# IEC 62443-4-1:2018 Cycle de vie de développement sécurisé des produits pour l'automatisation industrielle

Cycle de vie de développement sécurisé, huit pratiques

47 exigences. Cette norme peut être certifiée par un organisme accrédité. Version de 07/2026.

La norme IEC 62443-4-1 permet une certification, mais l'objet est particulier : ce qui est certifié, c'est le processus de développement d'une organisation de développement nommée, c'est-à-dire une version documentée et concrète du cycle de vie sécurisé. Ni un produit ni une personne n'est certifié. Les voies possibles sont ISASecure SDLA et le IECEE CB Scheme. En l'état actuel, un tel certificat ne crée pas de présomption de conformité avec le règlement européen sur la cyber-résilience (Cyber Resilience Act). Il ne faut pas la confondre avec IEC 62443-4-2, qui impose des exigences au composant lui-même. Cette liste est une aide de travail pour l'auto-évaluation, pas une preuve.

| Entreprise | Date | Établi par |
|---|---|---|
| | | |

## 5 Pratique 1 : Gestion de la sécurité (SM) 13

**SM-1** **Il existe un cycle de vie de développement de produit défini qui porte la sécurité à travers toutes les phases, du concept initial jusqu'au retrait de service du produit, et ce cycle de vie est bien celui réellement suivi dans la pratique.** Document

Comment le prouver: Description de processus ou instruction de travail énumérant les phases, les livrables par phase et les points de transfert, accompagnée de preuves issues d'un projet en cours montrant que les phases ont réellement été parcourues. Une petite organisation peut se contenter d'une page par phase plus une liste de contrôle dans le système de tickets ; l'important est que le processus documenté et la pratique quotidienne correspondent.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

**SM-2** **Chaque tâche du cycle de vie de développement sécurisé a un responsable désigné, et cette désignation est connue des personnes concernées.** Document

Comment le prouver: Matrice des rôles et responsabilités faisant correspondre chaque étape du processus à un rôle nommé, complétée par l'affectation actuelle des personnes à ces rôles. Avec seulement une poignée de personnes, un tableau avec rôle, tâche et personne suffit ; l'important est la règle de suppléance en cas de congés et d'arrêts maladie.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

**SM-3** **Il est défini de manière traçable quels produits, variantes, versions et composants relèvent du cycle de vie de développement sécurisé et lesquels n'en relèvent pas.** Document

Comment le prouver: Liste des produits et états de version concernés, avec une justification des inclusions et exclusions, tenue à jour à chaque nouvelle version. Dans la pratique, une colonne dans la vue d'ensemble des produits fonctionne bien, avec un oui ou un non par ligne plus une phrase de justification.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

**SM-4** **Les personnes qui assument des tâches de sécurité disposent de la compétence technique requise, et cette compétence est développée et actualisée de manière délibérée.**

Comment le prouver: Profil de compétences par rôle de sécurité, justificatifs de qualification, plan de formation et registres de présence, complétés par une vue d'ensemble des écarts. Les petites organisations en apportent la preuve par des certificats, la participation à des conférences ou webinaires et un court bilan annuel indiquant qui comble quel écart et pour quand, en faisant appel à une expertise externe si nécessaire.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

**SM-5** **Le périmètre du cycle de vie de développement sécurisé est délimité et nomme les sites, unités organisationnelles, contributions de fournisseurs et environnements de développement concernés, ainsi que les limites de ce périmètre.** Document

Comment le prouver: Déclaration de périmètre couvrant les sites, les équipes, les parties externalisées et les systèmes, plus un schéma des interfaces externes. Quiconque développe sur un site unique le consigne en quelques phrases et nomme explicitement ce qui se situe hors périmètre, comme des sous-ensembles développés en externe ou un hébergement chez un tiers.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SM-6** **Pour chaque élément livré aux utilisateurs, logiciel, micrologiciel, configurations et fichiers d'accompagnement, un contrôle d'intégrité est possible afin que les destinataires puissent détecter une modification non signalée.**

Comment le prouver: Signatures ou sommes de contrôle publiées par paquet livré, une description de la méthode et un exemple issu d'une version réelle, ainsi que des instructions destinées au client pour effectuer la vérification. Pour les petites équipes, un fichier de somme de contrôle signé à côté du téléchargement plus un paragraphe dans les notes de version suffisent.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SM-7** **Les environnements utilisés pour le développement, la compilation et les tests sont protégés contre les accès non autorisés et contre toute altération du code source, des outils de compilation et des artefacts.**

Comment le prouver: Concept de contrôle d'accès pour le dépôt, le serveur de compilation et les systèmes de test, listes d'accès avec la date de la dernière revue, journaux des modifications pertinentes pour la sécurité et preuve que les accès de production et de développement sont séparés. Sans service informatique interne, une connexion à double facteur, une branche principale protégée avec revue obligatoire et une revue semestrielle des personnes ayant encore accès suffisent.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SM-8** **Les clés privées utilisées pour signer les livraisons sont protégées contre la divulgation et l'usage abusif, et leur utilisation est restreinte aux personnes et systèmes autorisés.**

Comment le prouver: Description du stockage, de l'accès, du renouvellement et de la révocation des clés, preuve d'un stockage protégé tel qu'un jeton matériel ou un service de gestion de clés, plus des journaux des opérations de signature. Une petite organisation conserve la clé de signature sur un jeton matériel, documente les deux personnes ayant accès et tient une procédure prête pour le cas de perte.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SM-9** **Pour les composants achetés ou adoptés, y compris les logiciels open source, les attentes de sécurité placées sur le fournisseur sont définies et appliquées lors de la sélection.** Document

Comment le prouver: Exigences de sécurité dans les cahiers des charges ou contrats fournisseurs, critères de sélection pour les composants tiers, un inventaire de tous les composants tiers avec version et origine, plus l'évaluation du respect des attentes par le fournisseur. Sans service achats, une liste de composants tenue à jour avec une colonne indiquant si les mises à jour de sécurité et les canaux de signalement du fournisseur ont été vérifiés suffit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SM-10** **Les composants développés sur commande par un tiers sont soumis aux mêmes exigences de sécurité que le développement interne, et le respect de ces exigences est vérifié.**

Comment le prouver: Bon de commande ou documents contractuels indiquant les obligations de sécurité exigées, preuves fournies par le prestataire sur les pratiques appliquées, procès-verbaux de réception et résultats de vos propres contrôles sur le travail livré. Sans budget d'audit, une garantie contractuelle, la transmission des résultats de test du prestataire et un contrôle par sondage effectué avant la réception suffisent.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SM-11** **Les constats liés à la sécurité provenant de toutes les sources, tests, revues, signalements d'utilisateurs et notifications de tiers, sont consignés, évalués quant à leur impact, dotés d'un responsable et d'une échéance, et suivis jusqu'à leur clôture.** Document

Comment le prouver: Système de défauts ou de tickets avec un marqueur dédié aux sujets de sécurité, et pour chaque entrée l'évaluation d'impact, le responsable, l'échéance et la note de clôture, plus un rapport sur les points ouverts. Une petite équipe utilise une étiquette dans le système de tickets existant et un point permanent à l'ordre du jour de la réunion hebdomadaire.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SM-12** **Avant la publication d'un produit, il est vérifié et prouvé que les étapes prévues du cycle de vie de développement sécurisé ont bien été réalisées et que les enregistrements associés ont été produits.** Document

Comment le prouver: Revue de publication pour chaque version, comparée aux étapes du processus, avec des références aux enregistrements correspondants et une décision de publication documentée avec date et signature. Dans la pratique, une liste de contrôle de publication n'autorisant aucune livraison sans cases entièrement cochées fonctionne bien ; les points ouverts sont justifiés et assortis d'une date.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SM-13** **Le cycle de vie de développement sécurisé lui-même est régulièrement remis en question et amélioré, en s'appuyant sur les enseignements tirés des incidents, des résultats de tests, des retours clients et de l'évolution du paysage des menaces.**

Comment le prouver: Enregistrements de la revue de processus, par exemple une revue de direction ou une rétrospective, avec les changements de processus déclenchés, leur état de mise en œuvre et une référence à la cause racine. Quiconque utilise les niveaux de maturité de la norme consigne l'état actuel et la cible pour chaque pratique ; le niveau de maturité 4 exige précisément cette preuve d'amélioration continue. Pour une petite organisation, une réunion par an avec compte rendu et trois améliorations concrètes suffit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

## 6 Pratique 2 : Spécification des exigences de sécurité (SR) 5

**SR-1** **Le contexte d'utilisation prévu du produit est décrit : environnement d'exploitation attendu, mesures de sécurité supposées être fournies par cet environnement, groupes d'utilisateurs et rôles prévus, limites de confiance supposées, et les usages pour lesquels le produit n'est explicitement pas destiné.** Document

Comment le prouver: Une description du contexte de sécurité du produit, soit sous forme de document autonome, soit comme section fixe du cahier des charges du produit, couvrant l'environnement réseau, les protections externes supposées telles qu'un pare-feu ou un contrôle d'accès physique, une liste des rôles, et une liste explicite des usages hors périmètre. Une petite organisation limite cela à deux pages, ajoute un schéma simple de l'environnement d'installation, et fait dater et approuver le document par le responsable produit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SR-2** **Un modèle de menaces existe pour le produit, qui cartographie les flux de données, les interfaces, les limites de confiance et les chemins d'attaque, nomme les menaces qui en résultent et leur impact possible, et attribue des contre-mesures. Il est revu et actualisé lors de changements pertinents et au moins une fois par version du produit, et les points ouverts sont suivis jusqu'à leur clôture.** Document

Comment le prouver: Modèle de menaces avec un diagramme de flux de données, une liste des menaces par interface, les contre-mesures attribuées et le statut des points ouverts, plus un historique des révisions avec date et auteur. Une petite organisation peut travailler à partir d'un tableau par interface, avec des colonnes pour ce qui pourrait mal tourner, la gravité que cela aurait, ce qui est fait pour y remédier, et qui le revoit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SR-3** **Les exigences de sécurité du produit sont définies et documentées. Elles couvrent les résultats du modèle de menaces, le contexte de sécurité du produit décrit, les obligations légales et contractuelles applicables et le niveau de sécurité visé, et elles incluent les capacités de sécurité que le produit lui-même doit fournir.** Document

Comment le prouver: Liste d'exigences ou outil de gestion des exigences avec un identifiant unique par exigence, la source de chaque entrée telle qu'une menace, un contrat client ou une obligation légale, et le niveau de sécurité visé. Une petite organisation gère cela sous forme d'un tableau unique avec une colonne d'identifiant fixe à laquelle la vérification et les tests se rattachent ensuite.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SR-4** **Chaque exigence de sécurité individuelle est formulée de manière à être non ambiguë, exempte de contradictions, vérifiable et traçable jusqu'à une fonction ou une interface précise du produit, et elle porte les informations nécessaires pour la vérifier ultérieurement sans clarification supplémentaire.**

Comment le prouver: Un échantillon de la liste des exigences montrant, pour chaque exigence, un critère d'acceptation mesurable et la fonction ou l'interface concernée, ainsi que la correspondance entre exigence et cas de test. Une petite organisation vérifie cela à l'aide d'un modèle de formulation fixe et de la question de contrôle consistant à savoir si un cas de test peut être rédigé à partir de l'exigence sans avoir besoin de demander des précisions.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SR-5** **Les exigences de sécurité sont revues avant d'être utilisées dans la conception et la mise en œuvre, avec la participation des parties concernées, telles que le développement, les tests, la responsabilité produit et, si utile, les ventes ou le client. La revue couvre l'exhaustivité par rapport au modèle de menaces et au contexte de sécurité du produit, l'exactitude et la vérifiabilité. Les constats sont consignés et suivis jusqu'à leur clôture.**

Comment le prouver: Compte rendu de revue avec date, participants et leurs rôles, la version des exigences revue, une liste de constats avec un responsable et un statut de clôture, et une note d'approbation. Une petite organisation gère cela comme une revue à deux personnes entre le développement et les tests, avec un compte rendu court et une ligne d'approbation dans la liste des exigences.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

## 7 Pratique 3 : Sécurité dès la conception (SD) 4

**SD-1** **Chaque produit dispose d'une description de conception qui recense les aspects pertinents pour la sécurité de l'architecture : quels composants existent, comment ils communiquent entre eux, où passent les limites de confiance, quelles interfaces externes sont exposées et par quels mécanismes les exigences de sécurité définies précédemment sont réalisées dans la conception.** Document

Comment le prouver: Document d'architecture ou spécification de conception contenant un diagramme montrant les composants, les flux de données et les limites de confiance, plus un tableau de correspondance entre chaque exigence de sécurité et l'élément de conception qui la met en œuvre. Un petit fournisseur se contente d'un diagramme tenu à jour plus deux ou trois pages d'explication ; l'important est qu'il soit versionné dans le dépôt et mis à jour à chaque changement d'architecture.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SD-2** **La conception est analysée systématiquement à la recherche de menaces. L'analyse nomme les objectifs de l'attaquant, les limites de confiance et interfaces concernées, les menaces qui en résultent avec leur évaluation, et les contre-mesures retenues dans la conception. Elle est répétée à chaque changement significatif de l'architecture ou de l'environnement, et les menaces identifiées sont suivies jusqu'à ce qu'une décision ait été prise pour chacune d'elles.** Document

Comment le prouver: Modèle de menaces par produit ou par version majeure, par exemple un tableau avec des colonnes pour la menace, l'interface concernée, l'évaluation, la contre-mesure et le statut, ainsi que le compte rendu de la séance de modélisation indiquant les participants et la date. Une petite équipe modélise de façon pragmatique lors d'un atelier de deux à trois heures en suivant le diagramme d'architecture, et consigne les points ouverts sous forme de tickets, de sorte que la preuve de suivi est produite sans effort supplémentaire.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SD-3** **La conception suit de manière démontrable des principes de conception sécurisée reconnus, parmi lesquels le moindre privilège, la surface d'attaque minimale, la défense en profondeur, les valeurs par défaut sécurisées, un comportement sûr en cas de défaillance et des mécanismes de sécurité aussi simples et vérifiables que possible. L'application de ces principes est visible dans la conception et justifiée.**

Comment le prouver: Une section de la description de conception ou une directive de conception interne nommant les principes, plus des preuves concrètes par principe dans le produit, comme la matrice des privilèges des services, la liste des ports ouverts avec justification, les valeurs par défaut à la livraison ou le comportement documenté de gestion des erreurs. Un petit fournisseur utilise une courte liste de contrôle de ces principes comme point fixe dans la revue de conception et archive la fiche remplie avec la conception.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

**SD-4** **La conception est revue par des pairs qualifiés avant le début de la mise en œuvre. La revue couvre l'exhaustivité par rapport aux exigences de sécurité, l'exactitude et l'efficacité des mécanismes de sécurité et les résultats de l'analyse de menaces. Des personnes ayant une compétence suffisante en sécurité y participent, les constats sont consignés et suivis jusqu'à leur clôture.** Document

Comment le prouver: Compte rendu de revue avec date, élément revu et sa version, participants et leurs rôles, liste des constats avec statut et la décision de publication. Une petite équipe rattache la revue à la pull request des documents de conception et laisse les constats sous forme de commentaires avec une note de clôture, ce qui prouve le suivi sans outillage supplémentaire. Lorsque la compétence en sécurité fait défaut en interne, faire appel à un relecteur externe rémunéré à l'heure pour les conceptions critiques est la solution pragmatique.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

## 8 Pratique 4 : Mise en œuvre sécurisée (SI) 2

**SI-1** **Il existe un processus défini pour vérifier la mise en œuvre réelle par rapport à la conception sécurisée : la revue confirme que les mesures de protection prévues dans la conception sont réellement présentes et efficaces dans le code, que la défense en profondeur est préservée, et qu'aucune nouvelle vulnérabilité n'a été introduite pendant la mise en œuvre. La revue est réalisée par du personnel dûment qualifié, et tout écart constaté est consigné et suivi jusqu'à sa clôture.**

Comment le prouver: Une procédure écrite pour la revue de mise en œuvre, accompagnée de comptes rendus de revue par composant ou par version : le module revu, la référence au document de conception, la date, le relecteur, les constats et leur statut de résolution. Comme preuves adaptées figurent les revues de pull request avec une liste de contrôle de sécurité obligatoire, les résultats d'analyse statique de code avec une évaluation documentée de chaque alerte, et les comptes rendus des séances de revue. Une petite équipe couvre cela avec le principe des quatre yeux, un modèle de revue conservé dans le dépôt dans lequel chaque mesure de conception est cochée individuellement, et un ticket par constat ouvert. Le point essentiel est que l'auteur du code ne soit jamais le relecteur de ce même code.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

**SI-2** **Des règles de codage sécurisé contraignantes s'appliquent à tous les travaux de développement liés à la sécurité et couvrent au minimum l'évitement des constructions et fonctions connues comme non sûres, le traitement des entrées et des erreurs, la gestion de la mémoire et des ressources, et l'utilisation de code de sécurité éprouvé plutôt que d'implémentations maison. Les règles s'appliquent par langage de programmation utilisé, sont connues de tous les développeurs, et sont mises à jour en cas de besoin, par exemple lorsque de nouveaux schémas d'attaque ou de nouveaux outils apparaissent.** Document

Comment le prouver: Une norme de codage sécurisé approuvée avec statut de version, périmètre par langage et date d'approbation, complétée par la preuve qu'elle s'applique réellement au travail quotidien : la configuration des linters et outils d'analyse dans le dépôt, une règle de compilation qui fait remonter les infractions, et la liste de présence de la session d'information. Les petites organisations n'écrivent pas une norme à partir de zéro ; elles déclarent contraignant un ensemble de règles publiques déjà établi, y ajoutent une courte liste de règles complémentaires propres, et ancrent le contrôle dans le pipeline afin que le respect soit démontré automatiquement.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

## 9 Pratique 5 : Vérification et validation de la sécurité par les tests (SVV) 5

**SVV-1** **Chaque exigence produit liée à la sécurité se voit attribuer au moins un cas de test, démontrant que la fonction de protection fonctionne comme prévu en exploitation normale, qu'elle se comporte comme spécifié en cas d'entrée invalide ou d'usage abusif, et que les paramètres par défaut livrés avec le produit correspondent à l'état sécurisé. L'exécution et le résultat sont consignés pour chaque version logicielle testée.** Document

Comment le prouver: Une matrice de traçabilité reliant exigence, cas de test et résultat, plus des journaux de test indiquant la date, la version ou le build testé, et le nom de la personne ayant réalisé le test. Un petit fournisseur ajoute simplement une colonne d'identifiant de cas de test à sa liste d'exigences et archive le journal de sortie de l'exécution automatisée des tests du pipeline de compilation comme fichier joint à la version correspondante.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SVV-2** **Les contre-mesures issues du modèle de menaces sont testées spécifiquement afin de confirmer qu'elles ferment réellement le chemin d'attaque supposé. Les tests sont effectués contre les menaces identifiées, et pas seulement contre un usage conforme, et les points ouverts sont intégrés au processus de gestion des défauts.**

Comment le prouver: Des cas de test qui référencent directement les entrées du modèle de menaces, par exemple un cas d'abus par identifiant de menace avec le comportement défensif attendu, ainsi que les journaux de ces exécutions. Sans dispositif lourd, il suffit d'ajouter au modèle de menaces une colonne référençant le cas de test et la date de la dernière vérification réussie.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SVV-3** **Le produit est examiné systématiquement à la recherche de vulnérabilités avant sa publication. Le périmètre couvre au minimum : l'examen des interfaces et services accessibles depuis l'extérieur, des tests avec des entrées malformées et mutées de façon aléatoire, la vérification des composants tiers utilisés au regard des vulnérabilités connues et signalées, et un contrôle des classes de faiblesses connues dans le code propre du fournisseur. Les constats sont consignés avec leur évaluation.** Document

Comment le prouver: Rapports des outils utilisés, indiquant le nom de l'outil, sa version et l'état des données de la base de vulnérabilités, journaux de fuzzing, une liste des composants tiers avec la date de la dernière comparaison, et la liste des constats avec évaluation et décision. Un petit fournisseur combine des outils standards gratuits, une analyse des dépendances et une analyse des ports et services sur le produit installé, et archive les résultats par version dans un dossier.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SVV-4** **Le candidat à la publication est soumis à une tentative d'attaque en conditions réalistes qui cherche activement à contourner les mécanismes de protection plutôt que de simplement les interroger. Le périmètre, les conditions limites et les bornes du test sont convenus à l'avance, et les faiblesses constatées sont traitées et suivies comme des défauts.**

Comment le prouver: La commande ou le mandat de test indiquant le périmètre et l'environnement de test, un rapport couvrant la démarche, les faiblesses exploitées et leur évaluation, plus les entrées dans le système de défauts ou de tickets avec la preuve de la correction ou d'une acceptation de risque justifiée. Les petits fournisseurs achètent généralement ce test à l'extérieur dans un budget de temps limité, ou le font réaliser par une personne n'ayant pas développé le produit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SVV-5** **L'indépendance du personnel de test est définie et adaptée au niveau de maturité visé. Quiconque a développé un composant ne le publie pas sur la seule base de ses propres tests, et à mesure que le niveau de maturité augmente, les tests relèvent d'une unité organisationnellement distincte ou d'un tiers externe. L'attribution réelle est traçable pour chaque test.**

Comment le prouver: Une définition des rôles au sein du processus de développement montrant la séparation entre la création et les tests, plus, pour chaque exécution ou rapport de test, le nom et le rôle enregistrés de la personne ayant réalisé le test. Une entreprise de deux personnes gère cela par une revue mutuelle avec une note documentée selon le principe des quatre yeux, et fait appel à une personne externe pour les tests de sécurité approfondis.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

## 10 Pratique 6 : Gestion des défauts de sécurité (DM) 6

**DM-1** **Il existe un canal défini par lequel les signalements de faiblesses de sécurité dans le produit sont reçus et consignés depuis toutes les directions : de l'équipe de développement elle-même, des tests et des revues, des clients et intégrateurs, de déclarants externes, et des avis concernant les composants tiers et open source utilisés. Le canal de signalement est repérable par des tiers, et chaque signalement est consigné avec sa date de réception et sa source.** Document

Comment le prouver: Une description du canal de signalement, le point de contact accessible publiquement (une page sécurité, un fichier security.txt, ou une boîte mail telle que security@), et le registre d'entrée listant la date, la source et une brève description pour chaque signalement. Une petite organisation peut fonctionner avec une boîte mail partagée et une seule feuille de calcul ou étiquette de ticket, à condition que chaque signalement y aboutisse, y compris ceux évoqués dans le chat interne des développeurs.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**DM-2** **Chaque signalement entrant est trié et examiné afin de déterminer s'il est pertinent pour la sécurité et quels produits, versions et composants il concerne. Les signalements qui s'avèrent non pertinents pour la sécurité, ou non applicables, sont également clôturés avec un motif indiqué plutôt que silencieusement écartés.**

Comment le prouver: Une note de tri pour chaque signalement indiquant le résultat (pertinent pour la sécurité, oui ou non), les versions concernées, et le motif de rejet le cas échéant, visible dans le ticket ou dans la liste d'entrée. Les équipes ayant un faible volume de signalements peuvent effectuer le tri lors d'une courte session récurrente et consigner le résultat en deux phrases par entrée.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**DM-3** **Les défauts de sécurité confirmés sont évalués selon une méthode cohérente : cause racine, versions et configurations concernées, impact potentiel sur l'exploitation et la sécurité, exploitabilité, et gravité au regard d'une échelle définie. Le résultat de l'évaluation est consigné et traçable.** Document

Comment le prouver: Un enregistrement d'évaluation ou un ensemble de champs de ticket pour chaque défaut couvrant la cause racine, la gravité et l'échelle appliquée (par exemple un système de notation courant avec un vecteur documenté), ainsi que la liste des versions concernées. Les petites équipes peuvent s'appuyer sur un modèle de champs fixe dans le système de tickets plus une demi-page décrivant l'échelle et les seuils déclenchant une action immédiate.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**DM-4** **Pour chaque défaut de sécurité évalué, une décision est prise sur la manière dont il sera traité : correction, mesure compensatoire, ou acceptation justifiée du risque. La décision découle de la gravité, elle est confiée à une personne responsable avec une échéance, et le défaut est suivi jusqu'à sa clôture.** Document

Comment le prouver: Une liste d'actions ou un statut de ticket indiquant le responsable, la date cible, le type de mesure et une note de clôture, relié à la base de code ou à la version dans laquelle la correction prend effet. Les risques résiduels acceptés nécessitent une brève justification écrite approuvée par la responsabilité produit. Une petite organisation peut tenir cela dans un tableau de tickets avec des échéances, sans outillage supplémentaire.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**DM-5** **Les utilisateurs concernés, les intégrateurs et les autres parties prenantes sont informés des défauts de sécurité dès que l'évaluation l'exige, en indiquant les versions concernées, l'impact, et la correction ou mesure compensatoire disponible. Les délais et le périmètre des destinataires de cette communication sont définis à l'avance, tout comme l'approche pour les signalements de tiers assortis de leur propre délai de divulgation.**

Comment le prouver: Avis ou bulletins de sécurité publiés comportant une date et une référence de version, la liste de diffusion ou le canal d'abonnés, et la règle écrite relative aux délais et à la divulgation coordonnée. Les fournisseurs ayant peu de clients peuvent se contenter d'un envoi unique à une liste de clients tenue à jour plus une page d'avis datée dont les modifications sont versionnées.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**DM-6** **Le traitement des défauts de sécurité est revu à intervalles fixes. La revue examine les cas ouverts et en retard, le délai entre le signalement et la correction, les causes racines récurrentes, et l'efficacité des mesures prises. Les améliorations de processus qui découlent de la revue sont mises en œuvre et leur mise en œuvre est suivie.** Document

Comment le prouver: Compte rendu de la revue périodique avec date, participants, chiffres sur les cas ouverts et en retard, et une liste des améliorations convenues avec responsable et échéance. Une petite organisation peut rattacher ce point à une réunion trimestrielle existante et conserver les chiffres et décisions sur une seule page.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

## 11 Pratique 7 : Gestion des mises à jour de sécurité (SUM) 5

**SUM-1** **Chaque mise à jour de sécurité du produit est vérifiée par rapport aux versions du produit et environnements d'exploitation pris en charge avant sa publication aux clients, et il existe un enregistrement montrant que la mise à jour ferme la vulnérabilité sans perturber le fonctionnement prévu du produit.** Document

Comment le prouver: Enregistrement de test par correctif couvrant la version du produit testée, la plateforme, les cas de test (efficacité contre la vulnérabilité plus non-régression des fonctions principales) et l'approbation de publication. Un petit fournisseur peut se contenter d'une courte entrée d'approbation de correctif dans le ticket : identifiant du ticket, vérifié par, vérifié le, résultat, avec le journal de l'exécution de test automatisée joint.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SUM-2** **Pour tous les composants du produit qui n'ont pas été développés en interne (bibliothèques tierces, système d'exploitation, environnements d'exécution), il est défini et prouvé comment leurs mises à jour de sécurité sont évaluées et soit adoptées dans le produit, soit rejetées avec une justification documentée.** Document

Comment le prouver: Inventaire des composants tiers avec version et origine, plus une entrée d'évaluation par vulnérabilité tierce signalée indiquant la décision (adoption, non concerné, couvert par une mesure compensatoire) et la justification. Les petites équipes exécutent une analyse automatisée des dépendances dans la compilation et conservent les décisions sous forme de commentaires sur le résultat de l'analyse ou dans une liste d'exceptions simplifiée.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SUM-3** **Pour chaque mise à jour de sécurité livrée, les utilisateurs reçoivent des informations d'accompagnement compréhensibles : quelles versions du produit sont concernées, quelle vulnérabilité est corrigée, quelle est sa gravité, si des effets secondaires ou des mesures compensatoires doivent être observés, et comment installer la mise à jour.** Document

Comment le prouver: Avis de sécurité ou notes de version publiés indiquant l'identifiant de la vulnérabilité, les versions concernées, l'évaluation de gravité, les étapes d'installation et les indications pour revenir à l'état précédent. Les petits fournisseurs tiennent une page publique unique avec une liste chronologique des avis de sécurité et y renvoient depuis le produit lui-même.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SUM-4** **Il existe une voie définie et protégée contre les altérations par laquelle les utilisateurs obtiennent les mises à jour de sécurité, et l'authenticité et l'intégrité d'une mise à jour peuvent être vérifiées côté utilisateur avant son installation.**

Comment le prouver: Description du canal de livraison (zone de téléchargement, serveur de mise à jour, support physique) ainsi que ses mesures de protection, plus la signature numérique ou la somme de contrôle par paquet et des instructions indiquant à l'utilisateur comment la vérifier. Les petits fournisseurs y parviennent en signant sur le serveur de compilation, en publiant la somme de contrôle à côté du téléchargement et en désignant un emplacement clair où la clé publique est conservée.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

**SUM-5** **Des objectifs de délai définis existent pour la mise à disposition des mises à jour de sécurité, gradués selon la gravité de la vulnérabilité ; les délais réellement atteints sont suivis, et tout objectif manqué est justifié et accompagné d'une mesure provisoire pour les utilisateurs.** Document

Comment le prouver: Spécification interne avec une fenêtre de temps par catégorie de gravité (par exemple critique <= 30 jours, élevée <= 90 jours) et une évaluation par vulnérabilité : date de signalement, date de publication du correctif, jours écoulés, motif de l'écart. Les petits fournisseurs conservent cela sous forme de deux champs de date dans le ticket de vulnérabilité et revoient la liste une fois par trimestre plutôt que de mettre en place un système de métriques dédié.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

## 12 Pratique 8 : Lignes directrices de sécurité pour le déploiement et l'exploitation du produit (SG) 7

**SG-1** **Chaque produit est accompagné d'une description de sa stratégie de défense en profondeur : elle nomme les couches de protection intégrées au produit lui-même, les met en correspondance avec les menaces qu'elles contrent, et montre quel effet protecteur ne résulte que de l'interaction de plusieurs couches.** Document

Comment le prouver: Une section dans la documentation du produit livrée, ou un concept de sécurité séparé, qui indique pour chaque couche de protection le mécanisme, la menace couverte et les limites de son effet. Une petite organisation conserve cela sous forme d'un tableau de deux pages : colonne couche de protection, colonne menace tirée de son propre modèle de menaces, colonne risque résiduel. Un renvoi croisé au modèle de menaces de SR-2 suffit, le contenu n'a pas à être tenu à jour en double.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

**SG-2** **La documentation nomme les mesures de sécurité que le produit ne fournit pas lui-même mais attend de l'environnement de déploiement, par exemple la segmentation réseau, des pare-feu en amont, un contrôle d'accès physique ou un service d'horodatage externe, et indique clairement que le niveau de sécurité garanti n'est pas atteint sans ces mesures.** Document

Comment le prouver: Un chapitre de prérequis de déploiement dans le manuel, ou un schéma d'architecture de référence avec zones et conduits dans lequel les mesures à fournir par le propriétaire de l'actif sont explicitement indiquées. Une liste d'hypothèses sur l'environnement s'est révélée utile en pratique, tirée directement du contexte de sécurité du produit et relue à chaque version du produit.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

**SG-3** **Il existe un guide de configuration de référence sécurisée qui recense tous les paramètres, services, ports et interfaces pertinents pour la sécurité, indique l'état recommandé à la livraison et décrit l'impact d'un écart par rapport à cette recommandation.** Document

Comment le prouver: Guide de durcissement avec un tableau de paramètres : paramètre, valeur recommandée, effet, effet secondaire en cas d'écart. Plus la liste des services et ports actifs dans la configuration par défaut avec une justification de leur maintien activé. Une petite équipe conserve ce tableau juste à côté du fichier de configuration dans le dépôt et l'exporte dans la documentation de livraison, afin qu'il reste aligné avec le produit.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

**SG-4** **Pour l'exploitation continue, il existe un guide décrivant comment le produit est exploité de manière sécurisée, surveillé et maintenu dans son état sécurisé, y compris la sauvegarde et la restauration, la journalisation et le traitement des messages d'événements pertinents pour la sécurité.** Document

Comment le prouver: Guide d'exploitation avec des sections sur la journalisation, les sauvegardes, le redémarrage et les messages d'événements. Comme preuve complémentaire, une liste des messages pertinents pour la sécurité émis par le produit, chacun accompagné d'une courte action recommandée, afin que le propriétaire de l'actif n'ait pas à les interpréter seul.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

**SG-5** **La documentation explique comment les comptes utilisateurs, les rôles et les permissions du produit sont configurés et maintenus, en particulier la séparation des rôles, le changement des identifiants par défaut et la suppression des comptes qui ne sont plus nécessaires.** Document

Comment le prouver: Un chapitre de gestion des comptes avec une vue d'ensemble des rôles et des droits attribués à chaque rôle, plus une note explicite sur les identifiants par défaut et leur changement lors de la mise en service. Une courte liste de contrôle de mise en service dans le manuel fonctionne bien en pratique, que le propriétaire de l'actif peut cocher et archiver.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

**SG-6** **Il existe un guide de mise hors service sécurisée qui décrit la suppression complète des données sensibles du produit, telles que les identifiants, les clés, les données de configuration et les journaux, avant que l'appareil ne soit transmis, réutilisé ou mis au rebut.** Document

Comment le prouver: Une section de mise hors service recensant tous les emplacements de stockage de données sensibles à l'intérieur du produit et la procédure d'effacement correspondante, y compris les cas où l'effacement est techniquement impossible et où le matériel doit être physiquement détruit. Une liste des stockages persistants tirée de la description d'architecture est utile ici, elle évite qu'un emplacement de stockage ne soit oublié.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

**SG-7** **La documentation de sécurité livrée aux utilisateurs est revue avant publication : elle est techniquement correcte, cohérente avec la version du produit livrée, complète par rapport au contenu prévu et compréhensible pour le public visé, et elle est mise à jour à chaque changement du produit.**

Comment le prouver: Un enregistrement de revue par document et par version de produit avec relecteur, date, constats et leur clôture, relié à l'approbation de publication. Une petite organisation résout cela avec le principe des quatre yeux dans la pull request de documentation : un développeur vérifie le contenu technique, une seconde personne vérifie la compréhensibilité, et l'approbation est consignée dans le ticket. Une version n'est livrable qu'une fois la revue documentée.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification