IEC 62443-4-1:2018 Levenscyclus voor veilige productontwikkeling voor industriële automatisering

Levenscyclus voor veilige ontwikkeling, acht praktijken

47 eisen. Deze norm is certificeerbaar door een geaccrediteerde instelling. Versie van 07/2026.

IEC 62443-4-1 kan gecertificeerd worden, maar het certificeringsobject is ongebruikelijk: wat wordt gecertificeerd is het ontwikkelproces van een met naam genoemde ontwikkelorganisatie, dus een concrete gedocumenteerde versie van de veilige levenscyclus. Niet een product en niet een persoon wordt gecertificeerd. De routes zijn ISASecure SDLA en het IECEE CB Scheme. Op dit moment leidt een dergelijk certificaat niet tot een vermoeden van conformiteit met de Cyberweerbaarheidsverordening van de EU (Cyber Resilience Act). Verwar dit niet met IEC 62443-4-2, die eisen stelt aan het component zelf. Deze lijst is een hulpmiddel voor zelfevaluatie, geen bewijs.

Bedrijf	Datum	Opgesteld door

5 Praktijk 1: Beveiligingsbeheer (SM) 13

SM-1 **Er bestaat een gedefinieerde productontwikkelingscyclus die beveiliging door alle fasen heen borgt, van het eerste concept tot de buitengebruikstelling van het product, en deze cyclus is degene die in de praktijk daadwerkelijk wordt gevolgd.** Document

Waaraan je het vaststelt: Procesbeschrijving of werkinstructie met de fasen, de op te leveren resultaten per fase en de overdrachtspunten, samen met bewijs uit een lopend project waaruit blijkt dat de fasen daadwerkelijk zijn doorlopen. Een kleine organisatie kan volstaan met een pagina per fase plus een checklist in het ticketsysteem; belangrijk is dat het gedocumenteerde proces en de dagelijkse praktijk overeenkomen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SM-2 **Elke taak in de veilige ontwikkelingscyclus heeft een aangewezen verantwoordelijke, en deze toewijzing is bekend bij de betrokken personen.** Document

Waaraan je het vaststelt: Rollen- en verantwoordelijkhedenmatrix die elke processtap koppelt aan een met naam genoemde rol, aangevuld met de actuele bezetting van die rollen. Met slechts een handvol mensen volstaat een tabel met rol, taak en persoon; belangrijk is de vervangingsregeling voor vakantie en ziekte.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SM-3 **Er is traceerbaar vastgelegd welke producten, varianten, releases en componenten onder de veilige ontwikkelingscyclus vallen en welke niet.** Document

Waaraan je het vaststelt: Lijst van de producten en versiestatussen binnen de reikwijdte met een onderbouwing voor opname en uitsluiting, bijgewerkt bij elke nieuwe release. In de praktijk werkt een kolom in het productoverzicht goed, met per rij een ja of nee plus een zin toelichting.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SM-4 **De mensen die beveiligingstaken op zich nemen, beschikken over de daarvoor benodigde technische competentie, en die competentie wordt bewust opgebouwd en actueel gehouden.**

Waaraan je het vaststelt: Competentieprofiel per beveiligingsrol, kwalificatieoverzichten, opleidingsplan en aanwezigheidsregistraties, aangevuld met een overzicht van openstaande hiaten. Kleine organisaties tonen dit aan met certificaten, deelname aan conferenties of webinars en een korte jaarlijkse evaluatie van wie welk hiaat wanneer sluit, waarbij indien nodig externe expertise wordt ingehuurd.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SM-5 **De reikwijdte van de veilige ontwikkelingscyclus is afgebakend en benoemt de betrokken locaties, organisatieonderdelen, leveranciersbijdragen en ontwikkelomgevingen, samen met de grenzen van die reikwijdte.** Document

Waaraan je het vaststelt: Reikwijdteverklaring die locaties, teams, uitbestede onderdelen en systemen omvat, plus een schets van de externe interfaces. Wie op één locatie ontwikkelt, legt dit in enkele zinnen vast en benoemt expliciet wat erbuiten valt, zoals extern ontwikkelde samenstellingen of hosting door derden.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SM-6 **Voor elk element dat aan gebruikers wordt geleverd, software, firmware, configuraties en bijbehorende bestanden, is een integriteitscontrole mogelijk, zodat ontvangers een ongemerkte wijziging kunnen detecteren.**

Waaraan je het vaststelt: Handtekeningen of gepubliceerde controlesommen per opleverpakket, een beschrijving van de methode en een voorbeeld uit een echte release, samen met instructies voor de klant over hoe de controle uit te voeren. Voor kleine teams volstaat een ondertekend controlesombestand naast de download plus een alinea in de release notes.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SM-7 **De omgevingen die worden gebruikt voor ontwikkeling, build en test zijn beschermd tegen ongeautoriseerde toegang en tegen manipulatie van broncode, buildhulpmiddelen en artefacten.**

Waaraan je het vaststelt: Toegangsbeveiligingsconcept voor repository, buildserver en testsystemen, toegangslijsten met de datum van de laatste beoordeling, registraties van beveiligingsrelevante wijzigingen en bewijs dat productie- en ontwikkeltoegang gescheiden zijn. Zonder eigen IT-afdeling volstaan tweefactorauthenticatie, een beschermde hoofdbranch met verplichte review en een halfjaarlijkse controle van wie nog toegang heeft.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SM-8 **Privésleutels die worden gebruikt om leveringen te ondertekenen, zijn beschermd tegen openbaarmaking en misbruik, en het gebruik ervan is beperkt tot geautoriseerde personen en systemen.**

Waaraan je het vaststelt: Beschrijving van sleutelopslag, toegang, vernieuwing en intrekking, bewijs van beschermde opslag zoals een hardwaretoken of een sleutelbeheerdienst, plus registraties van ondertekeningshandelingen. Een kleine organisatie bewaart de ondertekeningssleutel op een hardwaretoken, documenteert de twee personen met toegang en houdt een procedure klaar voor het geval van verlies.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SM-9 **Voor ingekochte of overgenomen componenten, met inbegrip van opensourcesoftware, zijn de beveiligingsverwachtingen ten aanzien van de leverancier vastgelegd en worden deze toegepast bij de selectie.** Document

Waaraan je het vaststelt: Beveiligingseisen in leveranciersspecificaties of contracten, selectiecriteria voor componenten van derden, een inventarisatie van alle componenten van derden met versie en herkomst, plus de beoordeling of de leverancier aan de verwachtingen voldoet. Zonder inkoopafdeling volstaat een bijgehouden componentenlijst met een kolom waarin wordt vastgelegd of de beveiligingsupdates en meldkanalen van de leverancier zijn gecontroleerd.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SM-10 **Componenten die in opdracht door een derde partij zijn ontwikkeld, zijn onderworpen aan dezelfde beveiligingseisen als interne ontwikkeling, en de naleving ervan wordt geverifieerd.**

Waaraan je het vaststelt: Inkooporder of contractdocumenten waarin de vereiste beveiligingsverplichtingen zijn vastgelegd, bewijs van de dienstverlener over de toegepaste werkwijzen, acceptatieregistraties en resultaten van eigen controles op het opgeleverde werk. Zonder auditbudget volstaan een contractuele garantie, het aanleveren van de testresultaten van de leverancier en een eigen steekproefcontrole voorafgaand aan acceptatie.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SM-11 **Beveiligingsgerelateerde bevindingen uit alle bronnen, tests, reviews, gebruikersmeldingen en meldingen van derden, worden vastgelegd, beoordeeld op hun impact, toegewezen aan een verantwoordelijke met een streefdatum, en opgevolgd tot afsluiting.** Document

Waaraan je het vaststelt: Defecten- of ticketsysteem met een specifieke markering voor beveiligingsonderwerpen, en per item de impactbeoordeling, de verantwoordelijke, de streefdatum en de afsluitnotitie, plus een overzicht van openstaande punten. Een klein team gebruikt een label in het bestaande ticketsysteem en een vast agendapunt in het wekelijkse overleg.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SM-12 **Voordat een product wordt vrijgegeven, wordt geverifieerd en aangetoond dat de beoogde stappen van de veilige ontwikkelingscyclus daadwerkelijk zijn uitgevoerd en dat de bijbehorende registraties zijn opgesteld.** Document

Waaraan je het vaststelt: Releasebeoordeling per release waarbij wordt getoetst aan de processtappen, met verwijzingen naar de betreffende registraties en een gedocumenteerd releasebesluit met datum en handtekening. In de praktijk werkt een releasechecklist goed die geen levering toestaat zonder volledig afgevinkte punten; openstaande punten worden onderbouwd en van een datum voorzien.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SM-13 **De veilige ontwikkelingscyclus zelf wordt regelmatig ter discussie gesteld en verbeterd, op basis van inzichten uit incidenten, testresultaten, feedback van klanten en het dreigingslandschap.**

Waaraan je het vaststelt: Registraties van de procesbeoordeling, bijvoorbeeld een directiebeoordeling of retrospectief, met de daaruit voortvloeiende procesveranderingen, de status van implementatie en een verwijzing naar de grondoorzaak. Wie de volwassenheidsniveaus van de norm gebruikt, legt per praktijk de huidige stand en het streefniveau vast; volwassenheidsniveau 4 vereist precies dit bewijs van continue verbetering. Voor een kleine organisatie volstaat een jaarlijkse bijeenkomst met notulen en drie concrete verbeteringen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

6 Praktijk 2: Specificatie van beveiligingseisen (SR) 5

SR-1 **De beoogde productcontext is beschreven: de verwachte operationele omgeving, de beveiligingsmaatregelen waarvan wordt aangenomen dat die omgeving ze levert, de beoogde gebruikersgroepen en rollen, de veronderstelde vertrouwensgrenzen, en de toepassingen waarvoor het product expliciet niet is bedoeld.** Document

Waaraan je het vaststelt: Een beschrijving van de beveiligingscontext van het product, hetzij als apart document, hetzij als vast onderdeel van de productspecificatie, die de netwerkomgeving, veronderstelde externe beschermingsmaatregelen zoals een firewall of fysieke toegangsbeveiliging, een lijst van rollen, en een expliciete lijst van toepassingen buiten de reikwijdte omvat. Een kleine organisatie beperkt dit tot twee pagina's, voegt een eenvoudige schets van de installatieomgeving toe en laat de producteigenaar dit dateren en goedkeuren.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SR-2 **Er bestaat een dreigingsmodel voor het product dat gegevensstromen, interfaces, vertrouwensgrenzen en aanvalspaden in kaart brengt, de daaruit voortvloeiende dreigingen en hun mogelijke impact benoemt, en tegenmaatregelen toewijst. Het wordt beoordeeld en bijgewerkt bij relevante wijzigingen en ten minste eenmaal per productrelease, en openstaande punten worden opgevolgd tot ze zijn afgesloten.** Document

Waaraan je het vaststelt: Dreigingsmodel met een gegevensstroomdiagram, een dreigingslijst per interface, toegewezen tegenmaatregelen en de status van openstaande punten, plus een revisiegeschiedenis met datum en auteur. Een kleine organisatie kan werken met een tabel per interface, met kolommen voor wat er mis kan gaan, hoe ernstig dat zou zijn, wat eraan wordt gedaan, en wie het beoordeelt.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SR-3 **De beveiligingseisen voor het product zijn vastgesteld en gedocumenteerd. Ze omvatten de resultaten van het dreigingsmodel, de beschreven beveiligingscontext van het product, de toepasselijke wettelijke en contractuele verplichtingen en het beoogde beveiligingsniveau, en ze bevatten de beveiligingsfuncties die het product zelf moet leveren.** Document

Waaraan je het vaststelt: Eisenlijst of tool voor eisenbeheer met een uniek identificatienummer per eis, de bron van elk item zoals een dreiging, een klantcontract of een wettelijke verplichting, en het beoogde beveiligingsniveau. Een kleine organisatie werkt dit uit als één tabel met een vaste ID-kolom waarop verificatie en tests later aansluiten.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SR-4 **Elke afzonderlijke beveiligingseis is zo geformuleerd dat deze ondubbelzinnig, vrij van tegenstrijdigheden, toetsbaar en herleidbaar is tot een specifieke productfunctie of interface, en de eis bevat de informatie die nodig is om deze later zonder verdere toelichting te verifiëren.**

Waaraan je het vaststelt: Een steekproef uit de eisenlijst die voor elke eis een meetbaar acceptatiecriterium en de betrokken functie of interface toont, samen met de koppeling tussen eis en testgeval. Een kleine organisatie controleert dit met een vast formuleringssjabloon en de controlevraag of er een testgeval uit de eis kan worden geschreven zonder terugvraag.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SR-5 **De beveiligingseisen worden beoordeeld voordat ze worden gebruikt in ontwerp en implementatie, met betrokkenheid van de betrokken partijen, zoals ontwikkeling, test, producteigenaarschap en, waar nuttig, verkoop of de klant. De beoordeling omvat volledigheid ten opzichte van het dreigingsmodel en de beveiligingscontext van het product, juistheid en toetsbaarheid. Bevindingen worden vastgelegd en opgevolgd tot afsluiting.**

Waaraan je het vaststelt: Beoordelingsverslag met datum, deelnemers en hun rollen, de beoordeelde versie van de eisen, een lijst van bevindingen met een verantwoordelijke en afsluitstatus, en een goedkeuringsnotitie. Een kleine organisatie regelt dit als een beoordeling door twee personen, ontwikkeling en test, met een kort verslag en een goedkeuringsregel in de eisenlijst.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

7 Praktijk 3: Beveiliging door ontwerp (SD) 4

SD-1 **Elk product heeft een ontwerpbeschrijving die de beveiligingsrelevante aspecten van de architectuur vastlegt: welke componenten er zijn, hoe ze onderling communiceren, waar de vertrouwensgrenzen lopen, welke externe interfaces worden blootgesteld en met welke mechanismen de eerder vastgestelde beveiligingseisen in het ontwerp worden gerealiseerd.** Document

Waaraan je het vaststelt: Architectuurdocument of ontwerpspecificatie met een diagram dat componenten, gegevensstromen en vertrouwensgrenzen toont, plus een koppelingstabel van elke beveiligingseis naar het ontwerpelement dat deze realiseert. Een kleine leverancier komt uit met één bijgehouden diagram plus twee of drie pagina's toelichting; belangrijk is dat het versiebeheerd is in de repository en wordt bijgewerkt telkens wanneer de architectuur verandert.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SD-2 **Het ontwerp wordt systematisch geanalyseerd op dreigingen. De analyse benoemt de doelstellingen van de aanvaller, de betrokken vertrouwensgrenzen en interfaces, de daaruit voortvloeiende dreigingen met hun waardering, en de in het ontwerp getroffen tegenmaatregelen. De analyse wordt herhaald telkens wanneer de architectuur of de omgeving wezenlijk verandert, en geïdentificeerde dreigingen worden opgevolgd totdat over elk ervan een besluit is genomen.** Document

Waaraan je het vaststelt: Dreigingsmodel per product of per grote release, bijvoorbeeld een tabel met kolommen voor dreiging, betrokken interface, waardering, tegenmaatregel en status, samen met de notulen van de modelleersessie met deelnemers en datum. Een klein team modelleert pragmatisch in een workshop van twee tot drie uur aan de hand van het architectuurdiagram en legt openstaande punten vast als tickets, zodat het bewijs van opvolging zonder extra inspanning ontstaat.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SD-3 **Het ontwerp volgt aantoonbaar erkende principes voor veilig ontwerpen, waaronder minimale rechten, minimaal aanvalsoppervlak, gelaagde verdediging, veilige standaardinstellingen, veilig gedrag bij storingen en beveiligingsmechanismen die zo eenvoudig en toetsbaar mogelijk zijn. De toepassing van deze principes is zichtbaar in het ontwerp en onderbouwd.**

Waaraan je het vaststelt: Een paragraaf in de ontwerpbeschrijving of een interne ontwerprichtlijn die de principes benoemt, plus concreet bewijs per principe in het product, zoals de rechtenmatrix van de diensten, de lijst van open poorten met onderbouwing, de standaardinstellingen bij levering of het gedocumenteerde foutafhandelingsgedrag. Een kleine leverancier gebruikt een korte checklist van deze principes als vast onderdeel van de ontwerpbeoordeling en bewaart het ingevulde formulier bij het ontwerp.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SD-4 **Het ontwerp wordt door gekwalificeerde collega's beoordeeld voordat de implementatie begint. De beoordeling omvat volledigheid ten opzichte van de beveiligingseisen, de juistheid en doeltreffendheid van de beveiligingsmechanismen en de resultaten van de dreigingsanalyse. Personen met voldoende beveiligingscompetentie nemen deel, bevindingen worden vastgelegd en opgevolgd tot afsluiting.** Document

Waaraan je het vaststelt: Beoordelingsverslag met datum, het beoordeelde item inclusief versie, deelnemers en hun rollen, lijst van bevindingen met status en het releasebesluit. Een klein team koppelt de beoordeling aan de pull request van de ontwerpdocumenten en laat de bevindingen als opmerkingen achter met een afsluitnotitie, wat opvolging aantoont zonder aanvullende hulpmiddelen. Wanneer beveiligingscompetentie intern ontbreekt, is een extern beoordelaar die per uur wordt ingeschakeld voor de kritieke ontwerpen de pragmatische route.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

8 Praktijk 4: Veilige implementatie (SI) 2

SI-1 **Er bestaat een gedefinieerd proces om de daadwerkelijke implementatie te toetsen aan het veilige ontwerp: de beoordeling bevestigt dat de in het ontwerp voorziene beschermingsmaatregelen daadwerkelijk aanwezig en doeltreffend zijn in de code, dat de gelaagde verdediging behouden blijft, en dat er tijdens de implementatie geen nieuwe kwetsbaarheden zijn geïntroduceerd. De beoordeling wordt uitgevoerd door voldoende gekwalificeerd personeel, en eventuele geconstateerde afwijkingen worden vastgelegd en opgevolgd tot afsluiting.**

Waaraan je het vaststelt: Een schriftelijke procedure voor implementatiebeoordeling samen met beoordelingsverslagen per component of release: de beoordeelde module, de verwijzing naar het ontwerpdocument, de datum, de beoordelaar, de bevindingen en hun oplossingsstatus. Geschikt bewijs zijn pull request reviews met een verplichte beveiligingschecklist, resultaten van statische codeanalyse met een gedocumenteerde beoordeling van elke treffer, en notulen van beoordelingssessies. Een klein team dekt dit af met het vierogenprincipe, een beoordelingssjabloon in de repository waarin elke ontwerpmaatregel afzonderlijk wordt afgevinkt, en één ticket per openstaande bevinding. Het essentiële punt is dat de auteur van de code nooit de beoordelaar van diezelfde code is.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SI-2 **Bindende regels voor veilig programmeren gelden voor al het beveiligingsrelevante ontwikkelwerk en omvatten ten minste het vermijden van bekende onveilige constructies en functies, de omgang met invoer en fouten, het beheer van geheugen en resources, en het gebruik van beproefde beveiligingscode in plaats van zelf geschreven implementaties. De regels gelden per gebruikte programmeertaal, zijn bekend bij alle ontwikkelaars, en worden bijgewerkt wanneer nodig, bijvoorbeeld wanneer nieuwe aanvalspatronen of nieuwe hulpmiddelen opkomen.** Document

Waaraan je het vaststelt: Een goedgekeurde standaard voor veilig programmeren met versiestatus, reikwijdte per taal en goedkeuringsdatum, aangevuld met bewijs dat deze in het dagelijkse werk wordt toegepast: de configuratie van linters en analysehulpmiddelen in de repository, een buildregel die overtredingen zichtbaar maakt, en de aanwezigheidslijst van de instructiesessie. Kleine organisaties schrijven geen standaard vanaf nul; ze verklaren een gevestigde openbare regelset bindend, voegen een korte lijst met eigen aanvullende regels toe, en verankeren de controle in de pipeline, zodat naleving automatisch wordt aangetoond.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

9 Praktijk 5: Beveiligingsverificatie en -validatietests (SVV) 5

SVV-1 **Elke beveiligingsgerelateerde producteis heeft ten minste één testgeval toegewezen gekregen, waarmee wordt aangetoond dat de beschermingsfunctie tijdens normaal gebruik werkt zoals bedoeld, dat deze zich gedraagt zoals gespecificeerd bij ongeldige invoer of misbruik, en dat de standaardinstellingen waarmee het product wordt geleverd overeenkomen met de veilige toestand. Uitvoering en uitkomst worden vastgelegd voor elke geteste softwareversie.** Document

Waaraan je het vaststelt: Een traceerbaarheidsmatrix die eis, testgeval en resultaat aan elkaar koppelt, plus testverslagen met de datum, de geteste versie of build, en de naam van de persoon die de test heeft uitgevoerd. Een kleine leverancier voegt eenvoudig een kolom met testgeval-ID toe aan de eisenlijst en archiveert het uitvoerlogboek van de geautomatiseerde testrun uit de buildpipeline als bijlage bij de betreffende versie.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SVV-2 **De uit het dreigingsmodel afgeleide tegenmaatregelen worden specifiek getest om te bevestigen dat ze het veronderstelde aanvalspad daadwerkelijk afsluiten. Er wordt getest tegen de geïdentificeerde dreigingen, niet alleen tegen correct gebruik, en openstaande punten worden ingebracht in het defectafhandelingsproces.**

Waaraan je het vaststelt: Testgevallen die rechtstreeks verwijzen naar de items van het dreigingsmodel, bijvoorbeeld één misbruikscenario per dreigings-ID met het verwachte verdedigingsgedrag, samen met de verslagen van die testruns. Zonder zwaar instrumentarium volstaat het om aan het dreigingsmodel een kolom toe te voegen die verwijst naar het testgeval en de datum van de laatste geslaagde controle.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SVV-3 **Het product wordt vóór vrijgave systematisch onderzocht op kwetsbaarheden. De reikwijdte omvat ten minste: onderzoek van de extern bereikbare interfaces en diensten, tests met misvormde en willekeurig gemuteerde invoer, toetsing van de gebruikte componenten van derden aan bekende gemelde kwetsbaarheden, en een controle op bekende zwakteklassen in de eigen code van de leverancier. Bevindingen worden vastgelegd samen met hun beoordeling.** Document

Waaraan je het vaststelt: Rapporten van de gebruikte hulpmiddelen, met vermelding van naam, versie en de gegevensstand van de kwetsbaarhedendatabase, fuzzingverslagen, een lijst van componenten van derden met de datum van de laatste vergelijking, en de bevindingenlijst met beoordeling en besluit. Een kleine leverancier combineert gratis standaardtools, een dependencyscan en een poort- en dienstenscan tegen het geïnstalleerde product, en bewaart de uitvoer per release in één map.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SVV-4 **De releasekandidaat wordt onderworpen aan een aanvalspoging onder realistische omstandigheden, waarbij actief wordt geprobeerd de beschermingsmechanismen te omzeilen in plaats van deze alleen te bevragen. Reikwijdte, randvoorwaarden en grenzen van de test worden vooraf overeengekomen, en de gevonden zwakheden worden behandeld en opgevolgd als defecten.**

Waaraan je het vaststelt: De opdracht of testorder met vermelding van reikwijdte en testomgeving, een rapport over de aanpak, de benutte zwakheden en hun beoordeling, plus de items in het defecten- of ticketsysteem met bewijs van herstel of van een onderbouwde risicoacceptatie. Kleine leveranciers kopen deze test doorgaans extern in met een afgebakend tijdsbudget, of laten deze uitvoeren door iemand die het product niet heeft ontwikkeld.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SVV-5 **De onafhankelijkheid van het testpersoneel is vastgelegd en passend bij het beoogde volwassenheidsniveau. Wie een component heeft ontwikkeld, geeft deze niet vrij op basis van uitsluitend eigen tests, en naarmate het volwassenheidsniveau stijgt, ligt de verantwoordelijkheid voor het testen bij een organisatorisch gescheiden eenheid of een externe partij. De daadwerkelijke toewijzing is voor elke test herleidbaar.**

Waaraan je het vaststelt: Een rollenverdeling binnen het ontwikkelproces waaruit de scheiding tussen creatie en testen blijkt, plus, voor elke testrun of elk testrapport, de vastgelegde naam en rol van de persoon die de test heeft uitgevoerd. Een bedrijf met twee personen regelt dit via wederzijdse beoordeling met een gedocumenteerde vierogennotitie, en schakelt een externe persoon in voor de diepgaande beveiligingstests.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

10 Praktijk 6: Beheer van beveiligingsdefecten (DM) 6

DM-1 **Er bestaat een vastgesteld kanaal waarlangs meldingen van beveiligingszwakheden in het product vanuit alle richtingen worden ontvangen en geregistreerd: van het ontwikkelteam zelf, van tests en beoordelingen, van klanten en integrators, van externe melders, en van adviezen over gebruikte componenten van derden en opensourcecomponenten. Het meldkanaal is vindbaar voor externe partijen, en elke melding wordt vastgelegd met de ontvangstdatum en de herkomst.** Document

Waaraan je het vaststelt: Een beschrijving van het meldkanaal, het publiek bereikbare contactpunt (een beveiligingspagina, een security.txt bestand, of een postbus zoals security@), en het intakeregister met datum, herkomst en een korte beschrijving per melding. Een kleine organisatie kan werken met een gedeelde postbus en één spreadsheet of ticketlabel, zolang elke melding daar terechtkomt, inclusief meldingen die in de interne ontwikkelaarschat naar voren komen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

DM-2 **Elke binnenkomende melding wordt getrieerd en onderzocht om vast te stellen of deze beveiligingsrelevant is en welke producten, versies en componenten worden geraakt. Meldingen die niet beveiligingsrelevant blijken te zijn, of niet van toepassing zijn, worden ook afgesloten met een vermelde reden in plaats van stilzwijgend terzijde gelegd.**

Waaraan je het vaststelt: Een triagenotitie per melding met de uitkomst (beveiligingsrelevant ja of nee), de betrokken versies, en de reden van afwijzing waar van toepassing, zichtbaar in het ticket of in de intakelijst. Teams met een laag meldingsvolume kunnen de triage uitvoeren in een korte terugkerende sessie en de uitkomst in twee zinnen per item vastleggen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

DM-3 **Bevestigde beveiligingsdefecten worden beoordeeld volgens een consistente methode: grondoorzaak, betrokken versies en configuraties, potentiële impact op werking en beveiliging, uitbuitbaarheid, en ernst tegen een vastgestelde schaal. Het resultaat van de beoordeling wordt vastgelegd en is herleidbaar.** Document

Waaraan je het vaststelt: Een beoordelingsverslag of een set ticketvelden per defect met grondoorzaak, ernst, en de toegepaste schaal (bijvoorbeeld een gangbaar puntensysteem met een gedocumenteerde vector), samen met de lijst van betrokken versies. Kleine teams kunnen steunen op een vast veldensjabloon in het ticketsysteem plus een halve pagina die de schaal en de drempels beschrijft die onmiddellijke actie vereisen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

DM-4 **Voor elk beoordeeld beveiligingsdefect wordt een besluit genomen over de aanpak: herstel, compenserende maatregel, of een onderbouwde risicoacceptatie. Het besluit volgt uit de ernst, wordt toegewezen aan een verantwoordelijke persoon en een streefdatum, en het defect wordt opgevolgd tot afsluiting.** Document

Waaraan je het vaststelt: Een actielijst of ticketstatus met verantwoordelijke, streefdatum, type maatregel, en een afsluitnotitie, gekoppeld aan de codebasislijn of de release waarin de oplossing van kracht wordt. Geaccepteerde restrisico's vereisen een korte schriftelijke onderbouwing die door het producteigenaarschap wordt goedgekeurd. Een kleine organisatie kan dit bijhouden op een ticketbord met streefdata, zonder aanvullende hulpmiddelen.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

DM-5 **Betrokken gebruikers, integrators en andere belanghebbenden worden over beveiligingsdefecten geïnformeerd zodra de beoordeling daartoe aanleiding geeft, met vermelding van de betrokken versies, de impact, en de beschikbare oplossing of compenserende maatregel. Tijdlijnen en de doelgroep van een dergelijke openbaarmaking zijn vooraf vastgesteld, evenals de aanpak voor meldingen van derden die met een eigen openbaarmakingstermijn komen.**

Waaraan je het vaststelt: Gepubliceerde beveiligingsmeldingen of adviezen met een datum en versievermelding, de distributielijst of het abonneekanaal, en de schriftelijke regel over tijdlijnen en gecoördineerde openbaarmaking. Leveranciers met weinig klanten kunnen volstaan met één mailing naar een bijgehouden klantenlijst plus een gedateerde adviespagina waarvan de wijzigingen worden bijgehouden in versies.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

DM-6 **De afhandeling van beveiligingsdefecten wordt op vaste tijdstippen beoordeeld. De beoordeling kijkt naar openstaande en achterstallige gevallen, de tijd van melding tot herstel, terugkerende grondoorzaken, en de doeltreffendheid van de getroffen maatregelen. Procesverbeteringen die uit de beoordeling voortvloeien, worden doorgevoerd en de doorvoering ervan wordt opgevolgd.** Document

Waaraan je het vaststelt: Notulen van de terugkerende beoordeling met datum, deelnemers, cijfers over openstaande en achterstallige gevallen, en een lijst van overeengekomen verbeteringen met verantwoordelijke en streefdatum. Een kleine organisatie kan dit punt koppelen aan een bestaand kwartaaloverleg en de cijfers en besluiten op één pagina bijhouden.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

11 Praktijk 7: Beheer van beveiligingsupdates (SUM) 5

SUM-1 **Elke beveiligingsupdate voor het product wordt geverifieerd tegen de ondersteunde productversies en operationele omgevingen voordat deze aan klanten wordt vrijgegeven, en er is een registratie die aantoont dat de update de kwetsbaarheid verhelpt zonder de beoogde productfunctie te verstoren.** Document

Waaraan je het vaststelt: Testverslag per patch met de geteste productversie, het platform, de testgevallen (doeltreffendheid tegen de kwetsbaarheid plus regressie van kernfuncties) en de vrijgavegoedkeuring. Een kleine leverancier kan werken met een korte goedkeuringsvermelding voor de patch in het ticket: ticket-ID, geverifieerd door, geverifieerd op, resultaat, met het logboek van de geautomatiseerde testrun als bijlage.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SUM-2 **Voor alle productcomponenten die niet intern zijn ontwikkeld (bibliotheken van derden, besturingssysteem, runtime-omgevingen), is vastgelegd en aangetoond hoe hun beveiligingsupdates worden beoordeeld en ofwel in het product worden opgenomen ofwel worden afgewezen met een gedocumenteerde onderbouwing.** Document

Waaraan je het vaststelt: Componenteninventaris van de onderdelen van derden met versie en herkomst, plus één beoordelingsvermelding per gemelde kwetsbaarheid van derden met het besluit (opnemen, niet geraakt, afgedekt door een compenserende maatregel) en de onderbouwing. Kleine teams voeren een geautomatiseerde dependencyscan uit in de build en houden de besluiten bij als opmerkingen bij het scanresultaat of in een beknopte uitzonderingslijst.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SUM-3 **Bij elke uitgebrachte beveiligingsupdate ontvangen gebruikers begrijpelijke begeleidende informatie: welke productversies worden geraakt, welke kwetsbaarheid wordt verholpen, hoe ernstig deze is, of er bijwerkingen of compenserende maatregelen in acht moeten worden genomen, en hoe de update wordt geïnstalleerd.** Document

Waaraan je het vaststelt: Gepubliceerde beveiligingsadviezen of release notes met het kwetsbaarheidsidentificatienummer, de betrokken versies, de ernstclassificatie, de installatiestappen en instructies voor het terugzetten naar de vorige toestand. Kleine leveranciers houden één publieke pagina bij met een chronologische lijst van beveiligingsadviezen en verwijzen ernaar vanuit het product.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SUM-4 **Er is een vastgestelde en tegen manipulatie beschermde route waarlangs gebruikers beveiligingsupdates verkrijgen, en de authenticiteit en integriteit van een update kunnen aan gebruikerszijde worden geverifieerd voordat deze wordt geïnstalleerd.**

Waaraan je het vaststelt: Beschrijving van het leveringskanaal (downloadgebied, updateserver, fysieke media) samen met de beschermingsmaatregelen ervan, plus de digitale handtekening of controlesom per pakket en instructies die de gebruiker vertellen hoe deze te verifiëren. Kleine leveranciers bereiken dit door te ondertekenen op de buildserver, de controlesom naast de download te publiceren en één duidelijke locatie te benoemen waar de publieke sleutel wordt bewaard.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SUM-5 **Er bestaan vastgestelde tijddoelen voor het beschikbaar stellen van beveiligingsupdates, gegradeerd naar de ernst van de kwetsbaarheid; de daadwerkelijk gehaalde tijden worden bijgehouden, en elk gemist doel wordt onderbouwd en ondersteund door een tussentijdse maatregel voor gebruikers.** Document

Waaraan je het vaststelt: Interne specificatie met een tijdvenster per ernstcategorie (bijvoorbeeld kritiek <= 30 dagen, hoog <= 90 dagen) en een evaluatie per kwetsbaarheid: meldingsdatum, datum van patchuitgifte, verstreken dagen, reden van afwijking. Kleine leveranciers houden dit bij als twee datumvelden in het kwetsbaarheidsticket en beoordelen de lijst eenmaal per kwartaal in plaats van een apart metriekensysteem op te zetten.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

12 Praktijk 8: Beveiligingsrichtlijnen voor inzet en gebruik van het product (SG) 7

SG-1 **Elk product wordt geleverd met een beschrijving van de strategie voor gelaagde verdediging: deze benoemt de beschermingslagen die in het product zelf zijn ingebouwd, koppelt ze aan de dreigingen die ze tegengaan, en toont welk beschermend effect pas ontstaat door de samenwerking van meerdere lagen.** Document

Waaraan je het vaststelt: Een paragraaf in de geleverde productdocumentatie, of een apart beveiligingsconcept, die per beschermingslaag het mechanisme, de gedekte dreiging en de grenzen van het effect vermeldt. Een kleine organisatie houdt dit bij als een tabel van twee pagina's: kolom beschermingslaag, kolom dreiging overgenomen uit het eigen dreigingsmodel, kolom restrisico. Een kruisverwijzing naar het dreigingsmodel uit SR-2 volstaat, de inhoud hoeft niet dubbel te worden bijgehouden.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SG-2 **De documentatie benoemt de beveiligingsmaatregelen die het product niet zelf levert maar verwacht van de inzetomgeving, bijvoorbeeld netwerksegmentatie, voorgeschakelde firewalls, fysieke toegangsbeveiliging of een externe tijddienst, en maakt duidelijk dat het gewaarborgde beveiligingsniveau zonder deze maatregelen niet wordt bereikt.** Document

Waaraan je het vaststelt: Een hoofdstuk over inzetvoorwaarden in de handleiding, of een referentiearchitectuurtekening met zones en verbindingen waarin de door de asset-eigenaar te leveren maatregelen expliciet zijn gemarkeerd. Een lijst met aannames over de omgeving heeft zich in de praktijk bewezen, rechtstreeks afgeleid van de beveiligingscontext van het product en opnieuw doorgenomen bij elke productversie.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SG-3 **Er bestaat een handleiding voor een veilige basisconfiguratie die alle beveiligingsrelevante instellingen, diensten, poorten en interfaces opsomt, de aanbevolen toestand bij levering vermeldt en het effect van afwijking van die aanbeveling beschrijft.** Document

Waaraan je het vaststelt: Hardeningshandleiding met een instellingentabel: parameter, aanbevolen waarde, effect, bijwerking bij afwijking. Plus de lijst van diensten en poorten die in de standaardconfiguratie actief zijn, met de onderbouwing waarom ze ingeschakeld blijven. Een klein team houdt deze tabel direct naast het configuratiebestand in de repository en exporteert deze naar de opleverdocumentatie, zodat deze afgestemd blijft op het product.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SG-4 **Voor het lopende gebruik bestaat er een handleiding die beschrijft hoe het product veilig wordt gebruikt, bewaakt en in zijn veilige toestand wordt gehouden, met inbegrip van back-up en herstel, logging en de omgang met beveiligingsrelevante gebeurtenismeldingen.** Document

Waaraan je het vaststelt: Gebruikshandleiding met paragrafen over logging, back-ups, herstart en gebeurtenismeldingen. Als aanvullend bewijs een lijst van de beveiligingsrelevante meldingen die het product uitzendt, elk met een korte aanbevolen actie, zodat de asset-eigenaar deze niet alleen hoeft te interpreteren.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SG-5 **De documentatie legt uit hoe gebruikersaccounts, rollen en rechten van het product worden ingesteld en onderhouden, in het bijzonder scheiding van rollen, het wijzigen van standaardreferenties en het verwijderen van accounts die niet langer nodig zijn.** Document

Waaraan je het vaststelt: Een hoofdstuk over accountbeheer met een overzicht van rollen en de aan elke rol toegekende rechten, plus een expliciete vermelding over standaardreferenties en het wijzigen ervan bij ingebruikname. Een korte checklist voor ingebruikname in de handleiding werkt in de praktijk goed, die de asset-eigenaar kan afvinken en archiveren.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SG-6 **Er bestaat een handleiding voor veilige buitengebruikstelling die de volledige verwijdering van gevoelige gegevens uit het product beschrijft, zoals referenties, sleutels, configuratiegegevens en logbestanden, voordat het apparaat wordt doorgegeven, hergebruikt of afgevoerd.** Document

Waaraan je het vaststelt: Een paragraaf over buitengebruikstelling die elke opslaglocatie van gevoelige gegevens binnen het product en de bijbehorende wisprocedure vermeldt, met inbegrip van de gevallen waarin wissen technisch onmogelijk is en de hardware fysiek moet worden vernietigd. Een lijst van persistente opslag, overgenomen uit de architectuurbeschrijving, helpt hierbij; deze voorkomt dat een opslaglocatie wordt vergeten.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing

SG-7 **De aan gebruikers geleverde beveiligingsdocumentatie wordt vóór vrijgave beoordeeld: deze is technisch juist, consistent met de geleverde productversie, volledig ten opzichte van de beoogde inhoud en begrijpelijk voor de beoogde doelgroep, en wordt bijgewerkt telkens wanneer het product verandert.**

Waaraan je het vaststelt: Een beoordelingsverslag per document en productversie met beoordelaar, datum, bevindingen en hun afsluiting, gekoppeld aan de vrijgavegoedkeuring. Een kleine organisatie lost dit op met het vierogenprincipe in de pull request van de documentatie: één ontwikkelaar controleert de technische inhoud, een tweede persoon controleert de begrijpelijkheid, en de goedkeuring wordt vastgelegd in het ticket. Een versie mag pas worden uitgeleverd zodra de beoordeling is gedocumenteerd.

◯ Open ◯ In behandeling ◯ Voldaan ◯ Niet van toepassing

Bewijs / onderbouwing