IEC 62443-4-1:2018 Ciclo di vita di sviluppo sicuro dei prodotti per l'automazione industriale

Ciclo di vita di sviluppo sicuro, otto pratiche

47 requisiti. Questa norma è certificabile da un organismo accreditato. Versione di 07/2026.

La norma IEC 62443-4-1 ammette la certificazione, ma l'oggetto è insolito: ciò che viene certificato è il processo di sviluppo di un'organizzazione di sviluppo nominata, cioè una versione documentata e concreta del ciclo di vita sicuro. Non viene certificato né un prodotto né una persona. I percorsi sono ISASecure SDLA e lo IECEE CB Scheme. Allo stato attuale, un simile certificato non genera una presunzione di conformità con il Regolamento sulla Ciberresilienza dell'UE (Cyber Resilience Act). Da non confondere con la IEC 62443-4-2, che pone requisiti sul componente stesso. Questo elenco è un supporto di lavoro per l'autovalutazione, non una prova.

Azienda	Data	Redatto da

5 Pratica 1: Gestione della sicurezza (SM) 13

SM-1 **Esiste un ciclo di vita di sviluppo del prodotto definito che porta la sicurezza attraverso ogni fase, dal concetto iniziale fino alla dismissione del prodotto, e questo ciclo di vita è quello effettivamente seguito nella pratica.** Documento

Come si dimostra: Descrizione del processo o istruzione di lavoro che elenca le fasi, i deliverable per fase e i punti di passaggio di consegne, insieme a evidenze di un progetto in corso che dimostrino che le fasi sono state effettivamente percorse. Una piccola organizzazione può bastare con una pagina per fase più una lista di controllo nel sistema di ticket; ciò che conta è che il processo documentato e la prassi quotidiana coincidano.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SM-2 **Ogni attività del ciclo di vita di sviluppo sicuro ha un responsabile assegnato, e questa assegnazione è nota alle persone coinvolte.** Documento

Come si dimostra: Matrice dei ruoli e delle responsabilità che assegna ogni fase del processo a un ruolo nominato, integrata dall'attuale copertura di quei ruoli. Con solo poche persone è sufficiente una tabella con ruolo, attività e persona; la parte importante è la regola di sostituzione per ferie e malattie.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SM-3 **È definito in modo tracciabile quali prodotti, varianti, versioni e componenti rientrano nel ciclo di vita di sviluppo sicuro e quali no.** Documento

Come si dimostra: Elenco dei prodotti e degli stati di versione inclusi nell'ambito con la motivazione delle inclusioni ed esclusioni, aggiornato a ogni nuova versione. In pratica funziona bene una colonna nella panoramica prodotti, con un sì o un no per riga più una frase di motivazione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SM-4 **Le persone che si assumono compiti di sicurezza possiedono la competenza tecnica richiesta, e tale competenza viene costruita e aggiornata in modo deliberato.**

Come si dimostra: Profilo di competenza per ruolo di sicurezza, registrazioni delle qualifiche, piano di formazione e registri di partecipazione, integrati da una panoramica delle lacune. Le organizzazioni piccole lo documentano tramite certificati, partecipazione a conferenze o webinar e una breve revisione annuale su chi colma quale lacuna entro quando, ricorrendo a competenze esterne dove necessario.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SM-5 **L'ambito del ciclo di vita di sviluppo sicuro è delimitato e indica le sedi, le unità organizzative, i contributi dei fornitori e gli ambienti di sviluppo coinvolti, insieme ai confini di tale ambito.** Documento

Come si dimostra: Dichiarazione di ambito che copre sedi, team, parti esternalizzate e sistemi, più uno schema delle interfacce esterne. Chi sviluppa in una singola sede lo documenta in poche frasi e indica esplicitamente ciò che ne resta fuori, come assiemi sviluppati esternamente o hosting presso terzi.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SM-6 **Per ogni elemento consegnato agli utenti, software, firmware, configurazioni e file di accompagnamento, è possibile un controllo di integrità, in modo che i destinatari possano rilevare una modifica non avvertita.**

Come si dimostra: Firme o checksum pubblicati per ogni pacchetto di consegna, una descrizione del metodo e un esempio tratto da una versione reale, insieme a istruzioni per il cliente su come eseguire il controllo. Per i team piccoli è sufficiente un file di checksum firmato accanto al download più un paragrafo nelle note di versione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SM-7 **Gli ambienti utilizzati per sviluppo, build e test sono protetti da accessi non autorizzati e da manomissioni del codice sorgente, degli strumenti di build e degli artefatti.**

Come si dimostra: Concetto di controllo degli accessi per repository, server di build e sistemi di test, elenchi di accesso con la data dell'ultima revisione, registrazioni delle modifiche rilevanti per la sicurezza ed evidenza che l'accesso di produzione e quello di sviluppo sono separati. Senza un reparto IT interno, bastano l'accesso a due fattori, un ramo principale protetto con revisione obbligatoria e una revisione semestrale di chi ha ancora accesso.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SM-8 **Le chiavi private utilizzate per firmare le consegne sono protette da divulgazione e uso improprio, e il loro utilizzo è limitato a persone e sistemi autorizzati.**

Come si dimostra: Descrizione della conservazione, dell'accesso, del rinnovo e della revoca delle chiavi, evidenza di una conservazione protetta come un token hardware o un servizio di gestione delle chiavi, più registrazioni delle operazioni di firma. Una piccola organizzazione conserva la chiave di firma su un token hardware, documenta le due persone con accesso e tiene pronta una procedura per il caso di smarrimento.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SM-9 **Per i componenti acquistati o adottati, incluso il software open source, le aspettative di sicurezza poste al fornitore sono definite e vengono applicate durante la selezione.** Documento

Come si dimostra: Requisiti di sicurezza nelle specifiche o nei contratti con i fornitori, criteri di selezione per i componenti di terze parti, un inventario di tutti i componenti di terze parti con versione e origine, più la valutazione se il fornitore soddisfa le aspettative. Senza un ufficio acquisti, è sufficiente un elenco di componenti aggiornato con una colonna che registri se sono stati verificati gli aggiornamenti di sicurezza e i canali di segnalazione del fornitore.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SM-10 **I componenti sviluppati su commissione da terzi sono soggetti agli stessi requisiti di sicurezza dello sviluppo interno, e il rispetto di tali requisiti viene verificato.**

Come si dimostra: Ordine di acquisto o documenti contrattuali che indicano gli obblighi di sicurezza richiesti, evidenza da parte del fornitore di servizi sulle pratiche applicate, registrazioni di accettazione e risultati dei propri controlli sul lavoro consegnato. Senza un budget per audit, sono sufficienti una garanzia contrattuale, la consegna dei risultati di test del fornitore e un controllo a campione proprio prima dell'accettazione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SM-11 **I riscontri relativi alla sicurezza provenienti da tutte le fonti, test, revisioni, segnalazioni degli utenti e notifiche di terzi, vengono registrati, valutati nel loro impatto, assegnati a un responsabile con una scadenza, e seguiti fino alla chiusura.** Documento

Come si dimostra: Sistema di difetti o ticket con un contrassegno dedicato per i temi di sicurezza, e per ogni voce la valutazione dell'impatto, il responsabile, la scadenza e la nota di chiusura, più un report sui punti aperti. Un piccolo team utilizza un'etichetta nel sistema di ticket esistente e un punto fisso all'ordine del giorno della riunione settimanale.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SM-12 **Prima che un prodotto venga rilasciato si verifica e si documenta che le fasi previste del ciclo di vita di sviluppo sicuro sono state effettivamente svolte e che le relative registrazioni sono state prodotte.** Documento

Come si dimostra: Revisione di rilascio per ogni versione, confrontata con le fasi del processo, riferimenti alle rispettive registrazioni e una decisione di rilascio documentata con data e firma. In pratica funziona bene una lista di controllo di rilascio che non consente la spedizione senza tutte le caselle spuntate; i punti aperti vengono motivati e dotati di una data.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SM-13 **Il ciclo di vita di sviluppo sicuro stesso viene regolarmente messo in discussione e migliorato, attingendo alle conoscenze derivanti da incidenti, risultati dei test, riscontri dei clienti e dall'evoluzione del panorama delle minacce.**

Come si dimostra: Registrazioni della revisione del processo, ad esempio un riesame di direzione o una retrospettiva, con le modifiche di processo innescate, il loro stato di attuazione e un riferimento alla causa radice. Chi utilizza i livelli di maturità della norma registra lo stato attuale e l'obiettivo per ogni pratica; il livello di maturità 4 richiede esattamente questa evidenza di miglioramento continuo. Per una piccola organizzazione basta una riunione all'anno con verbale e tre miglioramenti concreti.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

6 Pratica 2: Specifica dei requisiti di sicurezza (SR) 5

SR-1 **Viene descritto il contesto d'uso previsto del prodotto: ambiente operativo atteso, misure di sicurezza che si presume siano fornite da tale ambiente, gruppi di utenti e ruoli previsti, confini di fiducia assunti, e gli usi per i quali il prodotto è esplicitamente non destinato.** Documento

Come si dimostra: Una descrizione del contesto di sicurezza del prodotto, come documento a sé stante o come sezione fissa della specifica di prodotto, che copra l'ambiente di rete, le protezioni esterne assunte come un firewall o un controllo di accesso fisico, un elenco dei ruoli e un elenco esplicito degli usi fuori ambito. Una piccola organizzazione la limita a due pagine, aggiunge uno schema semplice dell'ambiente di impianto e la fa datare e approvare dal responsabile di prodotto.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SR-2 **Esiste un modello delle minacce per il prodotto che rappresenta i flussi di dati, le interfacce, i confini di fiducia e i percorsi di attacco, indica le minacce risultanti e il loro possibile impatto, e assegna le contromisure. Viene rivisto e aggiornato in caso di modifiche rilevanti e almeno una volta per ogni versione del prodotto, e i punti aperti vengono seguiti fino alla chiusura.** Documento

Come si dimostra: Modello delle minacce con un diagramma dei flussi di dati, un elenco delle minacce per ogni interfaccia, le contromisure assegnate e lo stato dei punti aperti, più uno storico delle revisioni con data e autore. Una piccola organizzazione può lavorare con una tabella per interfaccia, con colonne per cosa potrebbe andare storto, quanto sarebbe grave, cosa si fa al riguardo e chi la rivede.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SR-3 **I requisiti di sicurezza del prodotto sono definiti e documentati. Coprono i risultati del modello delle minacce, il contesto di sicurezza del prodotto descritto, gli obblighi legali e contrattuali applicabili e il livello di sicurezza target, e includono le capacità di sicurezza che il prodotto stesso deve fornire.** Documento

Come si dimostra: Elenco dei requisiti o strumento di gestione dei requisiti con un identificativo univoco per ogni requisito, l'origine di ciascuna voce, come una minaccia, un contratto con il cliente o un obbligo legale, e il livello di sicurezza target. Una piccola organizzazione lo gestisce come un'unica tabella con una colonna ID fissa a cui successivamente si agganciano verifica e test.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SR-4 **Ogni singolo requisito di sicurezza è formulato in modo inequivocabile, privo di contraddizioni, verificabile e tracciabile fino a una specifica funzione o interfaccia del prodotto, e contiene le informazioni necessarie per verificarlo in seguito senza ulteriori chiarimenti.**

Come si dimostra: Un campione dell'elenco dei requisiti che mostri, per ogni requisito, un criterio di accettazione misurabile e la funzione o interfaccia interessata, insieme alla corrispondenza tra requisito e caso di test. Una piccola organizzazione lo verifica con un modello di formulazione fisso e la domanda di controllo se sia possibile scrivere un caso di test a partire dal requisito senza dover chiedere chiarimenti.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SR-5 **I requisiti di sicurezza vengono rivisti prima di essere utilizzati nella progettazione e nell'implementazione, con il coinvolgimento delle parti interessate, come sviluppo, test, responsabile di prodotto e, dove utile, vendite o il cliente. La revisione copre la completezza rispetto al modello delle minacce e al contesto di sicurezza del prodotto, la correttezza e la verificabilità. I riscontri vengono registrati e seguiti fino alla chiusura.**

Come si dimostra: Registrazione della revisione con data, partecipanti e relativi ruoli, la versione dei requisiti sottoposta a revisione, un elenco dei riscontri con responsabile e stato di chiusura, e una nota di approvazione. Una piccola organizzazione lo gestisce come una revisione a due persone tra sviluppo e test, con una breve registrazione e una riga di approvazione nell'elenco dei requisiti.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

7 Pratica 3: Sicurezza fin dalla progettazione (SD) 4

SD-1 **Ogni prodotto dispone di una descrizione di progettazione che coglie gli aspetti rilevanti per la sicurezza dell'architettura: quali componenti esistono, come comunicano tra loro, dove corrono i confini di fiducia, quali interfacce esterne sono esposte e con quali meccanismi i requisiti di sicurezza definiti in precedenza vengono realizzati nella progettazione.** Documento

Come si dimostra: Documento di architettura o specifica di progettazione contenente un diagramma che mostri i componenti, i flussi di dati e i confini di fiducia, più una tabella di corrispondenza tra ogni requisito di sicurezza e l'elemento di progettazione che lo implementa. Un piccolo fornitore si accontenta di un diagramma mantenuto aggiornato più due o tre pagine di spiegazione; ciò che conta è che sia sotto controllo di versione nel repository e aggiornato ogni volta che l'architettura cambia.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SD-2 **La progettazione viene analizzata sistematicamente alla ricerca di minacce. L'analisi indica gli obiettivi dell'attaccante, i confini di fiducia e le interfacce interessate, le minacce risultanti insieme alla loro valutazione, e le contromisure adottate nella progettazione. Viene ripetuta ogni volta che l'architettura o l'ambiente cambiano in modo sostanziale, e le minacce individuate vengono seguite finché non è stata presa una decisione su ciascuna di esse.** Documento

Come si dimostra: Modello delle minacce per prodotto o per ogni versione principale, ad esempio una tabella con colonne per minaccia, interfaccia interessata, valutazione, contromisura e stato, insieme al verbale della sessione di modellazione con partecipanti e data. Un piccolo team modella in modo pragmatico in un workshop di due o tre ore seguendo il diagramma di architettura e registra i punti aperti come ticket, in modo che l'evidenza del monitoraggio venga prodotta senza sforzo aggiuntivo.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SD-3 **La progettazione segue in modo dimostrabile principi di progettazione sicura riconosciuti, tra cui il privilegio minimo, la superficie di attacco minima, la difesa in profondità, le impostazioni predefinite sicure, il comportamento sicuro in caso di guasto e meccanismi di sicurezza il più possibile semplici e verificabili. L'applicazione di questi principi è visibile nella progettazione ed è motivata.**

Come si dimostra: Una sezione nella descrizione di progettazione o una linea guida di progettazione interna che indichi i principi, più evidenze concrete per ogni principio nel prodotto, come la matrice dei privilegi dei servizi, l'elenco delle porte aperte con relativa motivazione, le impostazioni predefinite di consegna o il comportamento documentato di gestione degli errori. Un piccolo fornitore utilizza una breve lista di controllo di questi principi come voce fissa nella revisione di progettazione e archivia il foglio compilato insieme alla progettazione.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SD-4 **La progettazione viene rivista da pari qualificati prima dell'inizio dell'implementazione. La revisione copre la completezza rispetto ai requisiti di sicurezza, la correttezza e l'efficacia dei meccanismi di sicurezza e i risultati dell'analisi delle minacce. Partecipano persone con competenza di sicurezza sufficiente, i riscontri vengono registrati e seguiti fino alla chiusura.** Documento

Come si dimostra: Registrazione della revisione con data, elemento sottoposto a revisione con relativa versione, partecipanti e ruoli, elenco dei riscontri con stato e decisione di rilascio. Un piccolo team allega la revisione alla pull request dei documenti di progettazione e lascia i riscontri come commenti con una nota di chiusura, il che documenta il monitoraggio senza strumenti aggiuntivi. Dove manca la competenza di sicurezza interna, coinvolgere un revisore esterno a ore per le progettazioni critiche è la via pragmatica.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

8 Pratica 4: Implementazione sicura (SI) 2

SI-1 **Esiste un processo definito per verificare l'implementazione effettiva rispetto alla progettazione sicura: la revisione conferma che le misure di protezione previste nella progettazione sono effettivamente presenti ed efficaci nel codice, che la difesa in profondità è preservata, e che non sono state introdotte nuove vulnerabilità durante l'implementazione. La revisione viene svolta da personale adeguatamente qualificato, e ogni scostamento riscontrato viene registrato e seguito fino alla chiusura.**

Come si dimostra: Una procedura scritta per la revisione dell'implementazione insieme a registrazioni di revisione per componente o versione: il modulo rivisto, il riferimento al documento di progettazione, la data, il revisore, i riscontri e il loro stato di risoluzione. Come evidenza adeguata servono le revisioni delle pull request con una lista di controllo di sicurezza obbligatoria, i risultati dell'analisi statica del codice con una valutazione documentata di ogni segnalazione, e i verbali delle sessioni di revisione. Un piccolo team copre questo aspetto con il principio dei quattro occhi, un modello di revisione conservato nel repository in cui ogni misura di progettazione viene spuntata singolarmente, e un ticket per ogni riscontro aperto. Il punto essenziale è che l'autore del codice non sia mai il revisore dello stesso codice.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SI-2 **Regole vincolanti di codifica sicura si applicano a tutto il lavoro di sviluppo rilevante per la sicurezza e coprono almeno l'evitare costrutti e funzioni insicuri noti, la gestione degli input e degli errori, la gestione della memoria e delle risorse, e l'uso di codice di sicurezza collaudato invece di implementazioni proprie. Le regole si applicano per ogni linguaggio di programmazione utilizzato, sono note a tutti gli sviluppatori, e vengono aggiornate quando necessario, ad esempio quando emergono nuovi schemi di attacco o nuovi strumenti.** Documento

Come si dimostra: Uno standard di codifica sicura approvato con stato di versione, ambito per linguaggio e data di approvazione, integrato da evidenza che venga applicato nel lavoro quotidiano: la configurazione di linter e strumenti di analisi nel repository, una regola di build che segnala le violazioni, e l'elenco delle presenze al briefing. Le organizzazioni piccole non scrivono uno standard da zero; dichiarano vincolante un insieme di regole pubbliche già affermato, aggiungono un breve elenco di regole proprie supplementari, e ancorano il controllo nella pipeline in modo che il rispetto venga dimostrato automaticamente.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

9 Pratica 5: Verifica e validazione della sicurezza mediante test (SVV) 5

SVV-1 **Ogni requisito di prodotto rilevante per la sicurezza ha assegnato almeno un caso di test, che dimostra che la funzione di protezione funziona come previsto durante il funzionamento normale, che si comporta come specificato in presenza di input non validi o di uso improprio, e che le impostazioni predefinite di consegna del prodotto corrispondono allo stato sicuro. L'esecuzione e l'esito vengono registrati per ogni versione software testata.**

Documento

Come si dimostra: Una matrice di tracciabilità che collega requisito, caso di test e risultato, più registrazioni di test che mostrino la data, la versione o build testata, e il nome della persona che ha eseguito il test. Un piccolo fornitore aggiunge semplicemente una colonna con l'ID del caso di test al proprio elenco di requisiti e archivia il log di output dell'esecuzione automatica dei test dalla pipeline di build come file allegato alla rispettiva versione.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SVV-2 **Le contromisure derivate dal modello delle minacce vengono testate specificamente per confermare che chiudono effettivamente il percorso di attacco assunto. I test vengono eseguiti a fronte delle minacce individuate, non solo a fronte di un uso conforme, e i punti aperti vengono inseriti nel processo di gestione dei difetti.**

Come si dimostra: Casi di test che fanno riferimento direttamente alle voci del modello delle minacce, ad esempio un caso di abuso per ogni ID di minaccia con il comportamento difensivo atteso, insieme alle registrazioni di tali esecuzioni. Senza macchinari pesanti è sufficiente aggiungere al modello delle minacce una colonna che faccia riferimento al caso di test e alla data dell'ultimo controllo riuscito.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SVV-3 **Il prodotto viene esaminato sistematicamente alla ricerca di vulnerabilità prima del rilascio. L'ambito copre almeno: l'esame delle interfacce e dei servizi raggiungibili dall'esterno, i test con input malformati e mutati in modo casuale, la revisione dei componenti di terze parti utilizzati rispetto alle vulnerabilità note e segnalate, e una verifica delle classi di debolezza note nel codice proprio del fornitore. I riscontri vengono registrati insieme alla loro valutazione.**

Documento

Come si dimostra: Report degli strumenti utilizzati, che indicano nome dello strumento, versione e lo stato dei dati del database delle vulnerabilità, registrazioni di fuzzing, un elenco dei componenti di terze parti con la data dell'ultimo confronto, e l'elenco dei riscontri con valutazione e decisione. Un piccolo fornitore combina strumenti standard gratuiti, una scansione delle dipendenze e una scansione di porte e servizi sul prodotto installato, e archivia gli output per ogni versione in una cartella.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SVV-4 **Il candidato al rilascio viene sottoposto a un tentativo di attacco in condizioni realistiche che cerca attivamente di aggirare i meccanismi di protezione, anziché limitarsi a interrogarli. Ambito, condizioni al contorno e limiti del test vengono concordati in anticipo, e le debolezze riscontrate vengono gestite e seguite come difetti.**

Come si dimostra: L'incarico o l'ordine di test che indica ambito e ambiente di test, un report che copre l'approccio, le debolezze sfruttate e la loro valutazione, più le voci nel sistema di difetti o ticket con evidenza della correzione o di un'accettazione motivata del rischio. I piccoli fornitori acquistano tipicamente questo test esternamente con un budget di tempo delimitato, oppure lo fanno eseguire da una persona che non ha sviluppato il prodotto.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SVV-5 **L'indipendenza del personale addetto ai test è definita ed è adeguata al livello di maturità previsto. Chi ha sviluppato un componente non lo rilascia basandosi unicamente sui propri test, e con l'aumentare del livello di maturità i test sono di competenza di un'unità organizzativamente separata o di terzi esterni. L'assegnazione effettiva è tracciabile per ogni test.**

Come si dimostra: Una definizione dei ruoli all'interno del processo di sviluppo che mostri la separazione tra creazione e test, più, per ogni esecuzione o report di test, il nome e il ruolo registrati della persona che ha eseguito il test. Un'attività a conduzione di due persone gestisce questo aspetto attraverso una revisione reciproca con una nota documentata a quattro occhi, e coinvolge una persona esterna per i test di sicurezza approfonditi.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

10 Pratica 6: Gestione dei difetti di sicurezza (DM) 6

DM-1 Documento

Esiste un canale definito attraverso il quale vengono ricevute e registrate le segnalazioni di debolezze di sicurezza nel prodotto da ogni direzione: dal team di sviluppo stesso, da test e revisioni, da clienti e integratori, da segnalatori esterni, e da avvisi su componenti di terze parti e open source utilizzati. Il canale di segnalazione è individuabile da parte di terzi, e ogni segnalazione viene registrata con la relativa data di ricezione e la sua origine.

Come si dimostra: Una descrizione del canale di segnalazione, il punto di contatto pubblicamente raggiungibile (una pagina di sicurezza, un file security.txt, o una casella come security@), e il registro di ingresso con data, origine e una breve descrizione per ogni segnalazione. Una piccola organizzazione può lavorare con una casella condivisa e un unico foglio di calcolo o etichetta di ticket, purché ogni segnalazione vi confluisca, incluse quelle sollevate nella chat interna degli sviluppatori.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

DM-2

Ogni segnalazione in arrivo viene classificata ed esaminata per determinare se è rilevante per la sicurezza e quali prodotti, versioni e componenti riguarda. Anche le segnalazioni che risultano non rilevanti per la sicurezza, o non applicabili, vengono chiuse indicando un motivo, anziché essere scartate silenziosamente.

Come si dimostra: Una nota di classificazione per ogni segnalazione che indichi l'esito (rilevante per la sicurezza sì o no), le versioni interessate, e il motivo del rifiuto dove applicabile, visibile nel ticket o nell'elenco di ingresso. I team con un basso volume di segnalazioni possono svolgere la classificazione in una breve sessione periodica e registrare l'esito in due frasi per ogni voce.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

DM-3 Documento

I difetti di sicurezza confermati vengono valutati con un metodo coerente: causa radice, versioni e configurazioni interessate, potenziale impatto sull'operatività e sulla sicurezza, sfruttabilità e gravità rispetto a una scala definita. Il risultato della valutazione viene registrato ed è tracciabile.

Come si dimostra: Una registrazione di valutazione o un insieme di campi del ticket per ogni difetto che copra la causa radice, la gravità e la scala applicata (ad esempio un sistema di valutazione comune con un vettore documentato), insieme all'elenco delle versioni interessate. I piccoli team possono affidarsi a un modello di campi fisso nel sistema di ticket più mezza pagina che descriva la scala e le soglie che innescano un'azione immediata.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

DM-4 Documento

Per ogni difetto di sicurezza valutato viene presa una decisione su come verrà gestito: correzione, misura compensativa, o un'accettazione motivata del rischio. La decisione deriva dalla gravità, viene assegnata a una persona responsabile e a una scadenza, e il difetto viene seguito fino alla chiusura.

Come si dimostra: Un elenco di azioni o lo stato del ticket che mostri responsabile, data obiettivo, tipo di misura, e una nota di chiusura, collegato alla baseline di codice o alla versione in cui la correzione diventa effettiva. I rischi residui accettati necessitano di una breve motivazione scritta approvata dal responsabile di prodotto. Una piccola organizzazione può gestire questo aspetto in una bacheca di ticket con scadenze, senza strumenti aggiuntivi.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

DM-5

Gli utenti interessati, gli integratori e le altre parti interessate vengono informati sui difetti di sicurezza non appena la valutazione lo richiede, indicando le versioni interessate, l'impatto e la correzione o misura compensativa disponibile. Le tempistiche e l'ambito dei destinatari di tale divulgazione sono definiti in anticipo, così come l'approccio alle segnalazioni di terzi che arrivano con una propria scadenza di divulgazione.

Come si dimostra: Avvisi o bollettini di sicurezza pubblicati con data e riferimento di versione, l'elenco di distribuzione o il canale di iscrizione, e la regola scritta su tempistiche e divulgazione coordinata. I fornitori con pochi clienti possono utilizzare un unico invio a un elenco clienti aggiornato più una pagina di avvisi datata le cui modifiche sono versionate.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

DM-6 **La gestione dei difetti di sicurezza viene rivista a intervalli fissi. La revisione esamina i casi aperti e scaduti, il tempo trascorso dalla segnalazione alla correzione, le cause radice ricorrenti e l'efficacia delle misure adottate. I miglioramenti al processo derivanti dalla revisione vengono attuati e la loro attuazione viene seguita.**

Documento

Come si dimostra: Verbale della revisione periodica con data, partecipanti, dati sui casi aperti e scaduti, e un elenco dei miglioramenti concordati con responsabile e scadenza. Una piccola organizzazione può aggiungere questo punto a una riunione trimestrale già esistente e mantenere i dati e le decisioni su una sola pagina.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

11 Pratica 7: Gestione degli aggiornamenti di sicurezza (SUM) 5

SUM-1 **Ogni aggiornamento di sicurezza del prodotto viene verificato rispetto alle versioni di prodotto e agli ambienti operativi supportati prima di essere rilasciato ai clienti, ed esiste una registrazione che dimostra che l'aggiornamento chiude la vulnerabilità senza compromettere la funzione prevista del prodotto.**

Documento

Come si dimostra: Registrazione di test per ogni patch che copra la versione di prodotto testata, la piattaforma, i casi di test (efficacia contro la vulnerabilità più la regressione delle funzioni principali) e l'approvazione del rilascio. Un piccolo fornitore può lavorare con una breve voce di approvazione della patch nel ticket: ID ticket, verificato da, verificato il, risultato, con il log dell'esecuzione automatica dei test allegato.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SUM-2 **Per tutti i componenti di prodotto non sviluppati internamente (librerie di terze parti, sistema operativo, ambienti di runtime), è definito e documentato come vengono valutati i rispettivi aggiornamenti di sicurezza e come vengono adottati nel prodotto oppure respinti con una motivazione documentata.**

Documento

Come si dimostra: Inventario dei componenti delle parti di terze parti con versione e origine, più una voce di valutazione per ogni vulnerabilità di terze parti segnalata, indicando la decisione (adottare, non interessato, coperto da una misura compensativa) e la motivazione. I piccoli team eseguono una scansione automatica delle dipendenze nella build e mantengono le decisioni come commenti sul risultato della scansione o in un semplice elenco di eccezioni.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SUM-3 **Per ogni aggiornamento di sicurezza distribuito, gli utenti ricevono informazioni di accompagnamento comprensibili: quali versioni di prodotto sono interessate, quale vulnerabilità viene corretta, quanto è grave, se occorre tenere conto di effetti collaterali o misure compensative, e come si installa l'aggiornamento.**

Documento

Come si dimostra: Avvisi di sicurezza o note di versione pubblicati che indicano l'identificativo della vulnerabilità, le versioni interessate, la valutazione di gravità, i passaggi di installazione e le indicazioni per tornare allo stato precedente. I piccoli fornitori mantengono un'unica pagina pubblica con un elenco cronologico degli avvisi di sicurezza e vi rimandano dall'interno del prodotto.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SUM-4 **Esiste un percorso definito e protetto da manomissioni attraverso il quale gli utenti ottengono gli aggiornamenti di sicurezza, e l'autenticità e l'integrità di un aggiornamento possono essere verificate lato utente prima dell'installazione.**

Come si dimostra: Descrizione del canale di distribuzione (area di download, server di aggiornamento, supporto fisico) insieme alle relative misure di protezione, più la firma digitale o il checksum per ogni pacchetto e istruzioni che indichino all'utente come verificarlo. I piccoli fornitori raggiungono questo obiettivo firmando sul server di build, pubblicando il checksum accanto al download e indicando un unico luogo chiaro in cui è conservata la chiave pubblica.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

SUM-5 **Esistono obiettivi di tempo definiti per la disponibilità degli aggiornamenti di sicurezza, graduati in base alla gravità della vulnerabilità; i tempi effettivamente raggiunti vengono monitorati, e ogni obiettivo mancato viene motivato e supportato da una misura provvisoria per gli utenti.** Documento

Come si dimostra: Specifica interna con una finestra temporale per categoria di gravità (ad esempio critica <= 30 giorni, alta <= 90 giorni) e una valutazione per ogni vulnerabilità: data di segnalazione, data di rilascio della patch, giorni trascorsi, motivo dello scostamento. I piccoli fornitori mantengono questo aspetto come due campi data nel ticket della vulnerabilità e rivedono l'elenco una volta al trimestre invece di allestire un sistema di metriche dedicato.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

12 Pratica 8: Linee guida di sicurezza per l'implementazione e l'esercizio del prodotto (SG) 7

SG-1 **Ogni prodotto è accompagnato da una descrizione della propria strategia di difesa in profondità: indica i livelli di protezione integrati nel prodotto stesso, li collega alle minacce che contrastano, e mostra quale effetto protettivo emerge solo dall'interazione di più livelli.** Documento

Come si dimostra: Una sezione nella documentazione di prodotto consegnata, o un concetto di sicurezza separato, che indichi per ogni livello di protezione il meccanismo, la minaccia coperta e i limiti del suo effetto. Una piccola organizzazione mantiene questo come una tabella di due pagine: colonna livello di protezione, colonna minaccia tratta dal proprio modello delle minacce, colonna rischio residuo. È sufficiente un riferimento incrociato al modello delle minacce di SR-2, il contenuto non deve essere mantenuto due volte.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SG-2 **La documentazione indica le misure di sicurezza che il prodotto non fornisce da sé ma che si attende dall'ambiente di implementazione, ad esempio la segmentazione di rete, firewall a monte, il controllo di accesso fisico o un servizio orario esterno, e chiarisce che il livello di sicurezza garantito non viene raggiunto senza tali misure.** Documento

Come si dimostra: Un capitolo sui prerequisiti di implementazione nel manuale, o uno schema di architettura di riferimento con zone e condotti in cui vengono contrassegnate esplicitamente le misure da fornire a cura del proprietario dell'asset. Nella pratica si è dimostrato utile un elenco di assunzioni sull'ambiente, derivato direttamente dal contesto di sicurezza del prodotto e riletto a ogni versione del prodotto.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SG-3 **Esiste una guida alla configurazione di base sicura che elenca tutte le impostazioni, i servizi, le porte e le interfacce rilevanti per la sicurezza, indica lo stato di consegna raccomandato e descrive l'impatto di uno scostamento da tale raccomandazione.** Documento

Come si dimostra: Guida all'hardening con una tabella delle impostazioni: parametro, valore raccomandato, effetto, effetto collaterale in caso di scostamento. Più l'elenco dei servizi e delle porte attivi nella configurazione predefinita con la motivazione del perché restano abilitati. Un piccolo team mantiene questa tabella proprio accanto al file di configurazione nel repository e la esporta nella documentazione di consegna, in modo che resti allineata al prodotto.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SG-4 **Per l'esercizio continuativo esiste una guida che descrive come il prodotto viene gestito in modo sicuro, monitorato e mantenuto nel suo stato sicuro, incluso backup e ripristino, registrazione degli eventi e la gestione dei messaggi di evento rilevanti per la sicurezza.** Documento

Come si dimostra: Guida operativa con sezioni su registrazione degli eventi, backup, riavvio e messaggi di evento. Come evidenza aggiuntiva, un elenco dei messaggi rilevanti per la sicurezza emessi dal prodotto, ciascuno con una breve azione raccomandata, in modo che il proprietario dell'asset non debba interpretarli da solo.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SG-5 **La documentazione spiega come vengono impostati e mantenuti gli account utente, i ruoli e i permessi del prodotto, in particolare la separazione dei ruoli, la modifica delle credenziali predefinite e la rimozione degli account non più necessari.** Documento

Come si dimostra: Un capitolo di gestione degli account con una panoramica dei ruoli e dei diritti assegnati a ciascun ruolo, più una nota esplicita sulle credenziali predefinite e sulla loro modifica in fase di messa in servizio. Nella pratica funziona bene una breve lista di controllo di messa in servizio nel manuale, che il proprietario dell'asset possa spuntare e archiviare.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SG-6 **Esiste una guida per la dismissione sicura che descrive la rimozione completa dei dati sensibili dal prodotto, come credenziali, chiavi, dati di configurazione e log, prima che il dispositivo venga ceduto, riutilizzato o smaltito.** Documento

Come si dimostra: Una sezione di dismissione che elenchi ogni ubicazione di archiviazione di dati sensibili all'interno del prodotto e la relativa procedura di cancellazione, compresi i casi in cui la cancellazione è tecnicamente impossibile e l'hardware deve essere distrutto fisicamente. Qui aiuta un elenco della memoria persistente tratto dalla descrizione dell'architettura, che evita che un'ubicazione di archiviazione venga dimenticata.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

SG-7 **La documentazione di sicurezza consegnata agli utenti viene rivista prima del rilascio: è tecnicamente corretta, coerente con la versione di prodotto consegnata, completa rispetto al contenuto previsto e comprensibile per il pubblico a cui è destinata, e viene aggiornata ogni volta che il prodotto cambia.**

Come si dimostra: Una registrazione di revisione per ogni documento e versione di prodotto con revisore, data, riscontri e la loro chiusura, collegata all'approvazione del rilascio. Una piccola organizzazione risolve questo aspetto con il principio dei quattro occhi nella pull request della documentazione: uno sviluppatore verifica il contenuto tecnico, una seconda persona verifica la comprensibilità, e l'approvazione viene registrata nel ticket. Una versione è distribuibile solo una volta documentata la revisione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione