IEC 62443-4-1:2018 Saugaus produkto kūrimo būvio ciklas pramoninėje automatikoje

Saugaus kūrimo būvio ciklas, aštuonios praktikos

47 reikalavimai. Pagal šį standartą galima sertifikuotis akredituotoje sertifikavimo įstaigoje. Redakcija 07/2026.

Pagal IEC 62443-4-1 galima sertifikuotis, tačiau sertifikavimo objektas yra neįprastas: sertifikuojamas įvardytos kūrimo organizacijos kūrimo procesas, tai yra viena konkreti dokumentuota saugaus būvio ciklo versija. Nesertifikuojamas nei produktas, nei asmuo. Galimi keliai yra ISASecure SDLA ir IECEE CB Scheme. Pagal šiandienos padėtį toks sertifikatas nesukuria atitikties prezumpcijos pagal EU Cyber Resilience Act. Jo nedera painioti su IEC 62443-4-2, kuris kelia reikalavimus pačiam komponentui. Šis sąrašas yra darbo priemonė įsivertinimui, o ne įrodymas.

Įmonė	Data	Pildė

5 1 praktika: Saugumo valdymas (SM) 13

SM-1 **Yra nustatytas produkto kūrimo būvio ciklas, kuris saugumą perneša per kiekvieną etapą nuo pradinės koncepcijos iki produkto eksploatacijos nutraukimo, ir būtent šio ciklo iš tikrųjų laikomasi kasdieniame darbe.** Dokumentas

Iš ko tai galima atpažinti: Proceso aprašas arba darbo instrukcija, kurioje išvardyti etapai, kiekvieno etapo rezultatai ir perdavimo taškai, kartu su vykdomo projekto įrodymu, rodančiu, kad etapai iš tikrųjų buvo pereiti. Maža įmonė apsieina su vienu puslapiu kiekvienam etapui ir kontroliniu sąrašu užduočių sistemoje; svarbiausia, kad dokumentuotas procesas ir kasdienė praktika sutaptų.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SM-2 **Kiekviena saugaus kūrimo būvio ciklo užduotis turi paskirtą atsakingąjį, ir šis paskyrimas yra žinomas dalyvaujantiems žmonėms.** Dokumentas

Iš ko tai galima atpažinti: Vaidmenų ir atsakomybių matrica, kurioje kiekvienas proceso žingsnis susietas su įvardytu vaidmeniu, papildyta esamu tų vaidmenų užėmimu. Kai žmonių yra tik keletas, pakanka lentelės su vaidmeniu, užduotimi ir asmeniu; svarbiausia yra pavadavimo tvarka atostogų ir ligos atvejais.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SM-3 **Atsekamai nustatyta, kurie produktai, variantai, laidos ir komponentai patenka į saugaus kūrimo būvio ciklą, o kurie ne.** Dokumentas

Iš ko tai galima atpažinti: Į taikymo sritį patenkančių produktų ir versijų būsenų sąrašas su įtraukimo ir neįtraukimo pagrindimu, atnaujinamas su kiekviena nauja laida. Praktikoje gerai veikia stulpelis produktų apžvalgoje, kuriame kiekvienoje eilutėje yra taip arba ne ir vienas pagrindimo sakinys.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SM-4 **Žmonės, kurie imasi saugumo užduočių, turi joms reikalingą dalykinę kompetenciją, ir ši kompetencija yra sąmoningai ugdoma bei atnaujinama.**

Iš ko tai galima atpažinti: Kiekvieno saugumo vaidmens kompetencijos profilis, kvalifikacijos įrašai, mokymo planas ir dalyvavimo įrašai, papildyti spragų apžvalga. Mažos įmonės tai įrodo pažymėjimais, dalyvavimu konferencijose ar internetiniuose seminaruose ir trumpa metine peržiūra, kas kurią spragą iki kada uždaro, o kur reikia, perka išorinę kompetenciją.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SM-5 **Saugaus kūrimo būvio ciklo taikymo sritis yra apibrėžta ir įvardija dalyvaujančias vietas, organizacinius padalinius, tiekėjų indėlį ir kūrimo aplinkas kartu su tos srities ribomis.** Dokumentas

Iš ko tai galima atpažinti: Taikymo srities aprašas, apimantis vietas, komandas, perduotas vykdyti dalis ir sistemas, kartu su išorinių sąsajų eskizu. Kas kuria vienoje vietoje, tai užrašo keliais sakiniais ir aiškiai įvardija, kas lieka už ribų, pavyzdžiui, išorėje sukurti mazgai arba trečiosios šalies prieglobos paslauga.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SM-6 **Kiekvienam naudotojams perduodamam elementui, programinei įrangai, programinei aparatinei įrangai, konfigūracijoms ir lydimiesiems failams, yra galima vientisumo patikra, kad gavėjai galėtų atpažinti nepastebėtą pakeitimą.**

Iš ko tai galima atpažinti: Kiekvieno pristatymo paketo parašai arba paskelbtos kontrolinės sumos, metodo aprašas ir vienas pavyzdys iš tikros laidos kartu su nurodymais klientui, kaip atlikti patikrą. Mažoms komandoms pakanka pasirašyto kontrolinių sumų failo šalia atsisiuntimo ir vienos pastraipos laidos aprašyme.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SM-7 **Kūrimo, kompiliavimo ir testavimo aplinkos yra apsaugotos nuo neteisėtos prieigos ir nuo pirminio kodo, kompiliavimo įrankių bei artefaktų klastojimo.**

Iš ko tai galima atpažinti: Saugyklos, kompiliavimo serverio ir testavimo sistemų prieigos valdymo koncepcija, prieigų sąrašai su paskutinės peržiūros data, su saugumu susijusių pakeitimų įrašai ir įrodymas, kad gamybinė ir kūrimo prieigos yra atskirtos. Neturint savo informacinių technologijų padalinio, pakanka dviejų veiksnių prisijungimo, apsaugotos pagrindinės šakos su būtina peržiūra ir kas pusmetį atliekamos peržiūros, kas dar turi prieigą.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SM-8 **Privatieji raktai, kuriais pasirašomi pristatymai, yra apsaugoti nuo atskleidimo ir netinkamo naudojimo, o jų naudojimas leidžiamas tik įgaliotiems žmonėms ir sistemoms.**

Iš ko tai galima atpažinti: Rakto saugojimo, prieigos, atnaujinimo ir atšaukimo aprašas, apsaugoto saugojimo įrodymas, pavyzdžiui, aparatinė raktų laikmena arba raktų valdymo paslauga, ir pasirašymo veiksmų įrašai. Maža įmonė laiko pasirašymo raktą aparatinėje raktų laikmenoje, dokumentuoja du prieigą turinčius žmones ir turi parengtą procedūrą praradimo atvejui.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SM-9 **Perkamiems arba perimamiems komponentams, įskaitant atvirojo kodo programinę įrangą, tiekėjui keliami saugumo lūkesčiai yra nustatyti ir taikomi atrenkant.** Dokumentas

Iš ko tai galima atpažinti: Saugumo reikalavimai tiekėjų specifikacijose arba sutartyse, trečiųjų šalių komponentų atrankos kriterijai, visų trečiųjų šalių komponentų sąrašas su versija ir šaltiniu bei vertinimas, ar tiekėjas atitinka lūkesčius. Neturint pirkimų padalinio, pakanka palaikomo komponentų sąrašo su stulpeliu, kuriame žymima, ar buvo patikrinti tiekėjo saugumo atnaujinimai ir pranešimo kanalai.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SM-10 **Trečiosios šalies pagal užsakymą sukurtiems komponentams taikomi tie patys saugumo reikalavimai kaip ir savam kūrimui, o jų laikymasis yra tikrinamas.**

Iš ko tai galima atpažinti: Užsakymas arba sutarties dokumentai, kuriuose nurodyti reikalaujami saugumo įsipareigojimai, paslaugų teikėjo įrodymai apie taikomas praktikas, priėmimo įrašai ir savų pateikto darbo patikrų rezultatai. Neturint audito biudžeto, pakanka sutartinio patikinimo, teikėjo testavimo rezultatų pateikimo ir vienos savos atrankinės patikros prieš priėmimą.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SM-11 **Su saugumu susiję pastebėjimai iš visų šaltinių, testų, peržiūrų, naudotojų pranešimų ir trečiųjų šalių informacijos, yra registruojami, vertinami pagal poveikį, jiems paskiriamas atsakingas asmuo ir terminas, o jie sekami iki uždarymo.** Dokumentas

Iš ko tai galima atpažinti: Defektų arba užduočių sistema su atskira saugumo temų žyma, o kiekviename įraše poveikio vertinimas, atsakingas asmuo, terminas ir uždarymo pastaba, kartu su ataskaita apie neuždarytus punktus. Maža komanda naudoja žymą esamoje užduočių sistemoje ir nuolatinį darbotvarkės punktą savaitiniame susitikime.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SM-12 **Prieš išleidžiant produktą yra patikrinama ir įrodoma, kad numatyti saugaus kūrimo būvio ciklo žingsniai iš tikrųjų buvo atlikti ir kad susiję įrašai buvo parengti.** Dokumentas

Iš ko tai galima atpažinti: Kiekvienos laidos peržiūra lyginant su proceso žingsniais, nuorodos į atitinkamus įrašus ir dokumentuotas išleidimo sprendimas su data ir parašu. Praktikoje gerai veikia laidos kontrolinis sąrašas, kuris neleidžia išsiųsti be visų varnelių; neuždaryti punktai pagrindžiami ir jiems nustatoma data.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SM-13 **Pats saugaus kūrimo būvio ciklas yra reguliariai kritiškai vertinamas ir gerinamas remiantis incidentų, testavimo rezultatų, klientų atsiliepimų ir grėsmių aplinkos įžvalgomis.**

Iš ko tai galima atpažinti: Proceso peržiūros įrašai, pavyzdžiui, vadovybinė vertinamoji analizė arba retrospektyva, su inicijuotais proceso pakeitimais, jų įgyvendinimo būsena ir nuoroda į pagrindinę priežastį. Kas naudoja standarto brandos lygius, užrašo esamą ir siekiamą būklę kiekvienai praktikai; 4 brandos lygis reikalauja būtent šio nuolatinio gerinimo įrodymo. Mažai įmonei pakanka vieno susitikimo per metus su protokolu ir trijų konkrečių patobulinimų.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

6 2 praktika: Saugumo reikalavimų specifikavimas (SR) 5

SR-1 **Numatytas produkto kontekstas yra aprašytas: tikėtina veikimo aplinka, saugumo priemonės, kurių tikimasi iš tos aplinkos, numatytos naudotojų grupės ir vaidmenys, prielaidos apie pasitikėjimo ribas ir naudojimo atvejai, kuriems produktas aiškiai nėra skirtas.** Dokumentas

Iš ko tai galima atpažinti: Produkto saugumo konteksto aprašas kaip atskiras dokumentas arba kaip pastovus produkto specifikacijos skyrius, apimantis tinklo aplinką, numanomas išorines apsaugas, pavyzdžiui, užkardą ar fizinės prieigos valdymą, vaidmenų sąrašą ir aiškų į taikymo sritį nepatenkančių naudojimo atvejų sąrašą. Maža įmonė apsiriboja dviem puslapiais, prideda paprastą gamyklos aplinkos eskizą, o produkto savininkas jį patvirtina ir nurodo datą.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR-2 **Produktui yra parengtas grėsmių modelis, kuris atvaizduoja duomenų srautus, sąsajas, pasitikėjimo ribas ir atakų kelius, įvardija iš jų kylančias grėsmes ir galimą jų poveikį bei priskiria atsakomąsias priemones. Jis peržiūrimas ir atnaujinamas įvykus reikšmingiems pakeitimams ir bent kartą kiekvienai produkto laidai, o neuždaryti punktai sekami, kol uždaromi.** Dokumentas

Iš ko tai galima atpažinti: Grėsmių modelis su duomenų srautų diagrama, kiekvienos sąsajos grėsmių sąrašu, priskirtomis atsakomosiomis priemonėmis ir neuždarytų punktų būsena, kartu su pakeitimų istorija, kurioje nurodyta data ir autorius. Maža įmonė gali dirbti su viena lentele kiekvienai sąsajai, kurios stulpeliai rodo, kas ten gali nutikti blogo, kiek tai būtų rimta, ką dėl to daroma ir kas tai peržiūri.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR-3 **Produkto saugumo reikalavimai yra nustatyti ir dokumentuoti. Jie apima grėsmių modelio rezultatus, aprašytą produkto saugumo kontekstą, taikomus teisinius ir sutartinius įsipareigojimus bei siekiamą saugumo lygį, taip pat saugumo galimybes, kurias užtikrina pats produktas.** Dokumentas

Iš ko tai galima atpažinti: Reikalavimų sąrašas arba reikalavimų valdymo įrankis su unikaliu kiekvieno reikalavimo identifikatoriumi, kiekvieno įrašo šaltiniu, pavyzdžiui, grėsme, kliento sutartimi ar teisiniu įsipareigojimu, ir siekiamu saugumo lygiu. Maža įmonė tai tvarko kaip vieną lentelę su pastoviu identifikatoriaus stulpeliu, prie kurio vėliau kabinasi verifikavimas ir testavimas.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR-4 **Kiekvienas atskiras saugumo reikalavimas suformuluotas taip, kad būtų vienareikšmis, be prieštaravimų, patikrinamas testais ir atsekamas iki konkrečios produkto funkcijos ar sąsajos, ir jame yra informacija, reikalinga vėliau jį verifikuoti be papildomų paaiškinimų.**

Iš ko tai galima atpažinti: Reikalavimų sąrašo pavyzdys, rodantis kiekvieno reikalavimo išmatuojamą priėmimo kriterijų ir susijusią funkciją ar sąsają, kartu su reikalavimų ir testavimo atvejų susiejimu. Maža įmonė tai tikrina pastoviu formuluotės šablonu ir kontroliniu klausimu, ar iš reikalavimo galima parašyti testavimo atvejį nieko papildomai neklausiant.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SR-5 **Saugumo reikalavimai yra peržiūrimi prieš juos naudojant projektuojant ir įgyvendinant, dalyvaujant susijusioms pusėms, tokioms kaip kūrimas, testavimas, produkto savininkas ir, kur naudinga, pardavimai arba klientas. Peržiūra apima išsamumą pagal grėsmių modelį ir produkto saugumo kontekstą, teisingumą ir patikrinamumą testais. Pastebėjimai registruojami ir sekami iki uždarymo.**

Iš ko tai galima atpažinti: Peržiūros įrašas su data, dalyviais ir jų vaidmenimis, peržiūrėta reikalavimų versija, pastebėjimų sąrašu su atsakingu asmeniu ir uždarymo būsena bei patvirtinimo pastaba. Maža įmonė tai atlieka kaip dviejų asmenų peržiūrą tarp kūrimo ir testavimo su trumpu įrašu ir patvirtinimo eilute reikalavimų sąraše.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

7 3 praktika: Saugumas jau projektuojant (SD) 4

SD-1 **Kiekvienas produktas turi projekto aprašą, kuriame užfiksuoti su saugumu susiję architektūros aspektai: kokie komponentai yra, kaip jie tarpusavyje susisiekia, kur eina pasitikėjimo ribos, kokios išorinės sąsajos yra atviros ir kokiais mechanizmais anksčiau nustatyti saugumo reikalavimai įgyvendinami projekte.** Dokumentas

Iš ko tai galima atpažinti: Architektūros dokumentas arba projekto specifikacija su diagrama, rodančia komponentus, duomenų srautus ir pasitikėjimo ribas, bei susiejimo lentele nuo kiekvieno saugumo reikalavimo iki jį įgyvendinančio projekto elemento. Mažas tiekėjas apsieina su viena palaikoma diagrama ir dviem trimis puslapiais paaiškinimo; svarbiausia, kad ji būtų saugykloje su versijų kontrole ir atnaujinama kaskart pasikeitus architektūrai.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SD-2 **Projektas yra sistemingai analizuojamas dėl grėsmių. Analizė įvardija užpuoliko tikslus, susijusias pasitikėjimo ribas ir sąsajas, iš jų kylančias grėsmes kartu su jų vertinimu ir projekte taikomas atsakomąsias priemones. Ji kartojama kaskart iš esmės pasikeitus architektūrai ar aplinkai, o nustatytos grėsmės sekamos, kol dėl kiekvienos jų priimamas sprendimas.** Dokumentas

Iš ko tai galima atpažinti: Grėsmių modelis kiekvienam produktui arba kiekvienai pagrindinei laidai, pavyzdžiui, lentelė su stulpeliais grėsmė, susijusi sąsaja, vertinimas, atsakomoji priemonė ir būsena, kartu su modeliavimo sesijos protokolu, kuriame nurodyti dalyviai ir data. Maža komanda modeliuoja pragmatiškai per dviejų ar trijų valandų dirbtuves pagal architektūros diagramą ir neuždarytus punktus registruoja kaip užduotis, todėl sekimo įrodymas atsiranda be papildomų pastangų.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SD-3 **Projektas įrodomai laikosi pripažintų saugaus projektavimo principų, tarp jų mažiausios privilegijos, mažiausio atakos paviršiaus, giliosios gynybos, saugių numatytųjų nuostatų, saugaus elgesio sutrikus veikimui bei kuo paprastesnių ir kuo lengviau patikrinamų saugumo mechanizmų. Šių principų taikymas matomas projekte ir yra pagrįstas.**

Iš ko tai galima atpažinti: Projekto aprašo skyrius arba vidinė projektavimo gairė, įvardijanti principus, ir konkretus kiekvieno principo įrodymas produkte, pavyzdžiui, paslaugų privilegijų matrica, atvirų prievadų sąrašas su pagrindimu, pristatomos numatytosios nuostatos arba dokumentuotas klaidų apdorojimo elgesys. Mažas tiekėjas naudoja trumpą šių principų kontrolinį sąrašą kaip pastovų projekto peržiūros punktą ir užpildytą lapą laiko kartu su projektu.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SD-4 **Projektą prieš prasidedant įgyvendinimui peržiūri kvalifikuoti kolegos. Peržiūra apima išsamumą pagal saugumo reikalavimus, saugumo mechanizmų teisingumą ir rezultatyvumą bei grėsmių analizės rezultatus. Dalyvauja žmonės, turintys pakankamą saugumo kompetenciją, pastebėjimai registruojami ir sekami iki uždarymo.** Dokumentas

Iš ko tai galima atpažinti: Peržiūros įrašas su data, peržiūrimu objektu ir jo versija, dalyviais ir jų vaidmenimis, pastebėjimų sąrašu su būsena ir išleidimo sprendimu. Maža komanda peržiūrą susieja su projekto dokumentų sujungimo prašymu ir pastebėjimus palieka kaip komentarus su uždarymo pastaba, taip sekimas įrodomas be jokių papildomų įrankių. Kur savo saugumo kompetencijos trūksta, pragmatiškas kelias yra išorinis peržiūrėtojas, samdomas valandiniu pagrindu kritiniams projektams.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

8 4 praktika: Saugus įgyvendinimas (SI) 2

SI-1 **Yra nustatytas procesas, kaip faktinis įgyvendinimas tikrinamas pagal saugų projektą: peržiūra patvirtina, kad projekte numatytos apsaugos priemonės kode iš tikrųjų yra ir veikia, kad gilioji gynyba išlaikoma ir kad įgyvendinant nebuvo įnešta naujų pažeidžiamumų. Peržiūrą atlieka tinkamai kvalifikuoti darbuotojai, o rasti nukrypimai registruojami ir sekami iki uždarymo.**

Iš ko tai galima atpažinti: Rašytinė įgyvendinimo peržiūros procedūra kartu su kiekvieno komponento ar laidos peržiūros įrašais: peržiūrėtas modulis, nuoroda į projekto dokumentą, data, peržiūrėtojas, pastebėjimai ir jų sprendimo būsena. Tinkami įrodymai yra sujungimo prašymų peržiūros su būtinu saugumo kontroliniu sąrašu, statinės kodo analizės rezultatai su dokumentuotu kiekvieno radinio vertinimu ir peržiūros sesijų protokolai. Maža komanda tai užtikrina keturių akių principu, saugykloje laikomu peržiūros šablonu, kuriame kiekviena projekto priemonė pažymima atskirai, ir viena užduotimi kiekvienam neuždarytam pastebėjimui. Svarbiausia, kad kodo autorius niekada nebūtų to paties kodo peržiūrėtojas.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SI-2 **Visam su saugumu susijusiam kūrimo darbui galioja įpareigojančios saugaus programavimo taisyklės, kurios apima bent žinomų nesaugių konstrukcijų ir funkcijų vengimą, įvesties ir klaidų tvarkymą, atminties bei išteklių valdymą ir patikrinto saugumo kodo naudojimą vietoj savo rašytų realizacijų. Taisyklės galioja kiekvienai naudojamai programavimo kalbai, yra žinomos visiems kūrėjams ir atnaujinamos, kai reikia, pavyzdžiui, atsiradus naujiems atakų būdams ar naujiems įrankiams.** Dokumentas

Iš ko tai galima atpažinti: Patvirtintas saugaus programavimo standartas su versijos būsena, taikymo sritimi kiekvienai kalbai ir patvirtinimo data, papildytas įrodymu, kad jis veikia kasdieniame darbe: kodo tikrintuvų ir analizės įrankių konfigūracija saugykloje, kompiliavimo taisyklė, kuri iškelia pažeidimus, ir instruktažo dalyvių sąrašas. Mažos įmonės nerašo standarto nuo nulio; jos paskelbia įpareigojančiu nusistovėjusį viešą taisyklių rinkinį, prideda trumpą savų papildomų taisyklių sąrašą ir įtvirtina patikrą kūrimo grandinėje, kad laikymasis būtų parodomas automatiškai.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

9 5 praktika: Saugumo verifikavimo ir validavimo testavimas (SVV) 5

SVV-1 **Kiekvienam su saugumu susijusiam produkto reikalavimui priskirtas bent vienas testavimo atvejis, rodantis, kad apsaugos funkcija įprastai veikiant veikia kaip numatyta, kad gavusi netinkamą įvestį ar naudojama netinkamai ji elgiasi kaip nurodyta ir kad su produktu pateikiamos numatytosios nuostatos atitinka saugią būseną. Vykdymas ir rezultatas registruojami kiekvienai testuotai programinės įrangos versijai.** Dokumentas

Iš ko tai galima atpažinti: Atsekamumo matrica, siejanti reikalavimą su testavimo atveju ir rezultatu, bei testavimo įrašai su data, testuojama versija arba kompiliacija ir testą atlikusio asmens vardu. Mažas tiekėjas tiesiog prideda testavimo atvejo identifikatoriaus stulpelį prie savo reikalavimų sąrašo, o automatinio testavimo iš kūrimo grandinės išvesties žurnalą archyvuoja kaip failą prie atitinkamos versijos.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SVV-2 **Iš grėsmių modelio kylančios atsakomosios priemonės testuojamos tikslingai, siekiant patvirtinti, kad jos iš tikrųjų uždaro numatytą atakos kelią. Testuojama pagal nustatytas grėsmes, o ne tik pagal tvarkingą naudojimą, ir neuždaryti punktai perduodami į defektų tvarkymo procesą.**

Iš ko tai galima atpažinti: Testavimo atvejai, tiesiogiai nurodantys grėsmių modelio įrašus, pavyzdžiui, vienas piktnaudžiavimo atvejis kiekvienam grėsmės identifikatoriui su laukiamu gynybiniu elgesiu, kartu su tų vykdymų įrašais. Be sudėtingų priemonių pakanka grėsmių modelyje pridėti stulpelį su nuoroda į testavimo atvejį ir paskutinės sėkmingos patikros data.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SVV-3 **Prieš išleidimą produktas sistemingai tiriamas dėl pažeidžiamumų. Į apimtį patenka bent: iš išorės pasiekiamų sąsajų ir paslaugų tyrimas, testavimas netaisyklinga ir atsitiktinai keičiama įvestimi, naudojamų trečiųjų šalių komponentų palyginimas su žinomais paskelbtais pažeidžiamumais ir savo kodo patikra dėl žinomų silpnybių klasių. Pastebėjimai registruojami kartu su jų vertinimu.** Dokumentas

Iš ko tai galima atpažinti: Naudotų įrankių ataskaitos su įrankio pavadinimu, versija ir pažeidžiamumų duomenų bazės duomenų atnaujinimo data, atsitiktinės įvesties testavimo įrašai, trečiųjų šalių komponentų sąrašas su paskutinio palyginimo data ir pastebėjimų sąrašas su vertinimu bei sprendimu. Mažas tiekėjas derina nemokamus standartinius įrankius, priklausomybių patikrą ir įdiegto produkto prievadų bei paslaugų patikrą, o kiekvienos laidos išvestis laiko viename aplanke.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SVV-4 **Laidos kandidatas realiomis sąlygomis patiria atakos bandymą, kuris aktyviai siekia apeiti apsaugos mechanizmus, o ne tik juos užklausti. Testo apimtis, kraštinės sąlygos ir ribos sutariamos iš anksto, o rastos silpnybės tvarkomos ir sekamos kaip defektai.**

Iš ko tai galima atpažinti: Užsakymas arba testavimo pavedimas su apimtimi ir testavimo aplinka, ataskaita apie taikytą metodą, išnaudotas silpnybes ir jų vertinimą, bei įrašai defektų arba užduočių sistemoje su ištaisymo arba pagrįsto rizikos prisiėmimo įrodymu. Maži tiekėjai šį testą paprastai perka išorėje kaip ribotą laiko biudžetą arba paveda jį atlikti asmeniui, kuris produkto nekūrė.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SVV-5 **Testuojančių darbuotojų nepriklausomumas yra nustatytas ir atitinka siekiamą brandos lygį. Kas komponentą sukūrė, neišleidžia jo remdamasis vien savo paties testavimu, o kylant brandos lygiui už testavimą atsako organizaciškai atskiras padalinys arba išorės šalis. Faktinis paskyrimas yra atsekamas kiekvienam testui.**

Iš ko tai galima atpažinti: Vaidmenų apibrėžimas kūrimo procese, rodantis kūrimo ir testavimo atskyrimą, ir kiekvienam testavimo vykdymui ar testavimo ataskaitai užrašytas testą atlikusio asmens vardas bei vaidmuo. Dviejų asmenų įmonė tai sprendžia abipuse peržiūra su dokumentuota keturių akių pastaba, o giluminiam saugumo testavimui pasitelkia išorės asmenį.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

10 6 praktika: Saugumo defektų valdymas (DM) 6

DM-1 **Yra nustatytas kanalas, kuriuo iš visų pusių priimami ir registruojami pranešimai apie produkto saugumo silpnybes: iš pačios kūrimo komandos, iš testavimo ir peržiūrų, iš klientų ir integruotojų, iš išorės pranešėjų ir iš įspėjimų apie naudojamus trečiųjų šalių bei atvirojo kodo komponentus. Pranešimo kanalą išorės šalys gali rasti, o kiekvienas pranešimas registruojamas su gavimo data ir šaltiniu.** Dokumentas

Iš ko tai galima atpažinti: Pranešimo kanalo aprašas, viešai pasiekiamas kontaktinis taškas (saugumo puslapis, security.txt failas arba pašto dėžutė, tokia kaip security@), ir priėmimo registras, kuriame kiekvienam pranešimui nurodyta data, šaltinis ir trumpas aprašymas. Maža įmonė gali dirbti su bendra pašto dėžute ir viena skaičiuokle ar užduočių žyma, jei tik ten patenka kiekvienas pranešimas, įskaitant tuos, kurie iškyla vidiniame kūrėjų pokalbyje.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

DM-2 **Kiekvienas gaunamas pranešimas yra rūšiuojamas ir tiriamas siekiant nustatyti, ar jis susijęs su saugumu ir kuriems produktams, versijoms bei komponentams daro poveikį. Pranešimai, kurie pasirodo esą nesusiję su saugumu arba netaikytini, taip pat uždaromi nurodant priežastį, o ne tyliai atmetami.**

Iš ko tai galima atpažinti: Kiekvieno pranešimo rūšiavimo pastaba su rezultatu (susijęs su saugumu taip arba ne), paveiktomis versijomis ir atmetimo priežastimi, kur ji taikoma, matoma užduotyje arba priėmimo sąraše. Komandos, gaunančios nedaug pranešimų, gali rūšiuoti per trumpą pasikartojantį susitikimą ir rezultatą užrašyti dviem sakiniais kiekvienam įrašui.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

DM-3 **Patvirtinti saugumo defektai vertinami nuosekliu metodu: pagrindinė priežastis, paveiktos versijos ir konfigūracijos, galimas poveikis eksploatacijai ir saugumui, išnaudojamumas ir pavojingumas pagal nustatytą skalę. Vertinimo rezultatas registruojamas ir yra atsekamas.** Dokumentas

Iš ko tai galima atpažinti: Kiekvieno defekto vertinimo įrašas arba užduoties laukų rinkinys, apimantis pagrindinę priežastį, pavojingumą ir taikytą skalę (pavyzdžiui, plačiai naudojama pavojingumo vertinimo sistema su dokumentuotu vektoriumi), kartu su paveiktų versijų sąrašu. Mažos komandos gali remtis pastoviu laukų šablonu užduočių sistemoje ir puse puslapio, kuriame aprašyta skalė ir ribos, nuo kurių imamasi neatidėliotinų veiksmų.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

DM-4 **Kiekvienam įvertintam saugumo defektui priimamas sprendimas, kaip jis bus tvarkomas: ištaisymas, kompensuojanti priemonė arba pagrįstas rizikos prisiėmimas. Sprendimas kyla iš pavojingumo, jam paskiriamas atsakingas asmuo ir terminas, o defektas sekamas iki uždarymo.** Dokumentas

Iš ko tai galima atpažinti: Veiksmų sąrašas arba užduoties būsena su atsakingu asmeniu, terminu, priemonės rūšimi ir uždarymo pastaba, susieta su kodo baze arba laida, kurioje pataisa įsigalioja. Priimtoms liekamosioms rizikoms reikia trumpo rašytinio pagrindimo, kurį patvirtina produkto savininkas. Maža įmonė tai gali laikyti užduočių lentoje su terminais, be jokių papildomų įrankių.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

DM-5 **Paveikti naudotojai, integruotojai ir kitos suinteresuotosios šalys informuojami apie saugumo defektus, kai tik vertinimas to reikalauja, nurodant paveiktas versijas, poveikį ir prieinamą pataisą ar kompensuojančią priemonę. Tokio atskleidimo terminai ir gavėjų ratas nustatomi iš anksto, kaip ir elgesys su trečiųjų šalių pranešimais, turinčiais savo atskleidimo terminą.**

Iš ko tai galima atpažinti: Paskelbti saugumo pranešimai ar įspėjimai su data ir versijos nuoroda, platinimo sąrašas arba prenumeratorių kanalas ir rašytinė taisyklė dėl terminų bei koordinuoto atskleidimo. Tiekėjai, turintys nedaug klientų, gali naudoti vieną laišką pagal palaikomą klientų sąrašą ir įspėjimų puslapį su data, kurio pakeitimai yra versijuojami.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

DM-6 **Saugumo defektų tvarkymas peržiūrimas nustatytais intervalais. Peržiūra apžvelgia neuždarytus ir pavėluotus atvejus, laiką nuo pranešimo iki ištaisymo, pasikartojančias pagrindines priežastis ir taikytų priemonių rezultatyvumą. Iš peržiūros kylantys proceso patobulinimai įgyvendinami, o jų įgyvendinimas sekamas.** Dokumentas

Iš ko tai galima atpažinti: Pasikartojančios peržiūros protokolas su data, dalyviais, neuždarytų ir pavėluotų atvejų skaičiais bei sutartų patobulinimų sąrašu su atsakingu asmeniu ir terminu. Maža įmonė šį punktą gali prijungti prie esamo ketvirtinio susitikimo ir skaičius bei sprendimus laikyti viename puslapyje.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

11 7 praktika: Saugumo atnaujinimų valdymas (SUM) 5

SUM-1 **Kiekvienas produkto saugumo atnaujinimas prieš išleidžiant klientams yra patikrinamas su palaikomomis produkto versijomis ir veikimo aplinkomis, o įrašas rodo, kad atnaujinimas uždaro pažeidžiamumą netrikdydamas numatytos produkto funkcijos.** Dokumentas

Iš ko tai galima atpažinti: Kiekvienos pataisos testavimo įrašas su testuota produkto versija, platforma, testavimo atvejais (rezultatyvumas prieš pažeidžiamumą ir pagrindinių funkcijų regresija) ir išleidimo patvirtinimu. Mažas tiekėjas gali dirbti su trumpu pataisos patvirtinimo įrašu užduotyje: užduoties identifikatorius, kas patikrino, kada patikrino, rezultatas, pridedant automatinio testavimo žurnalą.

◯ Atviras ◯ Vykdomas ◯ Įvykdytas ◯ Netaikomas

Įrodymas / pagrindimas

SUM-2 **Visiems produkto komponentams, kurie sukurti ne savo jėgomis (trečiųjų šalių bibliotekos, operacinė sistema, vykdymo aplinkos), yra nustatyta ir įrodyta, kaip jų saugumo atnaujinimai vertinami ir arba perimami į produktą, arba atmetami su dokumentuotu pagrindimu.** Dokumentas

Iš ko tai galima atpažinti: Trečiųjų šalių dalių komponentų sąrašas su versija ir šaltiniu bei vienas vertinimo įrašas kiekvienam paskelbtam trečiosios šalies pažeidžiamumui su sprendimu (perimti, nepaveikta, padengta kompensuojančia priemone) ir pagrindimu. Mažos komandos kompiliavimo metu paleidžia automatinę priklausomybių patikrą ir sprendimus laiko kaip komentarus prie patikros rezultato arba trumpame išimčių sąraše.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SUM-3 **Su kiekvienu pateikiamu saugumo atnaujinimu naudotojai gauna suprantamą lydimąją informaciją: kurios produkto versijos yra paveiktos, kuris pažeidžiamumas ištaisytas, koks jo pavojingumas, ar reikia paisyti šalutinių poveikių bei kompensuojančių priemonių ir kaip atnaujinimas įdiegiamas.** Dokumentas

Iš ko tai galima atpažinti: Paskelbti saugumo įspėjimai arba laidos aprašai su pažeidžiamumo identifikatoriumi, paveiktomis versijomis, pavojingumo vertinimu, diegimo žingsniais ir nurodymais, kaip grįžti į ankstesnę būseną. Maži tiekėjai laiko vieną viešą puslapį su chronologiniu saugumo įspėjimų sąrašu ir pateikia nuorodą į jį iš paties produkto.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SUM-4 **Yra nustatytas ir nuo klastojimo apsaugotas kelias, kuriuo naudotojai gauna saugumo atnaujinimus, o atnaujinimo autentiškumą ir vientisumą naudotojo pusėje galima patikrinti prieš diegiant.**

Iš ko tai galima atpažinti: Pateikimo kanalo aprašas (atsisiuntimo sritis, atnaujinimų serveris, fizinės laikmenos) kartu su jo apsaugos priemonėmis, kiekvieno paketo skaitmeninis parašas arba kontrolinė suma ir nurodymai naudotojui, kaip tai patikrinti. Maži tiekėjai tai pasiekia pasirašydami kompiliavimo serveryje, skelbdami kontrolinę sumą šalia atsisiuntimo ir įvardydami vieną aiškią vietą, kurioje laikomas viešasis raktas.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SUM-5 **Yra nustatyti saugumo atnaujinimų pateikimo laiko tikslai, suskirstyti pagal pažeidžiamumo pavojingumą; faktiškai pasiekti laikai yra sekami, o kiekvienas nepasiektas tikslas pagrindžiamas ir palaikomas laikina priemone naudotojams.** Dokumentas

Iš ko tai galima atpažinti: Vidinis aprašas su laiko langu kiekvienai pavojingumo kategorijai (pavyzdžiui, kritinis <= 30 dienų, aukštas <= 90 dienų) ir kiekvieno pažeidžiamumo įvertinimas: pranešimo data, pataisos išleidimo data, praėjusios dienos, nukrypimo priežastis. Maži tiekėjai tai laiko kaip du datos laukus pažeidžiamumo užduotyje ir sąrašą peržiūri kartą per ketvirtį, užuot kūrę atskirą rodiklių sistemą.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

12 8 praktika: Saugumo gairės produktui diegti ir eksploatuoti (SG) 7

SG-1 **Su kiekvienu produktu pateikiamas jo giliosios gynybos strategijos aprašas: jis įvardija į patį produktą įdiegtus apsaugos sluoksnius, susieja juos su grėsmėmis, nuo kurių jie saugo, ir parodo, kuris apsaugos poveikis atsiranda tik keliems sluoksniams veikiant kartu.** Dokumentas

Iš ko tai galima atpažinti: Pateikiamos produkto dokumentacijos skyrius arba atskira saugumo koncepcija, kurioje kiekvienam apsaugos sluoksniui nurodytas mechanizmas, grėsmė, nuo kurios apsaugoma, ir jo poveikio ribos. Maža įmonė tai laiko kaip dviejų puslapių lentelę: stulpelis apsaugos sluoksnis, stulpelis grėsmė iš savo grėsmių modelio, stulpelis liekamoji rizika. Pakanka kryžminės nuorodos į SR-2 grėsmių modelį, turinio nereikia palaikyti du kartus.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SG-2 **Dokumentacija įvardija saugumo priemones, kurių produktas pats neužtikrina, bet tikisi iš diegimo aplinkos, pavyzdžiui, tinklo segmentavimą, priešais esančias užkardas, fizinės prieigos valdymą ar išorinę laiko paslaugą, ir aiškiai nurodo, kad be šių priemonių patikintas saugumo lygis nepasiekiamas.** Dokumentas

Iš ko tai galima atpažinti: Vadovo skyrius apie diegimo išankstines sąlygas arba pavyzdinės architektūros brėžinys su zonomis ir jungtimis, kuriame aiškiai pažymėtos priemonės, kurias pateikia turto savininkas. Praktikoje pasiteisino prielaidų apie aplinką sąrašas, išvestas tiesiai iš produkto saugumo konteksto ir peržiūrimas kiekvienai produkto versijai.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SG-3 **Yra saugios bazinės konfigūracijos vadovas, kuriame išvardytos visos su saugumu susijusios nuostatos, paslaugos, prievadai ir sąsajos, nurodyta rekomenduojama pateikimo būsena ir aprašytas nukrypimo nuo tos rekomendacijos poveikis.** Dokumentas

Iš ko tai galima atpažinti: Apsaugos sugriežtinimo vadovas su nuostatų lentele: parametras, rekomenduojama vertė, poveikis, šalutinis poveikis nukrypus. Kartu paslaugų ir prievadų, veikiančių numatytojoje konfigūracijoje, sąrašas su pagrindimu, kodėl jie lieka įjungti. Maža komanda šią lentelę laiko saugykloje šalia konfigūracijos failo ir eksportuoja ją į pateikimo dokumentaciją, todėl ji išlieka suderinta su produktu.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SG-4 **Nuolatinei eksploatacijai yra vadovas, aprašantis, kaip produktas saugiai eksploatuojamas, stebimas ir išlaikomas saugios būsenos, įskaitant atsarginę kopiją ir atkūrimą, įvykių registravimą ir su saugumu susijusių įvykių pranešimų tvarkymą.** Dokumentas

Iš ko tai galima atpažinti: Eksploatacijos vadovas su skyriais apie įvykių registravimą, atsargines kopijas, paleidimą iš naujo ir įvykių pranešimus. Kaip papildomas įrodymas, produkto siunčiamų su saugumu susijusių pranešimų sąrašas, kiekvienam su trumpu rekomenduojamu veiksmu, kad turto savininkui nereikėtų jų aiškintis vienam.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SG-5 **Dokumentacija paaiškina, kaip produkto naudotojų paskyros, vaidmenys ir teisės sukuriamos ir palaikomos, ypač vaidmenų atskyrimą, numatytųjų prisijungimo duomenų keitimą ir nebereikalingų paskyrų šalinimą.** Dokumentas

Iš ko tai galima atpažinti: Paskyrų valdymo skyrius su vaidmenų apžvalga ir kiekvienam vaidmeniui priskirtomis teisėmis bei aiškia pastaba apie numatytuosius prisijungimo duomenis ir jų keitimą paleidžiant eksploatuoti. Praktikoje gerai veikia trumpas paleidimo eksploatuoti kontrolinis sąrašas vadove, kurį turto savininkas gali pažymėti ir įsidėti į bylą.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SG-6 **Yra saugaus eksploatacijos nutraukimo vadovas, aprašantis visišką jautrių duomenų, tokių kaip prisijungimo duomenys, raktai, konfigūracijos duomenys ir žurnalai, pašalinimą iš produkto prieš perduodant, pakartotinai naudojant ar utilizuojant įrenginį.** Dokumentas

Iš ko tai galima atpažinti: Eksploatacijos nutraukimo skyrius, kuriame išvardytos visos jautrių duomenų saugojimo vietos produkte ir atitinkama trynimo procedūra, įskaitant atvejus, kai trynimas techniškai neįmanomas ir aparatinę įrangą tenka fiziškai sunaikinti. Čia padeda iš architektūros aprašo paimtas nuolatinių atminčių sąrašas, jis neleidžia pamiršti saugojimo vietos.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas

SG-7 **Naudotojams pateikiama saugumo dokumentacija peržiūrima prieš išleidimą: ji yra techniškai teisinga, suderinta su pateikiama produkto versija, išsami pagal numatytą turinį ir suprantama numatytai auditorijai, o pasikeitus produktui ji atnaujinama.**

Iš ko tai galima atpažinti: Kiekvieno dokumento ir produkto versijos peržiūros įrašas su peržiūrėtoju, data, pastebėjimais ir jų uždarymu, susietas su išleidimo patvirtinimu. Maža įmonė tai sprendžia keturių akių principu dokumentacijos sujungimo prašyme: vienas kūrėjas tikrina techninį turinį, antras asmuo tikrina suprantamumą, o patvirtinimas registruojamas užduotyje. Versiją galima siųsti tik tada, kai peržiūra yra dokumentuota.

○ Atviras ○ Vykdomas ○ Įvykdytas ○ Netaikomas

Įrodymas / pagrindimas