IEC 62443-4-1:2018 Säker utvecklingslivscykel för produkter inom industriell automation

Säker utvecklingslivscykel, åtta praxisområden

47 krav. Det går att certifiera sig mot denna standard hos ett ackrediterat certifieringsorgan. Utgåva 07/2026.

IEC 62443-4-1 går att certifiera mot, men föremålet är ovanligt: det som certifieras är utvecklingsprocessen hos en namngiven utvecklingsorganisation, alltså en konkret dokumenterad version av den säkra livscykeln. Varken en produkt eller en person certifieras. Vägarna är ISASecure SDLA och IECEE CB Scheme. Ett sådant certifikat medför enligt nuvarande läge ingen presumtion om överensstämmelse med EU Cyber Resilience Act. Blanda inte ihop den med IEC 62443-4-2, som ställer krav på själva komponenten. Denna lista är ett arbetsstöd för egenkontroll, inte ett bevis.

Företag	Datum	Upprättad av

5 Praxisområde 1: Säkerhetsstyrning (SM) 13

SM-1 **Det finns en fastställd livscykel för produktutveckling som bär säkerheten genom varje fas, från den första idén fram till avveckling av produkten, och det är denna livscykel som verkligen följs i det dagliga arbetet.** Dokument

Vad som styrker det: Processbeskrivning eller arbetsinstruktion som listar faserna, leveranserna per fas och överlämningspunkterna, tillsammans med bevis från ett pågående projekt som visar att faserna verkligen arbetades igenom. En liten verksamhet klarar sig med en sida per fas plus en checklista i ärendesystemet; det viktiga är att den dokumenterade processen och det dagliga arbetet stämmer överens.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SM-2 **Varje uppgift i den säkra utvecklingslivscykeln har en utpekad ansvarig, och denna fördelning är känd för dem som berörs.** Dokument

Vad som styrker det: Matris över roller och ansvar som kopplar varje processteg till en namngiven roll, kompletterad med den aktuella bemanningen av rollerna. Med bara en handfull personer räcker en tabell med roll, uppgift och person; det viktiga är ersättarordningen vid semester och sjukdom.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SM-3 **Det är spårbart fastställt vilka produkter, varianter, releaser och komponenter som omfattas av den säkra utvecklingslivscykeln och vilka som inte gör det.** Dokument

Vad som styrker det: En lista över produkterna och versionslägena som omfattas, med motivering till vad som räknas in och vad som lämnas utanför, uppdaterad vid varje ny release. I praktiken fungerar en kolumn i produktöversikten bra, med ja eller nej per rad plus en mening som motiverar valet.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SM-4 **De personer som tar sig an säkerhetsuppgifter har den tekniska kompetens som uppgifterna kräver, och kompetensen byggs upp och hålls aktuell på ett medvetet sätt.**

Vad som styrker det: Kompetensprofil per säkerhetsroll, redovisande dokument över kvalifikationer, utbildningsplan och redovisande dokument över närvaro, kompletterat med en översikt över luckorna. Små verksamheter visar detta med intyg, deltagande i konferenser eller webbinarier och en kort årlig genomgång av vem som stänger vilken lucka till när, och köper in extern expertis där det behövs.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SM-5 **Omfattningen av den säkra utvecklingslivscykeln är avgränsad och anger vilka orter, organisatoriska enheter, leverantörsbidrag och utvecklingsmiljöer som ingår, tillsammans med gränserna för omfattningen.** Dokument

Vad som styrker det: Beskrivning av omfattningen som täcker orter, team, utlagda delar och system, plus en skiss över de externa gränssnitten. Den som utvecklar på en enda ort dokumenterar detta i några meningar och namnger uttryckligen vad som ligger utanför, till exempel externt utvecklade moduler eller drift hos tredje part.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SM-6 **För varje del som levereras till användarna, programvara, fast programvara, konfigurationer och medföljande filer, går det att kontrollera integriteten så att mottagaren kan upptäcka en ändring som annars skulle passera obemärkt.**

Vad som styrker det: Digitala signaturer eller publicerade kontrollsummor per leveranspaket, en beskrivning av metoden och ett exempel från en verklig release, tillsammans med en instruktion till kunden om hur kontrollen utförs. För en liten verksamhet räcker en signerad kontrollsummefil bredvid nedladdningen plus ett stycke i releaseinformationen.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SM-7 **Utvecklings-, bygg- och testmiljöerna är skyddade mot obehörig åtkomst och mot manipulation av källkod, byggverktyg och artefakter.**

Vad som styrker det: Koncept för behörighetsstyrning av kodförrådet, byggservern och testsystemen, behörighetslistor med datum för den senaste genomgången, redovisande dokument över säkerhetsrelevanta ändringar och bevis för att åtkomsten till produktion och utveckling är åtskild. Utan egen IT-avdelning räcker tvåfaktorsinloggning, en skyddad huvudgren med obligatorisk granskning och en halvårsvis genomgång av vem som fortfarande har behörighet.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SM-8 **Privata nycklar som används för att signera leveranser är skyddade mot röjande och missbruk, och användningen är begränsad till behöriga personer och system.**

Vad som styrker det: Beskrivning av nyckelhanteringen med förvaring, åtkomst, förnyelse och spärr, bevis för skyddad förvaring, till exempel en maskinvarutoken eller en nyckelhanteringstjänst, plus redovisande dokument över signeringarna. En liten verksamhet förvarar signeringsnyckeln på en maskinvarutoken, dokumenterar de två personer som har åtkomst och har en rutin klar för fallet att nyckeln går förlorad.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SM-9 **För inköpta eller övertagna komponenter, inklusive programvara med öppen källkod, är de säkerhetsförväntningar som ställs på leverantören fastställda och de tillämpas vid valet.** Dokument

Vad som styrker det: Säkerhetskrav i leverantörsspecifikationer eller avtal, urvalskriterier för tredjepartskomponenter, en förteckning över alla tredjepartskomponenter med version och källa, plus bedömningen av om leverantören uppfyller förväntningarna. Utan egen inköpsavdelning räcker en underhållen komponentlista med en kolumn som dokumenterar om leverantörens säkerhetsuppdateringar och rapportvägar har kontrollerats.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SM-10 **Komponenter som en tredje part utvecklar på beställning omfattas av samma säkerhetskrav som den egna utvecklingen, och efterlevnaden verifieras.**

Vad som styrker det: Inköpsorder eller avtalshandlingar som anger de säkerhetsåtaganden som krävs, bevis från leverantören om de arbetssätt som tillämpas, redovisande dokument från godkännandet och resultat av de egna kontrollerna av det levererade arbetet. Utan budget för revision räcker en avtalad utfästelse, att leverantörens testresultat lämnas in och en egen stickprovskontroll före godkännandet.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SM-11 **Säkerhetsrelevanta resultat från alla källor, tester, granskningar, användarrapporter och meddelanden från tredje part, fångas upp, bedöms utifrån sin konsekvens, får en ansvarig och ett slutdatum och följs upp tills de är stängda.** Dokument

Vad som styrker det: Ärendesystem för fel med en egen märkning för säkerhetsfrågor, och per post konsekvensbedömningen, den ansvariga, slutdatumet och noteringen om stängning, plus en rapport över öppna punkter. En liten verksamhet använder en etikett i det befintliga ärendesystemet och en stående punkt på veckomötet.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SM-12 **Innan en produkt släpps är det verifierat och styrkt att de avsedda stegen i den säkra utvecklingslivscykeln verkligen genomfördes och att de tillhörande redovisande dokumenten togs fram.** Dokument

Vad som styrker det: En granskning per release mot processtegen, hänvisningar till respektive redovisande dokument och ett dokumenterat beslut om frisläppande med datum och underskrift. I praktiken fungerar en checklista för release bra, en som inte tillåter någon leverans utan fullständiga bockar; öppna punkter motiveras och får ett datum.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SM-13 **Den säkra utvecklingslivscykeln prövas och förbättras med regelbundna intervall, med lärdomar från incidenter, testresultat, återkoppling från kunder och hotbilden som underlag.**

Vad som styrker det: Redovisande dokument från genomgången av processen, till exempel ledningens genomgång eller en återblick, med de processändringar som utlöstes, deras införandestatus och en hänvisning till grundorsaken. Den som använder standardens mognadsnivåer dokumenterar nuläget och målet per praxisområde; mognadsnivå 4 kräver just detta bevis för ständig förbättring. För en liten verksamhet räcker ett möte per år med protokoll och tre konkreta förbättringar.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

6 Praxisområde 2: Specifikation av säkerhetskrav (SR) 5

SR-1 **Den avsedda produktomgivningen är beskriven: förväntad driftmiljö, de säkerhetsåtgärder som förutsätts finnas i den miljön, avsedda användargrupper och roller, antagna förtroendegränser och de användningar som produkten uttryckligen inte är avsedd för.** Dokument

Vad som styrker det: En beskrivning av produktens säkerhetskontext, antingen som ett eget dokument eller som ett fast avsnitt i produktspecifikationen, som täcker nätverksmiljön, antagna yttre skydd som brandvägg eller fysisk behörighetsstyrning, en lista över roller och en uttrycklig lista över användningar som ligger utanför omfattningen. En liten verksamhet håller detta till två sidor, lägger till en enkel skiss över anläggningsmiljön och låter produktansvarig datera och godkänna den.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR-2 **Det finns en hotmodell för produkten som kartlägger dataflöden, gränssnitt, förtroendegränser och angreppsvägar, namnger de hot som följer av dem och deras möjliga konsekvens och kopplar motåtgärder till dem. Den ses över och uppdateras vid relevanta ändringar och minst en gång per produktrelease, och öppna punkter följs upp tills de är stängda.** Dokument

Vad som styrker det: Hotmodell med ett dataflödesdiagram, en hotlista per gränssnitt, kopplade motåtgärder och status för öppna punkter, plus en ändringshistorik med datum och författare. En liten verksamhet arbetar med en tabell per gränssnitt, med kolumner för vad som kan gå fel där, hur allvarligt det vore, vad verksamheten gör åt det och vem som granskar det.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SR-3 **Säkerhetskraven på produkten är fastställda och dokumenterade. De täcker resultaten från hotmodellen, den beskrivna säkerhetskontexten för produkten, tillämpliga lagkrav och avtalade åtaganden och den avsedda säkerhetsnivån, och de omfattar de säkerhetsförmågor som produkten själv måste tillhandahålla.** Dokument

Vad som styrker det: Kravlista eller verktyg för kravhantering med en unik beteckning per krav, källan till varje post, till exempel ett hot, ett kundavtal eller ett lagkrav, och den avsedda säkerhetsnivån. En liten verksamhet driver detta som en enda tabell med en fast ID-kolumn som verifiering och test senare kopplar till.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR-4 **Varje enskilt säkerhetskrav är formulerat så att det är entydigt, fritt från motsägelser, testbart och spårbart till en bestämd produktfunktion eller ett bestämt gränssnitt, och det bär den information som behövs för att verifiera det senare utan ytterligare förtydliganden.**

Vad som styrker det: Ett stickprov ur kravlistan som per krav visar ett mätbart acceptanskriterium och den funktion eller det gränssnitt som berörs, tillsammans med kopplingen från krav till testfall. En liten verksamhet kontrollerar detta med en fast formuleringsmall och kontrollfrågan om ett testfall går att skriva utifrån kravet utan att fråga tillbaka.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SR-5 **Säkerhetskraven granskas innan de används i konstruktion och implementering, med de berörda parterna delaktiga, till exempel utveckling, test, produktansvar och där det är nyttigt försäljning eller kunden. Granskningen täcker fullständighet mot hotmodellen och produktens säkerhetskontext, riktighet och testbarhet. Resultaten dokumenteras och följs upp tills de är stängda.**

Vad som styrker det: Redovisande dokument från granskningen med datum, deltagare och deras roller, den granskade versionen av kraven, en lista över resultaten med ansvarig och status för stängning och en notering om godkännande. En liten verksamhet hanterar detta som en granskning mellan två personer från utveckling och test, med ett kort redovisande dokument och en rad om godkännande i kravlistan.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

7 Praxisområde 3: Säker konstruktion (SD) 4

SD-1 **Varje produkt har en konstruktionsbeskrivning som fångar de säkerhetsrelevanta delarna av arkitekturen: vilka komponenter som finns, hur de kommunicerar med varandra, var förtroendegränserna går, vilka externa gränssnitt som exponeras och genom vilka mekanismer de tidigare fastställda säkerhetskraven förverkligas i konstruktionen.** Dokument

Vad som styrker det: Arkitekturdokument eller konstruktionsspecifikation med ett diagram som visar komponenter, dataflöden och förtroendegränser, plus en kopplingstabell från varje säkerhetskrav till det konstruktionselement som förverkligar det. En liten verksamhet klarar sig med ett underhållet diagram plus två eller tre sidor förklaring; det viktiga är att det versionshanteras i kodförrådet och uppdateras så snart arkitekturen ändras.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SD-2 **Konstruktionen analyseras systematiskt med avseende på hot. Analysen namnger angriparens mål, de förtroendegränser och gränssnitt som berörs, de hot som följer av dem tillsammans med deras klassning och de motåtgärder som byggs in i konstruktionen. Den upprepas så snart arkitekturen eller omgivningen ändras väsentligt, och identifierade hot följs upp tills ett beslut har fattats om vart och ett av dem.** Dokument

Vad som styrker det: Hotmodell per produkt eller per större release, till exempel en tabell med kolumner för hot, berört gränssnitt, klassning, motåtgärd och status, tillsammans med protokoll från modelleringsmötet med deltagare och datum. En liten verksamhet modellerar pragmatiskt i en workshop på två till tre timmar längs arkitekturdiagrammet och dokumenterar öppna punkter som ärenden, så att beviset för uppföljningen uppstår utan extra arbete.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SD-3 **Konstruktionen följer påvisbart erkända principer för säker konstruktion, bland dem minsta möjliga behörighet, minsta möjliga angreppsyta, djupförsvar, säkra standardinställningar, säkert beteende vid fel och säkerhetsmekanismer som är så enkla och verifierbara som möjligt. Tillämpningen av principerna syns i konstruktionen och är motiverad.**

Vad som styrker det: Ett avsnitt i konstruktionsbeskrivningen eller en egen konstruktionsriktlinje som namnger principerna, plus konkreta bevis per princip i produkten, till exempel behörighetsmatrisen för tjänsterna, listan över öppna portar med motivering, standardinställningarna vid leverans eller det dokumenterade beteendet vid fel. En liten verksamhet använder en kort checklista över principerna som en fast punkt i konstruktionsgranskningen och arkiverar det ifyllda bladet tillsammans med konstruktionen.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SD-4 **Konstruktionen granskas av kvalificerade kollegor innan implementeringen börjar. Granskningen täcker fullständighet mot säkerhetskraven, riktigheten och verkan hos säkerhetsmekanismerna och resultaten från hotanalysen. Personer med tillräcklig säkerhetskompetens deltar, resultaten dokumenteras och följs upp tills de är stängda.** Dokument

Vad som styrker det: Redovisande dokument från granskningen med datum, det granskade objektet inklusive version, deltagare och deras roller, lista över resultaten med status och beslutet om godkännande. En liten verksamhet kopplar granskningen till pull request för konstruktionsdokumenten och lämnar resultaten som kommentarer med en notering om stängning, vilket styrker uppföljningen utan ytterligare verktyg. Saknas säkerhetskompetens i den egna verksamheten är en extern granskare på timbasis för de kritiska konstruktionerna den pragmatiska vägen.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

8 Praxisområde 4: Säker implementering (SI) 2

SI-1 **Det finns en fastställd process för att verifiera den faktiska implementeringen mot den säkra konstruktionen: granskningen bekräftar att de skyddsåtgärder som konstruktionen förutser verkligen finns i koden och är verkningsfulla, att djupförsvaret bevaras och att inga nya sårbarheter har införts under implementeringen. Granskningen utförs av personal med lämpliga kvalifikationer, och de avvikelser som hittas dokumenteras och följs upp tills de är stängda.**

Vad som styrker det: En skriven rutin för granskning av implementeringen tillsammans med redovisande dokument från granskningen per komponent eller release: den granskade modulen, hänvisningen till konstruktionsdokumentet, datum, granskaren, resultaten och status för åtgärdandet. Lämpliga bevis är granskningar i pull request med obligatorisk säkerhetschecklista, resultat från statisk kodanalys med en dokumenterad bedömning av varje träff och protokoll från granskningsmötena. En liten verksamhet täcker detta med fyraögonsprincipen, en granskningsmall i kodförrådet där varje åtgärd ur konstruktionen bockas av var för sig och ett ärende per öppet resultat. Det viktiga är att den som skrev koden aldrig granskar samma kod.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SI-2 **Bindande regler för säker kodning gäller för allt säkerhetsrelevant utvecklingsarbete och täcker minst att kända osäkra konstruktioner och funktioner undviks, hanteringen av indata och fel, hanteringen av minne och resurser och användningen av beprövad säkerhetskod i stället för egenskrivna lösningar. Reglerna gäller per programspråk som används, är kända för alla utvecklare och uppdateras vid behov, till exempel när nya angreppsmönster eller nya verktyg dyker upp.** Dokument

Vad som styrker det: En godkänd standard för säker kodning med versionsstatus, omfattning per språk och datum för godkännandet, kompletterad med bevis för att den får verkan i det dagliga arbetet: konfigurationen av linters och analysverktyg i kodförrådet, en byggregel som lyfter fram överträdelser och närvarolistan från genomgången. Små verksamheter skriver ingen standard från grunden; de förklarar ett etablerat offentligt regelverk bindande, lägger till en kort lista med egna tilläggsregler och förankrar kontrollen i byggkedjan så att efterlevnaden visas automatiskt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

9 Praxisområde 5: Test för verifiering och validering av säkerheten (SVV) 5

SVV-1 **Varje säkerhetsrelaterat produktkrav har minst ett testfall kopplat till sig som visar att skyddsfunktionen fungerar som avsett vid normal drift, att den beter sig som specificerat vid ogiltiga indata eller missbruk och att de standardinställningar som följer med produkten motsvarar det säkra läget. Genomförande och utfall dokumenteras för varje testad programvaruversion.** Dokument

Vad som styrker det: En spårbarhetsmatris som binder samman krav, testfall och resultat, plus redovisande dokument från testerna med datum, den version eller byggversion som testades och namnet på den som utförde testet. En liten verksamhet lägger helt enkelt till en kolumn med testfallets ID i kravlistan och arkiverar utdataloggen från den automatiska testkörningen i byggkedjan som en fil kopplad till respektive version.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SVV-2 **De motåtgärder som härleds ur hotmodellen testas särskilt för att bekräfta att de verkligen stänger den antagna angreppsvägen. Testerna riktas mot de identifierade hoten, inte bara mot regelrätt användning, och öppna punkter förs in i processen för felhantering.**

Vad som styrker det: Testfall som hänvisar direkt till posterna i hotmodellen, till exempel ett missbruksfall per hot-ID med det förväntade försvarsbeteendet, tillsammans med redovisande dokument från körningarna. Utan tunga verktyg räcker en kolumn i hotmodellen som hänvisar till testfallet och datum för den senaste lyckade kontrollen.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SVV-3 **Produkten undersöks systematiskt med avseende på sårbarheter före release. Omfattningen täcker minst: undersökning av de utifrån nåbara gränssnitten och tjänsterna, test med felformade och slumpmässigt muterade indata, granskning av de använda tredjepartskomponenterna mot kända rapporterade sårbarheter och en kontroll av kända svaghetsklasser i den egna koden. Resultaten dokumenteras tillsammans med bedömningen.** Dokument

Vad som styrker det: Rapporter från de verktyg som används med verktygets namn, version och sårbarhetsdatabasens uppdateringsläge, redovisande dokument från fuzzningen, en lista över tredjepartskomponenter med datum för den senaste jämförelsen och resultatlistan med bedömning och beslut. En liten verksamhet kombinerar fria standardverktyg, en beroendeskanning och en skanning av portar och tjänster mot den installerade produkten och lägger utdata per release i en mapp.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SVV-4 **Releasekandidaten utsätts för ett angreppsförsök under realistiska förhållanden som aktivt försöker kringgå skyddsmekanismerna i stället för att bara kontrollera att de finns. Omfattning, ramvillkor och gränser för testet avtalas i förväg, och de svagheter som hittas hanteras och följs upp som fel.**

Vad som styrker det: Uppdraget eller testbeställningen med omfattning och testmiljö, en rapport om tillvägagångssättet, de svagheter som utnyttjades och bedömningen av dem, plus posterna i ärendesystemet för fel med bevis för åtgärd eller för ett motiverat accepterande av risken. Små verksamheter köper vanligen detta test externt med en avgränsad tidsbudget eller låter det utföras av en person som inte utvecklade produkten.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SVV-5 **Testpersonalens oberoende är fastställt och står i rimlig proportion till den avsedda mognadsnivån. Den som utvecklade en komponent släpper den inte enbart utifrån sina egna tester, och med stigande mognadsnivå ligger testet hos en organisatoriskt skild enhet eller hos en extern part. Den faktiska fördelningen är spårbar för varje test.**

Vad som styrker det: En rollbeskrivning inom utvecklingsprocessen som visar uppdelningen mellan att skapa och att testa, plus namnet och rollen på den som utförde testet, dokumenterat för varje testkörning eller testrapport. En verksamhet med två personer löser detta med ömsesidig granskning och en dokumenterad notering om fyraögonsprincipen och tar in en extern person för de fördjupade säkerhetstesterna.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

10 Praxisområde 6: Hantering av säkerhetsfel (DM) 6

DM-1 **Det finns en fastställd kanal där rapporter om säkerhetssvagheter i produkten tas emot och dokumenteras från alla håll: från utvecklingsteamet självt, från test och granskningar, från kunder och integratörer, från externa rapportörer och från säkerhetsmeddelanden om använda tredjepartskomponenter och komponenter med öppen källkod. Rapportvägen går att hitta för utomstående, och varje rapport fångas upp med sitt mottagningsdatum och sin källa.** Dokument

Vad som styrker det: En beskrivning av rapportvägen, den offentligt nåbara kontaktpunkten (en säkerhetssida, en fil security.txt eller en brevlåda som security@) och ett mottagningsregister med datum, källa och en kort beskrivning per rapport. En liten verksamhet klarar sig med en delad brevlåda och ett enda kalkylblad eller en ärendeetikett, så länge varje rapport hamnar där, även de som väcks i den interna utvecklarchatten.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

DM-2 **Varje inkommande rapport sorteras och undersöks för att avgöra om den är säkerhetsrelevant och vilka produkter, versioner och komponenter den berör. Även rapporter som visar sig sakna säkerhetsrelevans eller inte vara tillämpliga stängs med angiven orsak i stället för att tyst läggas åt sidan.**

Vad som styrker det: En sorteringsnotering per rapport med utfallet (säkerhetsrelevant ja eller nej), de berörda versionerna och skälet till avslag där det är aktuellt, synlig i ärendet eller i mottagningslistan. Verksamheter med få rapporter kör sorteringen på ett kort återkommande möte och dokumenterar utfallet i två meningar per post.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

DM-3 **Bekräftade säkerhetsfel bedöms med en enhetlig metod: grundorsak, berörda versioner och konfigurationer, möjlig påverkan på drift och säkerhet, utnyttjbarhet och allvarlighetsgrad mot en fastställd skala. Bedömningens resultat dokumenteras och är spårbart.** Dokument

Vad som styrker det: Ett redovisande dokument från bedömningen eller en uppsättning ärendefält per fel som täcker grundorsak, allvarlighetsgrad och den skala som tillämpats (till exempel ett vanligt system för att bedöma allvarlighetsgrad med dokumenterad vektor), tillsammans med listan över berörda versioner. Små verksamheter förlitar sig på en fast fältmall i ärendesystemet plus en halv sida som beskriver skalan och de trösklar som utlöser omedelbar åtgärd.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

DM-4 **För varje bedömt säkerhetsfel finns ett beslut om hanteringen: rättning, kompenserande åtgärd eller ett motiverat accepterande av risken. Beslutet följer av allvarlighetsgraden, det får en ansvarig och ett slutdatum, och felet följs upp tills det är stängt.** Dokument

Vad som styrker det: En åtgärdslista eller ärendestatus med ansvarig, slutdatum, typ av åtgärd och en notering om stängning, kopplad till den kodbaslinje eller den release där rättningen får verkan. Accepterade restrisker behöver en kort skriftlig motivering som produktansvarig godkänner. En liten verksamhet håller detta på en ärendetavla med slutdatum, utan ytterligare verktyg.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

DM-5 **Berörda användare, integratörer och andra intressenter informeras om säkerhetsfel så snart bedömningen kräver det, med uppgift om berörda versioner, konsekvensen och den rättning eller kompenserande åtgärd som finns. Tidsramar och mottagarkretsen för sådant offentliggörande är fastställda i förväg, liksom hanteringen av rapporter från tredje part som kommer med ett eget slutdatum för offentliggörande.**

Vad som styrker det: Publicerade säkerhetsmeddelanden med datum och versionshänvisning, sändlistan eller prenumerationskanalen och den skrivna regeln om tidsramar och samordnat offentliggörande. Verksamheter med få kunder använder ett enda utskick till en underhållen kundlista plus en daterad meddelandesida vars ändringar versionshanteras.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

DM-6 **Hanteringen av säkerhetsfel ses över vid fastställda intervall. Genomgången tittar på öppna och försenade ärenden, tiden från rapport till åtgärd, återkommande grundorsaker och åtgärdernas verkan. De förbättringar av processen som följer av genomgången införs och införandet följs upp.** Dokument

Vad som styrker det: Protokoll från den återkommande genomgången med datum, deltagare, siffror över öppna och försenade ärenden och en lista över överenskomna förbättringar med ansvarig och slutdatum. En liten verksamhet lägger denna punkt på ett befintligt kvartalsmöte och håller siffrorna och besluten på en sida.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

11 Praxisområde 7: Hantering av säkerhetsuppdateringar (SUM) 5

SUM-1 **Varje säkerhetsuppdatering för produkten verifieras mot de produktversioner och driftmiljöer som stöds innan den släpps till kunderna, och det finns ett redovisande dokument som visar att uppdateringen stänger sårbarheten utan att störa den avsedda produktfunktionen.** Dokument

Vad som styrker det: Redovisande dokument från testet per säkerhetsuppdatering med den testade produktversionen, plattformen, testfallen (verkan mot sårbarheten plus regression av kärnfunktionerna) och godkännandet för release. En liten verksamhet klarar sig med en kort godkännandepost i ärendet: ärendets ID, verifierad av, verifierad den, resultat, med loggen från den automatiska testkörningen bifogad.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SUM-2 **För alla produktkomponenter som inte utvecklats i den egna verksamheten (tredjepartsbibliotek, operativsystem, körtidsmiljöer) är det fastställt och styrkt hur deras säkerhetsuppdateringar bedöms och antingen tas in i produkten eller avvisas med en dokumenterad motivering.** Dokument

Vad som styrker det: Komponentförteckning över tredjepartsdelarna med version och källa, plus en bedömningspost per rapporterad sårbarhet hos tredje part med beslutet (tas in, berör inte produkten, täcks av en kompenserande åtgärd) och motiveringen. Små verksamheter kör en automatisk beroendeskanning i byggkedjan och håller besluten som kommentarer till skanningsresultatet eller i en enkel undantagslista.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SUM-3 **För varje säkerhetsuppdatering som levereras får användarna begriplig medföljande information: vilka produktversioner som berörs, vilken sårbarhet som rättas, hur allvarlig den är, om sidoeffekter eller kompenserande åtgärder behöver beaktas och hur uppdateringen installeras.** Dokument

Vad som styrker det: Publicerade säkerhetsmeddelanden eller releaseinformation med sårbarhetens beteckning, de berörda versionerna, allvarlighetsgraden, installationsstegen och vägledning för att återgå till det tidigare läget. Små verksamheter håller en enda offentlig sida med en kronologisk lista över säkerhetsmeddelanden och länkar till den inifrån produkten.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SUM-4 **Det finns en fastställd och manipulationsskyddad väg där användarna hämtar säkerhetsuppdateringar, och en uppdaterings äkthet och integritet går att verifiera på användarsidan innan den installeras.**

Vad som styrker det: Beskrivning av leveranskanalen (nedladdningssida, uppdateringsserver, fysiska medier) tillsammans med dess skyddsåtgärder, plus den digitala signaturen eller kontrollsumman per paket och en instruktion som visar användaren hur den verifieras. Små verksamheter når dit genom att signera på byggservern, publicera kontrollsumman bredvid nedladdningen och peka ut en tydlig plats där den öppna nyckeln finns.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

SUM-5 **Det finns fastställda tidsmål för att göra säkerhetsuppdateringar tillgängliga, graderade efter sårbarhetens allvarlighetsgrad, de tider som faktiskt uppnås följs upp och varje mål som missas motiveras och kompletteras med en tillfällig åtgärd för användarna.** Dokument

Vad som styrker det: Intern specifikation med ett tidsfönster per allvarlighetsklass (till exempel kritisk <= 30 dagar, hög <= 90 dagar) och en utvärdering per sårbarhet: rapportdatum, datum för säkerhetsuppdateringens release, antal dagar som gick, orsak till avvikelse. Små verksamheter håller detta som två datumfält i sårbarhetsärendet och ser över listan en gång per kvartal i stället för att sätta upp ett eget system för nyckeltal.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

12 Praxisområde 8: Säkerhetsanvisningar för införande och drift av produkten (SG) 7

SG-1 **Varje produkt levereras med en beskrivning av sin strategi för djupförsvar: den namnger de skyddslager som är inbyggda i produkten själv, kopplar dem till de hot de motverkar och visar vilken skyddsverkan som uppstår först i samspelet mellan flera lager.** Dokument

Vad som styrker det: Ett avsnitt i den levererade produktdokumentationen eller ett eget säkerhetskoncept som per skyddslager anger mekanismen, det hot som täcks och gränserna för verkan. En liten verksamhet håller detta som en tabell på två sidor: kolumn skyddslager, kolumn hot hämtat ur den egna hotmodellen, kolumn restrisk. En korshänvisning till hotmodellen från SR-2 räcker, innehållet behöver inte underhållas två gånger.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SG-2 **Dokumentationen namnger de säkerhetsåtgärder som produkten inte själv tillhandahåller utan förväntar sig av driftmiljön, till exempel nätverkssegmentering, brandväggar framför produkten, fysisk behörighetsstyrning eller en extern tidstjänst, och gör klart att den utlovade säkerhetsnivån inte nås utan dessa åtgärder.** Dokument

Vad som styrker det: Ett kapitel om förutsättningar för införandet i handboken eller en referensarkitekturritning med zoner och kanaler där de åtgärder som tillgångsägaren svarar för är uttryckligen markerade. En lista över antagandena om omgivningen har visat sig nyttig i praktiken, härledd direkt ur produktens säkerhetskontext och genomläst på nytt för varje produktversion.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SG-3 **Det finns en anvisning för säker grundkonfiguration som listar alla säkerhetsrelevanta inställningar, tjänster, portar och gränssnitt, anger det rekommenderade läget vid leverans och beskriver följderna av att avvika från rekommendationen.** Dokument

Vad som styrker det: Härdningsanvisning med en inställningstabell: parameter, rekommenderat värde, verkan, sidoeffekt vid avvikelse. Plus listan över de tjänster och portar som är aktiva i standardkonfigurationen med en motivering till varför de förblir påslagna. En liten verksamhet håller tabellen direkt bredvid konfigurationsfilen i kodförrådet och exporterar den till leveransdokumentationen, så att den följer produkten.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SG-4 **För den löpande driften finns en anvisning som beskriver hur produkten drivs säkert, övervakas och hålls i sitt säkra läge, inklusive säkerhetskopiering och återläsning, loggning och hanteringen av säkerhetsrelevanta händelsemeddelanden.** Dokument

Vad som styrker det: Driftanvisning med avsnitt om loggning, säkerhetskopior, omstart och händelsemeddelanden. Som ytterligare bevis en lista över de säkerhetsrelevanta meddelanden produkten skickar, vart och ett med en kort rekommenderad åtgärd, så att tillgångsägaren inte behöver tolka dem på egen hand.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SG-5 **Dokumentationen förklarar hur produktens användarkonton, roller och behörigheter sätts upp och underhålls, särskilt uppdelningen av roller, byte av förvalda inloggningsuppgifter och borttagning av konton som inte längre behövs.** Dokument

Vad som styrker det: Ett kapitel om kontohantering med en översikt över rollerna och de rättigheter varje roll får, plus en uttrycklig notering om förvalda inloggningsuppgifter och om att byta dem vid idrifttagningen. En kort checklista för idrifttagningen i handboken fungerar bra i praktiken, en som tillgångsägaren kan bocka av och arkivera.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SG-6 **Det finns en anvisning för säker avveckling som beskriver hur känsliga uppgifter tas bort fullständigt ur produkten, till exempel inloggningsuppgifter, nycklar, konfigurationsdata och loggar, innan enheten lämnas vidare, återanvänds eller kasseras.** Dokument

Vad som styrker det: Ett avsnitt om avveckling som listar varje lagringsplats för känsliga uppgifter inuti produkten och den rutin för radering som hör till, inklusive de fall där radering är tekniskt omöjlig och maskinvaran måste förstöras fysiskt. En lista över de beständiga lagringsplatserna hämtad ur arkitekturbeskrivningen hjälper här, den hindrar att en lagringsplats glöms bort.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

SG-7 **Säkerhetsdokumentationen som levereras till användarna granskas före release: den är tekniskt riktig, stämmer med den levererade produktversionen, är fullständig mot det avsedda innehållet och begriplig för den avsedda målgruppen, och den uppdateras så snart produkten ändras.**

Vad som styrker det: Redovisande dokument från granskningen per dokument och produktversion med granskare, datum, resultat och deras stängning, kopplat till godkännandet för release. En liten verksamhet löser detta med fyraögonsprincipen i pull request för dokumentationen: en utvecklare kontrollerar det tekniska innehållet, en andra person kontrollerar begripligheten och godkännandet dokumenteras i ärendet. En version går att leverera först när granskningen är dokumenterad.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering