AYI NEDJIMI Consultants

Gestion vulnérabilités en environnement industriel et OT

Catégorie : Sécurité Industrielle OT/ICS Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Guide gestion des vulnérabilités OT : priorisation SSVC, patch management industriel, mesures compensatoires et workflow adapté aux contraintes ICS.

Résumé exécutif

La gestion des vulnérabilités en environnement industriel se heurte à des contraintes sans équivalent dans le monde IT qui rendent les approches traditionnelles de patch management inapplicables. L'impossibilité de patcher un automate sans arrêter le processus de production qu'il pilote, les firmwares obsolètes pour lesquels aucun correctif n'est disponible, et les systèmes legacy en fin de vie du constructeur mais toujours en service critique imposent une méthodologie fondamentalement différente. Ce guide propose une approche adaptée combinant la priorisation par le risque réel via le framework SSVC plutôt que le score CVSS seul, des mesures compensatoires structurées documentées et vérifiables, et un processus de patch management rigoureusement aligné sur les cycles de maintenance industriels pour réduire efficacement et durablement l'exposition aux vulnérabilités des systèmes de contrôle industriels.

Les systèmes de contrôle industriels accumulent des vulnérabilités à un rythme alarmant. CISA a publié plus de 400 advisories ICS en 2025, ciblant des automates programmables, des logiciels SCADA, des passerelles de protocole et des commutateurs industriels. Chaque advisory représente potentiellement une porte d'entrée exploitable par les groupes de menaces ciblant les infrastructures critiques. Pourtant, le taux de remédiation des vulnérabilités OT reste dramatiquement inférieur à celui du parc IT. Les raisons sont structurelles : un automate pilotant un processus continu ne peut pas être arrêté pour appliquer un patch sans planification minutieuse et validation préalable, certains constructeurs ne fournissent plus de correctifs pour des équipements en production depuis plus de quinze ans, et les équipes OT privilégient légitimement la stabilité du processus sur la correction des vulnérabilités théoriques. Cette tension entre impératif de sécurité et contraintes opérationnelles nécessite une approche de gestion des vulnérabilités fondamentalement différente de celle appliquée aux systèmes informatiques, intégrant la priorisation par le risque réel, les mesures compensatoires structurées et un processus de patch management aligné sur les réalités de la production industrielle.

Priorisation des vulnérabilités OT avec SSVC

Le score **CVSS**, standard de l'industrie IT pour évaluer la sévérité des vulnérabilités, présente des limitations majeures en contexte OT. Un CVSS de 9.8 sur un automate isolé derrière trois niveaux de segmentation représente un risque bien moindre qu'un CVSS 7.5 sur un serveur SCADA

exposé sur la DMZ industrielle. Le contexte d'exploitation, absent du score CVSS, est déterminant en environnement OT où les mesures compensatoires architecturales réduisent significativement le risque réel.

Le framework **SSVC** (Stakeholder-Specific Vulnerability Categorization), développé par CISA et Carnegie Mellon, propose une approche décisionnelle adaptée aux contraintes OT. SSVC évalue chaque vulnérabilité selon quatre axes : l'exploitation active dans la nature (active, public PoC, aucune), l'automatisabilité de l'exploitation, l'impact technique (contrôle partiel ou total) et l'impact sur la mission (sûreté, production, environnement). La décision finale se traduit en quatre actions : Track (surveiller), Track* (surveiller avec attention), Attend (traiter lors de la prochaine maintenance) ou Act (traiter immédiatement). Cette approche, intégrée dans le workflow du SOC convergent IT/OT, permet des décisions de priorisation objectives alignées sur le risque réel.

La vulnérabilité CVE-2020-15782 affectant les automates Siemens S7-1200 et S7-1500, permettant l'exécution de code natif via un contournement du sandbox du firmware, illustre les enjeux de priorisation OT. Avec un score CVSS de 8.1, cette vulnérabilité nécessitait une mise à jour de firmware impliquant un arrêt de chaque automate. Les organisations ayant appliqué SSVC ont pu prioriser la correction des automates exposés (accessibles depuis la DMZ ou pilotant des systèmes de sécurité) tout en appliquant des mesures compensatoires réseau sur les automates isolés en attente de la prochaine fenêtre de maintenance planifiée.

Comment organiser le patch management industriel ?

Le **patch management OT** s'organise autour des cycles de maintenance industriels plutôt que des cycles de publication des correctifs. Les arrêts planifiés (arrêts annuels, semi-annuels ou trimestriels selon l'industrie) constituent les fenêtres d'opportunité pour appliquer les correctifs accumulés. Le processus suit une séquence stricte : inventaire des correctifs disponibles, évaluation de la compatibilité avec les configurations en place, test sur un environnement de qualification, préparation des procédures d'application et de rollback, puis exécution pendant l'arrêt planifié.

La phase de *qualification des correctifs* est critique et souvent sous-estimée. Un correctif firmware validé par le constructeur peut introduire des régressions avec les programmes automate spécifiques ou les configurations réseau du site. L'idéal est de disposer d'un **environnement de test OT** reproduisant l'architecture de production pour valider chaque correctif avant son déploiement. Les organisations ne disposant pas de cette infrastructure peuvent négocier avec les constructeurs l'accès à des rapports de qualification détaillés ou s'appuyer sur le retour d'expérience d'organisations du même secteur via les ISAC. La traçabilité de chaque opération de patching s'inscrit dans l'architecture de log management et rétention de l'organisation.

Type d'actif OT	Cycle de patching typique	Contrainte principale	Approche recommandée
PLC/RTU	Annuel (arrêt planifié)	Arrêt processus requis	SSVC + mesures compensatoires
HMI/SCADA serveur	Trimestriel	Qualification applicative	Patch management classique adapté
Commutateurs industriels	Semestriel	Interruption réseau	Redondance avant patching
Postes d'ingénierie	Mensuel	Compatibilité outils SCADA	Gestion standard avec validation
Passerelles protocole	Annuel	Test d'interopérabilité	Qualification complète requise

Mon avis : L'objectif de « patcher toutes les vulnérabilités critiques en 30 jours », transposé de l'IT à l'OT, est irréaliste et contre-productif. Il pousse les équipes OT soit à ignorer les directives de sécurité (car impossibles à respecter), soit à prendre des risques inconsidérés sur la production. Un objectif réaliste combine une remédiation immédiate par mesures compensatoires réseau (segmentation, surveillance renforcée) avec une application des correctifs lors de la prochaine fenêtre de maintenance planifiée, qualifiée et documentée.

Quelles mesures compensatoires quand le patch est impossible ?

Pour les systèmes legacy en fin de vie ou les automates dont le constructeur ne fournit plus de correctifs, les **mesures compensatoires** constituent la seule option de réduction du risque. La première mesure, et la plus efficace, est le renforcement de la segmentation réseau : réduire au strict minimum les dispositifs pouvant communiquer avec le système vulnérable, via des règles de pare-feu granulaires incluant un filtrage protocolaire profond. Un automate Modbus vulnérable mais accessible uniquement depuis le serveur SCADA principal via un pare-feu inspectant le contenu des trames présente un risque résiduel considérablement réduit.

La deuxième mesure compensatoire est la **surveillance renforcée** ciblée sur le système vulnérable. Des règles de détection spécifiques, créées selon les principes de détection engineering, surveillent les tentatives d'exploitation de la vulnérabilité identifiée. Les IOC publiés dans l'advisory ICS-CERT sont traduits en signatures IDS déployées sur les sondes surveillant le segment réseau concerné. La troisième mesure est la réduction de la surface d'attaque par la désactivation de toute fonction non strictement nécessaire sur le système vulnérable, limitant les vecteurs d'exploitation disponibles pour un attaquant. Le cadre Zero Trust formalise cette approche de minimisation des privilèges et des expositions réseau.

Pourquoi l'inventaire des actifs OT est le prérequis fondamental ?

Aucune gestion de vulnérabilités efficace n'est possible sans un **inventaire exhaustif et à jour** des actifs OT. Cet inventaire doit capturer, pour chaque dispositif, le constructeur, le modèle, la version de firmware, les protocoles de communication, les interconnexions réseau et la criticité pour le processus industriel. La corrélation automatisée entre cet inventaire et les advisories ICS-CERT permet d'identifier immédiatement les systèmes impactés par chaque nouvelle vulnérabilité publiée.

Les solutions de découverte passive comme Nozomi Networks et Claroty construisent et maintiennent automatiquement cet inventaire en analysant le trafic réseau OT. Ces plateformes identifient les dispositifs, extraient les versions de firmware via les protocoles industriels, cartographient les communications et corrèlent automatiquement les actifs découverts avec les bases de vulnérabilités. L'intégration avec les outils de gestion des actifs IT (CMDB) permet une vue unifiée du patrimoine technologique, essentielle pour les audits de conformité NIS 2 qui exigent une connaissance précise des systèmes d'information des entités essentielles incluant les composants OT.

Quel pourcentage de vos actifs OT est inventorié avec la version exacte de firmware actuellement en production ?

Comment intégrer la gestion des vulnérabilités OT dans le cycle DevSecOps industriel ?

L'émergence du concept de *DevSecOps industriel* applique les principes d'intégration continue de la sécurité au cycle de vie des systèmes de contrôle. Dès la phase de conception d'un nouveau projet d'automatisation, l'analyse des vulnérabilités connues des composants sélectionnés (PLC, logiciel SCADA, commutateurs) influence les choix architecturaux. Les spécifications de sécurité intègrent des exigences de maintenabilité : capacité de mise à jour du firmware sans arrêt complet du processus (redondance hot-standby), accès distant sécurisé pour le diagnostic et le patching, et compatibilité avec les outils de découverte et de surveillance de vulnérabilités.

Pendant la phase d'exploitation, le processus de **gestion des changements** (Management of Change, MOC) intègre systématiquement l'évaluation de l'impact sécurité. Toute modification de configuration, mise à jour logicielle ou ajout de composant fait l'objet d'une analyse de vulnérabilités avant déploiement. Les retours d'expérience des opérations de patching alimentent une base de connaissances qui améliore progressivement l'efficacité du processus. L'approche de threat hunting vérifie régulièrement que les mesures compensatoires déployées pour les vulnérabilités non patchées restent effectives face à l'évolution des techniques d'attaque.

Faut-il scanner activement les systèmes OT pour les vulnérabilités ?

Le **scan de vulnérabilités actif** en environnement OT reste un sujet controversé. Les scanners IT traditionnels (Nessus, Qualys) peuvent provoquer des dysfonctionnements sur les automates anciens sensibles au trafic réseau inhabituel. Les scans authentifiés, nécessitant des identifiants d'accès aux systèmes OT, élargissent la surface d'attaque si ces identifiants sont compromis. Néanmoins, le scan actif fournit une visibilité sur les vulnérabilités que la découverte passive ne peut identifier (versions de logiciels applicatifs, configurations de sécurité des postes Windows).

L'approche recommandée est un **modèle hybride** : découverte passive continue via les sondes OT pour l'inventaire et le suivi des versions firmware, complétée par des scans actifs ciblés et planifiés sur les systèmes qui le tolèrent (serveurs SCADA, postes d'ingénierie, commutateurs managés) pendant les fenêtres de maintenance. Les automates en production ne doivent jamais être scannés activement sauf dans un environnement de test isolé. Tenable.ot et Claroty xDome proposent des approches de scan adaptées aux contraintes OT, combinant requêtes protocolaires légères et analyse passive pour minimiser le risque d'impact sur les processus industriels. L'intégration des résultats de scan dans le processus SSVC automatise la priorisation des vulnérabilités nouvellement identifiées, permettant aux équipes de sécurité OT de concentrer leurs efforts sur les failles présentant le risque réel le plus élevé dans le contexte spécifique de chaque installation industrielle, en tenant compte des mesures compensatoires déjà en place et de la criticité du processus physique piloté par chaque système vulnérable identifié lors du scan.

Sources et références : CISA ICS · ANSSI

Comment mesurer l'efficacité du programme de gestion des vulnérabilités OT ?

L'efficacité du programme de gestion des vulnérabilités OT se mesure par des **indicateurs opérationnels adaptés** aux contraintes industrielles. Le taux de couverture de l'inventaire (pourcentage d'actifs OT inventoriés avec version de firmware connue) mesure la capacité à identifier les systèmes impactés par chaque nouvelle vulnérabilité. Le délai moyen de qualification (temps entre la publication d'un advisory et la décision SSVC pour chaque actif impacté) évalue la réactivité du processus de triage. Le taux de remédiation dans les délais cibles (mesures compensatoires dans les 72 heures, correctifs lors de la prochaine maintenance planifiée) mesure l'efficacité opérationnelle du programme.

Le *risque résiduel agrégé*, calculé en combinant le nombre de vulnérabilités non corrigées, leur score SSVC et l'efficacité des mesures compensatoires déployées, fournit une vue synthétique de l'exposition aux vulnérabilités du parc OT. Les rapports de Dragos et les études sectorielles fournissent des benchmarks permettant de comparer cette exposition avec celle d'organisations similaires, identifiant les axes d'amélioration prioritaires pour réduire le risque global pesant sur les systèmes de contrôle industriels et les processus physiques qu'ils pilotent au quotidien.

À retenir : La gestion des vulnérabilités OT repose sur un inventaire exhaustif des actifs, une priorisation par le risque réel (SSVC plutôt que CVSS seul), un patch management aligné sur les cycles de maintenance industriels, et des mesures compensatoires structurées pour les systèmes non patchables. L'objectif n'est pas le « zero vulnerability » mais la réduction continue de l'exposition aux risques les plus critiques dans les contraintes opérationnelles de l'environnement industriel.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr