjeldab soovitusel kõrvalekaldumise mõju.

Mille järgi seda näeb: Turvakarastuse juhend koos seadete tabeliga: parameeter, soovitatav väärtus, toime, kõrvalmõju kõrvalekaldumisel. Lisaks vaikekonfiguratsioonis aktiivsete teenuste ja portide loend koos põhjendusega, miks need lubatuks jäävad. Väike meeskond hoiab seda tabelit hoidlas otse konfiguratsioonifaili kõrval ja ekspordib selle tarnedokumentatsiooni, nii et see püsib tootega kooskõlas.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SG-4

Dokument

Jooksva käitamise jaoks on olemas juhend, mis kirjeldab, kuidas toodet turvaliselt käitatakse, seiratakse ja hoitakse turvalises seisundis, sealhulgas varukoopia ja taastamine, logimine ning turvalisust puudutavate sündmusteade te käsitlemine.

Mille järgi seda näeb: Käitusjuhend jaotistega logimise, varukoopiate, taaskäivituse ja sündmusteade kohta. Täiendava tõendina loend turvalisust puudutavatest teadetest, mida toode väljastab, igaühe juures lühike soovitatav tegevus, nii et vara omanik ei tõlgenda neid üksi.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SG-5

Dokument

Dokumentatsioon selgitab, kuidas toote kasutajakontosid, rolle ja õigusi seadistatakse ja hoitakse ajakohasena, eelkõige rollide lahusust, vaiketunnuste muutmist ja mittevajalike kontode eemaldamist.

Mille järgi seda näeb: Kontohalduse peatükk koos rollide ülevaate ja igale rollile määratud õigustega, lisaks selge märkus vaiketunnuste ja nende muutmise kohta kasutuselevõtul. Praktikas toimib hästi lühike kasutuselevõtu kontrollnimekiri käsiraamatus, mille vara omanik saab läbi linnutada ja säilitada.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SG-6

Dokument

Olemas on turvalise kasutuselt kõrvaldamise juhend, mis kirjeldab tundlike andmete täielikku eemaldamist tootest, näiteks tunnused, võtmed, konfiguratsiooniandmed ja logid, enne seadme edasiandmist, taaskasutust või utiliseerimist.

Mille järgi seda näeb: Kasutuselt kõrvaldamise jaotis, kus on loetletud iga tundlike andmete salvestuskoht tootes ja vastav kustutamise kord, sealhulgas juhud, kus kustutamine on tehniliselt võimatu ja riistvara hävitatakse füüsiliselt. Siin aitab arhitektuurikirjeldusest võetud püsimalude loend, see hoiab ära salvestuskoha unustamise.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

SG-7

Kasutajatele tarnitav turvadokumentatsioon vaadatakse enne väljalaset üle: see on tehniliselt õige, kooskõlas tarnitava tooteversiooniga, kavandatud sisu suhtes täielik ja sihtrühmale arusaadav, ning seda ajakohastatakse iga toote muudatuse korral.

Mille järgi seda näeb: Ülevaate kirje iga dokumendi ja tooteversiooni kohta koos ülevaataja, kuupäeva, leidude ja nende sulgemisega, seotud väljalaske kinnitusega. Väike ettevõtte lahendab selle nelja silma põhimõttega dokumentatsiooni muudatustaotluses: üks arendaja kontrollib tehnilist sisu, teine inimene arusaadavust, ja kinnitus registreeritakse piletil. Versioon on tarnitav alles siis, kui ülevaatus on dokumenteeritud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus