COMMENT RÉDUIRE L'EXPOSITION AU RISQUE CYBER OT GRÂCE AU MAINTIEN EN CONDITION DE SÉCURITÉ ?

MISE EN PLACE **D'UN PROGRAMME DE REMÉDIATION EFFICACE EN MILIEU INDUSTRIEL**

GIMELEC

Nous décuplons les énergies

2025

TABLE **DES MATIÈRES**

REMERCIEMENTS

Le GIMELEC remercie Alexandre Delaby et Emmanuel Persichini pour leur patience à relire et leur partage de la vision de l'ANSSI.

Le GIMELEC remercie également les experts et professionnels du Club Cyber OT qui ont partagé leurs expertises, alimenté les réflexions et oeuvré à la création de ce document : Olivier Bohelay, Thierry Cornu, Olivier Cupif, Laurent Duquesne, Thomas Firmin, Éric Hervé, Thomas Guilloux, Florent Lefevre, Bruno Lignon, Pascal Nail, Pierre Paterni, Bernard Piqueras, Stéphane Potier.

Le GIMELEC remercie particulièrement Frédéric Bahuaud, Pablo Ramirez Garcia et Pascal Sitbon pour le temps et l'énergie qu'ils ont consacré à l'élaboration du présent livre blanc.

ÉDITO

À nous d'agir, ensemble

L'industrie 4.0 transforme en profondeur le paysage industriel, offrant des gains de performance majeurs grâce aux technologies numériques. Mais cette interconnexion accrue expose aussi les systèmes industriels à des cybermenaces sophistiquées, mettant en péril la continuité des opérations et la sécurité.

La convergence IT/OT amplifie ces vulnérabilités, rendant indispensable une cybersécurité intégrée dès la conception et tout au long du cycle de vie des systèmes. Face à ces défis, le GIMELEC et le CESIN unissent leurs forces pour structurer une réponse adaptée, en s'appuyant sur un Maintien en Condition de Sécurité (MCS) robuste, en phase avec la directive NIS 2 et le Cyber Resilience Act.

Ce livre blanc propose des solutions concrètes – bonnes pratiques, recommandations stratégiques et retours d'expérience – pour aider les industriels à renforcer la résilience de leurs infrastructures. Sécuriser notre industrie, c'est assurer sa compétitivité et sa souveraineté dans un monde où la cybersécurité est un enjeu stratégique.

Fabrice Bru,
Président du CESIN

Sécuriser l'industrie, c'est protéger son avenir

Le Maintien en Condition de Sécurité (MCS) est un levier essentiel pour assurer la pérennité des systèmes industriels face aux cybermenaces croissantes. Plus qu'une réponse technique, il implique une démarche continue, adaptée aux contraintes opérationnelles et aux évolutions réglementaires.

Fruit de 18 mois de travail collaboratif des meilleurs experts du Club Cyber OT du GIMELEC - en dialogue avec le CESIN - ce livre blanc fournit un cadre méthodologique structuré autour de quatre piliers : surveillance, identification des vulnérabilités, remédiation et amélioration continue. Il s'appuie sur une expertise de terrain pour offrir des recommandations pragmatiques et actionnables.

Garantir la sécurité des infrastructures industrielles exige une mobilisation collective et une approche concertée entre tous les acteurs. Ce document a vocation à guider les entreprises dans cette démarche stratégique, essentielle à la résilience et à la souveraineté numérique.

Yann Boujault,
Président du Club Cyber OT du GIMELEC

1 / INTRODUCTION

Les systèmes industriels modernes, notamment avec l'avènement de l'industrie 4.0, sont de plus en plus connectés, et donc plus vulnérables aux cyberattaques sophistiquées. En 2023, plus de 30 % des cyberattaques à travers le monde ont ciblé des infrastructures industrielles critiques, selon le rapport Fortinet (2023)[1]. Ces attaques, qui visent à la fois les environnements IT (Information Technology - informatique de gestion) et les systèmes OT (Operational Technology – informatique industrielle), représentent une menace croissante, tant pour la continuité des opérations que pour la sécurité des biens et des personnes.

Contrairement aux systèmes IT, où les priorités sont souvent la confidentialité et l'intégrité des données, les systèmes OT exigent avant tout la disponibilité des équipements et l'intégrité de leurs échanges, car une défaillance pourrait avoir des répercussions graves sur les processus physiques, et par exemple entraîner des interruptions majeures de production. Par conséquent, la gestion des vulnérabilités et des correctifs dans le monde OT présente des particularités bien différentes de celles du monde IT.

Les attaques ciblées (APT - Advanced Persistent Threats) sur des infrastructures industrielles ces dernières années ont montré une grande capacité à causer des dommages matériels considérables et à mettre en danger la vie des personnes. Parmi les incidents les plus marquants figurent des attaques comme NotPetya, qui ont paralysé des infrastructures critiques et causé des milliards de dollars de pertes financières. Cette menace constante a poussé les États à prendre des mesures réglementaires strictes pour protéger leurs infrastructures critiques, car leur bon fonctionnement est souvent essentiel à la stabilité d'un pays.

En réponse à ces menaces croissantes, la France a légiféré en 2013 avec la Loi de Programmation Militaire visant à protéger les infrastructures critique de la Nation pour les protéger de la menace étatique et des APT, ensuite la Directive NIS (Network and Information Security) adoptée en 2016[2] a marqué un tournant dans la régulation des infrastructures critiques en Europe. Elle demande aux opérateurs d'établir des politiques robustes de cybersécurité, notamment via le Maintien en Condition de Sécurité (MCS), mentionné dans la règle 4 de cette directive et dans la règle 16 de la Loi de Programmation Militaire (LPM). Cette approche est conçue pour garantir une protection continue des systèmes critiques.

Face à l'évolution des cybermenaces, la Directive NIS 2 a pour objectif de protéger le marché économique européen face à une menace de masse cybercriminelle croissante. Les articles 21 et 22 introduisent des mesures de gestion des risques cyber plus strictes au niveau européen, qui devront être transposées en droit français. Il est désormais impératif pour les entreprises de surveiller en continu l'apparition de nouvelles vulnérabilités (via des sources comme le CERT-FR) et proposer un plan de remédiation[3]. De plus, le Cyber Resilience Act (CRA), une réglementation européenne entrée en vigueur en 2024, prévoit de rendre les fournisseurs de technologies responsables de la cybersécurité de leurs produits tout au long de leur cycle de vie[3].

Pour aider les organisations industrielles à se conformer à ces exigences et à faire face à l'évolution rapide des cybermenaces, il est essentiel de mettre en œuvre un programme efficace de Maintien en Condition de Sécurité (MCS). Dans ce contexte, l'objectif de ce document est d'explorer les différents aspects du MCS afin d'assurer un haut niveau de résilience face aux risques cyber tout au long du cycle de vie des systèmes industriels. Nous examinerons à la fois les enjeux organisationnels et les défis techniques que rencontrent les systèmes industriels face aux nouvelles menaces et vulnérabilités, tout en proposant des recommandations pratiques basées sur des normes internationales et des retours d'expérience concrets.

Les standards internationaux tels que IEC- 62443 (notamment part 2 & part 3) ainsi que les guides publiés par NIST (NIST SP 800-40 Rev. 4 et NIST SP 800-82 Rev. 3), constituent des références incontournables pour la gestion de la sécurité dans les environnements industriels. De même, les recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) telles que les Mesures principales et détaillées fournissent des conseils pratiques pour sécuriser les systèmes d'information les plus critiques d'une entreprise.

Cependant, le secteur de la cybersécurité industrielle est confronté à un défi majeur : la pénurie de ressources humaines spécialisées. En 2023, la main-d'œuvre dédiée à la cybersécurité a augmenté de 10 %, mais le manque mondial de professionnels est estimé à 4 millions[4]. Cette pénurie complique la mise en œuvre des mesures de sécurité nécessaires pour les infrastructures industrielles.

[1] Global Threat Landscape Report 2H 2023 (fortinet.com)
[2] Directive - 2016/1148 - EN - EUR-Lex (europa.eu)
[3] La directive NIS 2 | ANSSI (cyber.gouv.fr)
[4] Cybersecurity Workforce Study 2023 (isc2.org)

Enfin, la question des assurances dans la gestion des cyber-risques évolue. Deux exemples illustrent le changement du rôle des assureurs : l'exemple de l'affaire Merck (2017), où la société a obtenu gain de cause en 2023 contre son assureur après l'attaque NotPetya[5] et plus récemment l'exemple de la décision de la Cour de Cassation en janvier 2025, suite à des escroqueries par phising, où les victimes d'arnaques portent leur responsabilité pleine et entière en cas de négligence grave (au sens cybersécurité)[6].

[5] Dans l'affaire NotPetya, Merck gagne en appel contre son assureur (lemondeinformatique.fr)
[6] Escroquerie bancaire - précisions quant aux conditions du remboursement du client par sa banque (courdecassation.fr)

2 SPÉCIFICITÉS DE L'ENVIRONNEMENT INDUSTRIEL

2.1 ÉTAT DE LA MENACE DANS LE MONDE INDUSTRIEL

ORIGINE DE LA MENACE DANS LE MONDE INDUSTRIEL

La menace cyber dans le monde industriel découle principalement des objectifs variés des attaquants, qui cherchent à exploiter les vulnérabilités des systèmes pour atteindre leurs propres motivations. Celles-ci peuvent inclure des actions de (hack)activisme, des motifs financiers, ou encore des intérêts géopolitiques. D'autres, par simple défi technique, cherchent à prouver qu'une faille existe et à en démontrer l'exploitation.

Ces dernières années, la menace s'est intensifiée dans le secteur industriel en raison de plusieurs facteurs. D'une part, le contexte géopolitique mondial a exacerbé les tensions entre États, entraînant une augmentation des cyberattaques soutenues par des acteurs étatiques ou parrainées par des gouvernements. D'autre part, l'appât du gain financier, notamment via des attaques par rançongiciels, a ciblé massivement les infrastructures industrielles, car une interruption des processus critiques exerce une pression considérable sur les victimes, qui se voient contraintes de payer pour éviter des pertes économiques majeures. Ces évolutions expliquent pourquoi l'industrie est devenue un terrain de prédilection pour une grande diversité d'attaquants cherchant à tirer parti de failles de sécurité dans des systèmes critiques.

Au-delà des motivations directes, les systèmes industriels représentent une cible de choix pour les attaquants en raison de leur fragilité inhérente. Les systèmes OT sont souvent basés sur des technologies plus anciennes, moins sécurisées, et difficiles à mettre à jour. Cette vulnérabilité structurelle augmente considérablement l'opportunité de succès pour un attaquant. La moindre perturbation dans ces environnements critiques peut entraîner des conséquences disproportionnées – que ce soit en termes d'arrêts de production, de dommages physiques ou de perturbations économiques – ce qui les rend particulièrement intéressants pour des attaques à grande échelle.

Enfin, il faut noter les capacités croissantes des acteurs malveillants, notamment avec l'apport de l'IA, pour s'attaquer aux systèmes industriels. La spécificité des systèmes OT n'est plus une protection contre les attaquants.

HISTORIQUE DES ATTAQUES DANS LE SECTEUR INDUSTRIEL

Les attaques cyber visant le secteur industriel ont progressivement évolué en ampleur et en sophistication, tirant parti des vulnérabilités spécifiques aux systèmes OT. Quelques-unes d'entre elles ont sans aucun doute marqué l'histoire des cyberattaques OT tant par leur impact que par les vecteurs d'attaques employés. Certaines de ces attaques sont détaillées en annexe I de ce document.

Les attaques observées dans l'industrie mettent en lumière la nécessité d'un maintien en condition de sécurité adapté aux systèmes OT, en tenant compte des vulnérabilités propres à ces environnements et des méthodes d'attaque en constante évolution.

Enfin, il faut noter les capacités croissantes des acteurs malveillants, notamment avec l'apport de l'IA, pour s'attaquer aux systèmes industriels. La spécificité des systèmes OT n'est plus une protection contre les attaquants.

TENDANCE EN FRANCE

En France, le paysage des menaces dans le secteur industriel a évolué rapidement. Selon l'ANSSI (Agence nationale de la sécurité des systèmes d'information), le nombre de cyberattaques contre des infrastructures critiques a augmenté de 255 % entre 2020 et 2021. Cette augmentation a été en grande partie attribuée à la numérisation croissante des industries et à l'interconnexion des systèmes OT avec des réseaux IT.

Publié en 2024, le « Rapport menaces et incidents »[7] de l'ANSSI indique qu'en 2023, l'ANSSI a observé des évolutions significatives dans les méthodes des cyberattaquants. Les opérations d'espionnage, qu'elles soient stratégiques ou industrielles, restent à un niveau élevé et ciblent de plus en plus les individus et les structures non gouvernementales manipulant des données sensibles. Les attaquants perfectionnent leurs techniques pour éviter d'être détectés.

Les attaques à but lucratif continuent également d'être fréquentes, avec des cybercriminels qui profitent d'outils largement disponibles pour viser des secteurs vulnérables, causant des interruptions d'activité et compromettant des données personnelles. Dans un contexte international tendu, les attaques de déstabilisation, en particulier les attaques DDoS, ont

[7] Rapport menaces et incidents - CERT-FR (ssi.gouv.fr)

augmenté, bien que leur impact soit limité. Des menaces d'opérations plus graves contre des infrastructures critiques européennes persistent, telles que la divulgation d'informations exfiltrées ou le sabotage.

Le temps moyen nécessaire pour corriger une faille de sécurité après sa détection doit impérativement être réduit, car il représente une fenêtre de vulnérabilité durant laquelle les organisations restent à la merci des attaques. Ces intrusions peuvent entraîner bien plus que des pertes financières immédiates : elles provoquent également des arrêts prolongés de production et perturbent gravement les chaînes d'approvisionnement, amplifiant ainsi leur impact.

SECTEURS, FRÉQUENCE ET TYPOLOGIE D'ATTAQUES

Malgré les efforts de sécurisation, les attaquants continuent de tirer parti de vulnérabilités non corrigées et de lacunes dans la gestion des systèmes d'information par les victimes. Cela contribue à une augmentation continue des risques cyber dans divers secteurs d'activité.

Le rapport « Threat Landscape 2024 »[8] de l'ENISA indique que les attaques ciblent principalement les secteurs de l'administration publique (19 %), des transports (11 %) et des finances (9 %). En parallèle, des secteurs comme l'infrastructure numérique (8 %) et les services aux entreprises subissent également des attaques fréquentes. Ces industries, du fait de leur criticité et de leur interconnexion, représentent des cibles de choix pour les attaquants cherchant à maximiser l'impact de leurs actions.

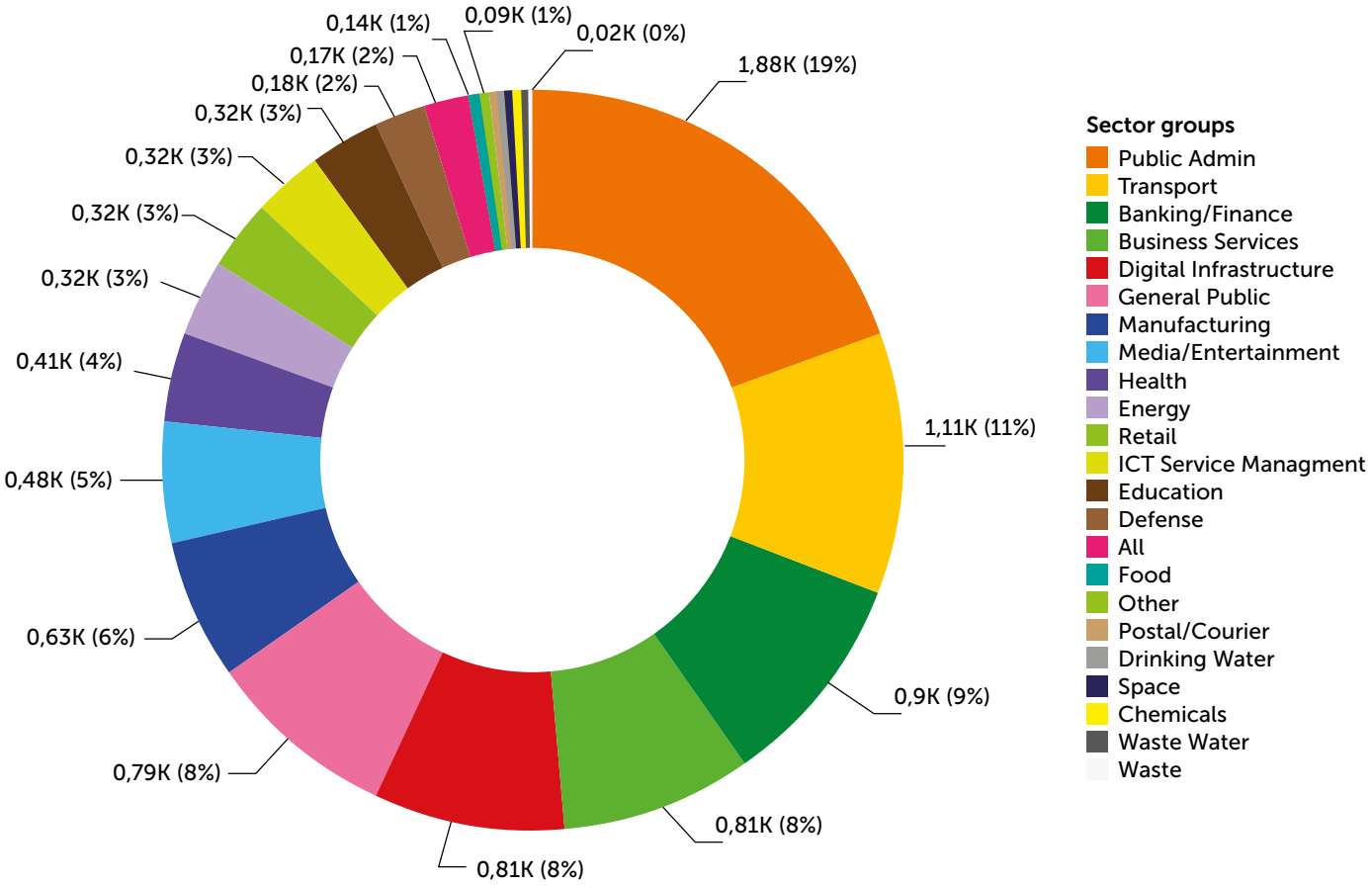


Figure 1 : Secteurs d'activité ciblés par nombre d'incidents[9]

[8] ENISA Threat Landscape 2024 — ENISA (europa.eu)
[9] ENISA Threat Landscape 2024 — ENISA (europa.eu)

Selon une étude de Fortinet[10], le nombre d'incidents a connu une forte augmentation : 31 % des entreprises interrogées ont déclaré avoir subi plus de 6 intrusions en 2023, contre seulement 11 % l'année précédente. Cette augmentation de la fréquence des attaques s'accompagne d'une intensification des conséquences, telles que la dégradation de la réputation des marques, qui touche 52 % des victimes, contre 34 % en 2023. La perte de données essentielles et de productivité est également en hausse, passant de 34 % à 43 % d'une année sur l'autre.

Le rapport ENISA 2023-2024 sur l'état de la menace cyber[11] révèle que 41,1 % des incidents de sécurité sont liés à des attaques de type DOS/DDOS/RDOS, tandis que 25,79 % sont des attaques par rançongiciels. Les incidents liés aux données (fuites, corruption) représentent environ 19,01 % des cas reportés. Ces statistiques soulignent la diversité des menaces et la nécessité d'adapter les mesures de défense à ces différentes typologies d'attaques.

Plus spécifiquement dans l'OT, Un nombre croissant de malwares conçus pour toucher les environnements industriels tel que INDUSTROYER.V2 et Pipedream émergent avec de nouvelles fonctionnalités et une nouvelle facilité de déploiement[12]. Cinq protocoles OT sont régulièrement ciblés : les protocoles utilisés dans les secteurs de l'automatisation industrielle et de l'énergie, comme Modbus (un tiers des attaques), suivis de près par Ethernet/IP, Step7, DNP3 (avec environ 18 % chacun) et IEC10X avec 10% des attaques. Les 2 % restants représentent de nombreux autres protocoles, dont la majorité est BACnet.

Ces exemples illustrent la diversité des attaques ciblant les systèmes industriels et permettent de tirer plusieurs conclusions essentielles pour la cybersécurité dans ce domaine :

- **Maintien en condition de sécurité :** la mise à jour continue des systèmes aide à réduire l'exposition aux vulnérabilités pour lesquelles des correctifs sont disponibles. Chaque jour, environ 100 nouvelles vulnérabilités sont publiées. Il est donc crucial de surveiller régulièrement son exposition et de prendre des mesures correctives pour limiter les risques.
- **Remédiation des vulnérabilités prioritaires :** il est impératif de corriger les vulnérabilités critiques dès leur découverte, en priorisant celles qui présentent le plus grand risque pour les systèmes. Une stratégie de remédiation rapide et ciblée permet de limiter les potentielles conséquences d'une attaque.
- **Surveillance des accès distants :** les accès distants aux infrastructures industrielles représentent un vecteur d'attaque particulièrement sensible. La mise en place de contrôles rigoureux et une surveillance accrue des connexions à distance sont essentielles pour limiter l'exposition des systèmes.
- **Communication et coordination entre acteurs du secteur :** une collaboration étroite entre les différents acteurs du secteur industriel est indispensable pour partager les informations et réagir rapidement face aux nouvelles menaces. Cette communication permet d'anticiper les risques et de bénéficier de retours d'expérience en cas d'attaque.
- **Protection des informations sensibles :** la protection des informations critiques est un pilier de la cybersécurité industrielle. Il est crucial de mettre en place des mesures de sécurité pour protéger les données sensibles contre les fuites et les exfiltrations malveillantes.

DIFFÉRENCES AVEC LES MENACES IT

Ces constats mettent en lumière trois particularités clés des cyberattaques sur les environnements industriels, distinctes de celles du domaine IT. Si certains vecteurs d'attaque sont communs, les conséquences dans l'industrie sont nettement plus graves, menaçant à la fois l'économie et la sécurité publique.

Dans l'industrie, les motivations des attaquants sont également plus diversifiées. Contrairement à l'IT, où les cybercriminels visent surtout des gains financiers (vol de données, rançongiciels), les attaques OT ont souvent des objectifs plus larges : sabotage, perturbations économiques ou encore espionnage industriel.

Enfin, la nature même de ces attaques varie profondément, reflétant les spécificités technologiques et les objectifs des environnements OT. Ces menaces, déjà complexes, deviennent encore plus redoutables avec la convergence croissante des systèmes IT et OT, ouvrant la voie à des attaques toujours plus sophistiquées.

[10] 2024 State of Operational Technology (fortinet.com)
[11] ENISA Threat Landscape 2024 (enisa.europa.eu)
[12] 2023 Global Threat Roundup Report: Trends in cyberattacks, exploits, and malware (forescout.com)

2.2 DIFFÉRENCES ENTRE LE MONDE IT ET OT

Les systèmes industriels, appelés aussi systèmes OT (Operational Technology), sont utilisés dans des secteurs comme l'énergie, les transports ou la production. Ils contrôlent des infrastructures et des processus physiques essentiels, qui exigent une disponibilité continue et ne tolèrent que peu, voire pas, d'interruptions. Un arrêt imprévu ou une défaillance peut entraîner des pertes financières, des dommages humains, matériels ou environnementaux, et même perturber des chaînes d'approvisionnement critiques comme l'eau, l'électricité, le gaz ou les transports.

Les systèmes de contrôle commande industriel (en anglais, ICS : Industrial Control System) répondent à des exigences strictes en matière de sûreté, fiabilité et performance.

Contrairement aux systèmes IT, qui se concentrent sur la gestion et la protection des données, les systèmes OT/ICS sont axés sur la gestion des processus physiques et des infrastructures critiques. Ils supervisent aussi les données nécessaires au pilotage industriel, tout en intégrant des éléments comme les systèmes de gestion technique des bâtiments (GTB/GTC) : contrôle d'accès, vidéosurveillance, chauffage, etc. De plus, les équipements IIoT (Industrial IoT), souvent délocalisés et exposés, ajoutent un niveau de risque. Une compromission de ces équipements peut directement affecter les processus industriels et la production.

La figure suivante illustre les différences fines de contextes et rôles de ces SI :

	SI IT	SI OT + Contrôle Commande
Objectifs du système	Traiter des données	Piloter des installations physiques, réguler des procédés, acquérir et traiter des données
Exigences fonctionnelles	Intégrité, confidentialité	Intégrité (sûreté de fonctionnement), disponibilité, traçabilité, temps-réel
Culture des intervenants	Informaticiens	Automaticiens, instrumentistes, mainteneurs
Environnement physique	Salles serveurs climatisées, bureaux	Ateliers de production (T°, humidité, vibrations, CEM, en extérieur, gaz)
Localisation géographique	Bureaux fermés, télétravail	Entrepôts, usines, voie publique, campagne, mer, air, montagne
Durée de vie	≈ 5 ans	10 à 40 ans
Gestion des incidents	Analyse post incident	Reproductibilité réduite
Composants	Systèmes standard, durcis face aux attaques cyber	Systèmes pour environnements difficiles, avec des capacités de calcul et mémoire plus réduites

Figure 2 : Critères de différenciation entre les mondes IT et OT[13]

[13] La cybersécurité des systèmes industriels (cyber.gouv.fr)

Ces différences impliquent des approches spécifiques en matière de cybersécurité. Tandis que dans l'IT, l'ordre de valeur en termes de priorité s'articule généralement sous la forme : 1. Confidentialité, 2. Intégrité, 3. Disponibilité, 4. Traçabilité, les priorités dans l'OT vont s'en retrouver modifiées de la sorte :

- **Disponibilité :** garantir un accès permanent aux données, applications et systèmes ;
- **Intégrité :** garantir que les données n'ont subi aucune modification non autorisée ;
- **Confidentialité :** garantir que les données ne sont accessibles qu'aux seules personnes autorisées ;
- **Traçabilité :** garantir l'enregistrement de l'ensemble des activités critiques sur le SI (connexions, modifications, échanges spécifiques).

La figure suivante synthétise les périmètres d'intervention et les priorités des différents SI :

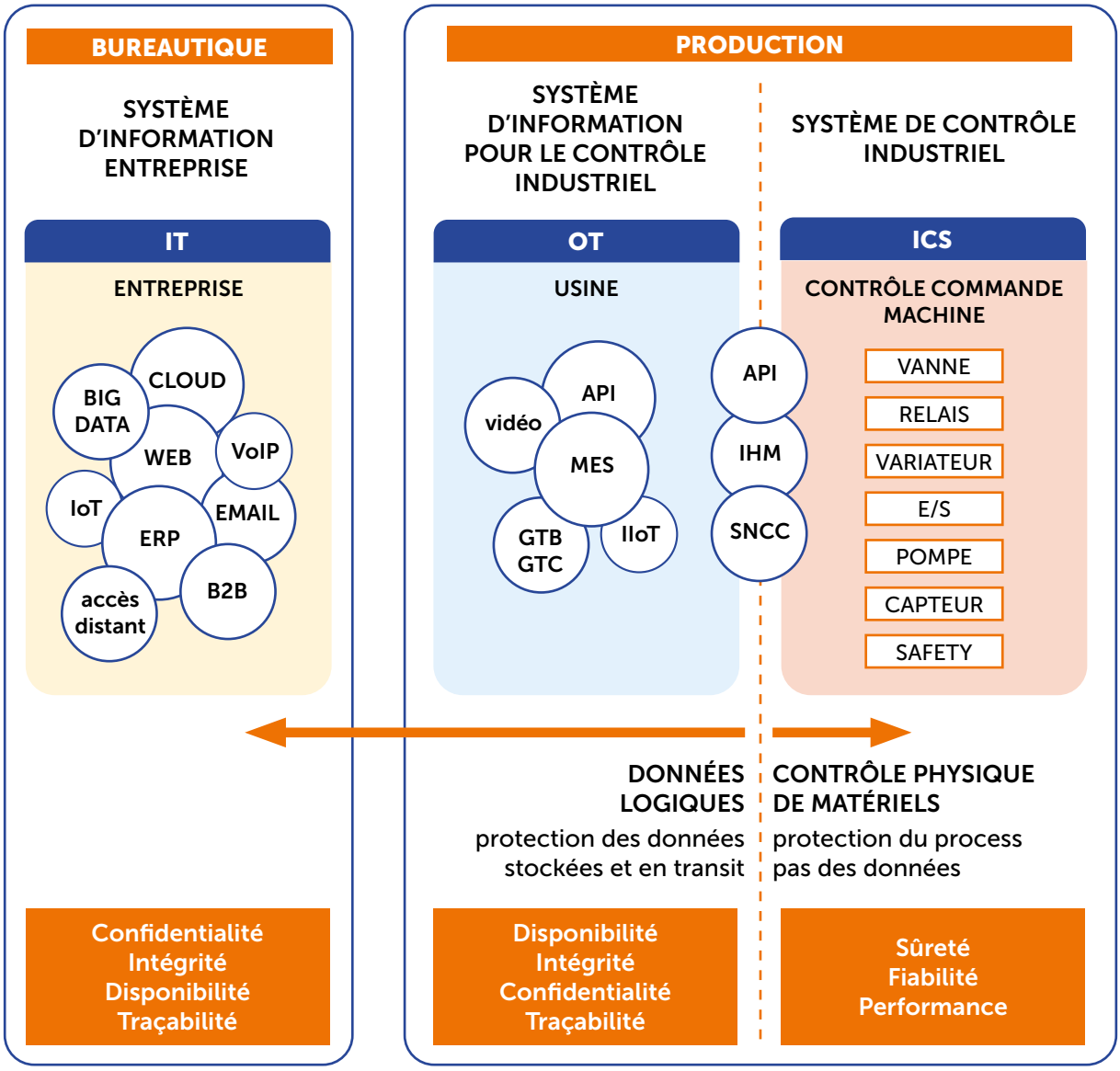


Figure 3 : Priorités des critères de protection cybersécurité en fonction des zones du SI[14]

[14] icsmodel.infracritical.com

En définitive, c'est toute la culture de la cybersécurité, principalement issue du monde IT, qui doit donc être adaptée au contexte de la production industrielle, et des SI OT. La vigilance doit être accrue vis-à-vis des attaques cyber, car une majorité des systèmes industriels sont par conception moins sécurisés (absence de chiffrement, protocoles moins robustes, réseaux peu segmentés, etc.), même si cela a tendance à changer avec les équipements les plus récents.

Pour répondre à ces enjeux spécifiques, dans les environnements industriels, un modèle propre à la cyber sécurité industrielle, le modèle "Purdue"[15], est employé afin de définir les différents niveaux de communication des éléments qui interviennent dans le contrôle informatique d'un site industriel.

Même si la cybersécurité industrielle s'intéresse à tous les niveaux du modèle Purdue, les niveaux 1, 2 et 3 sont tout particulièrement concernés ; le niveau 3.5 de la figure 1 ci-après constitutant une zone transitoire entre les infrastructures IT de l'entreprise et le domaine OT (industriel).

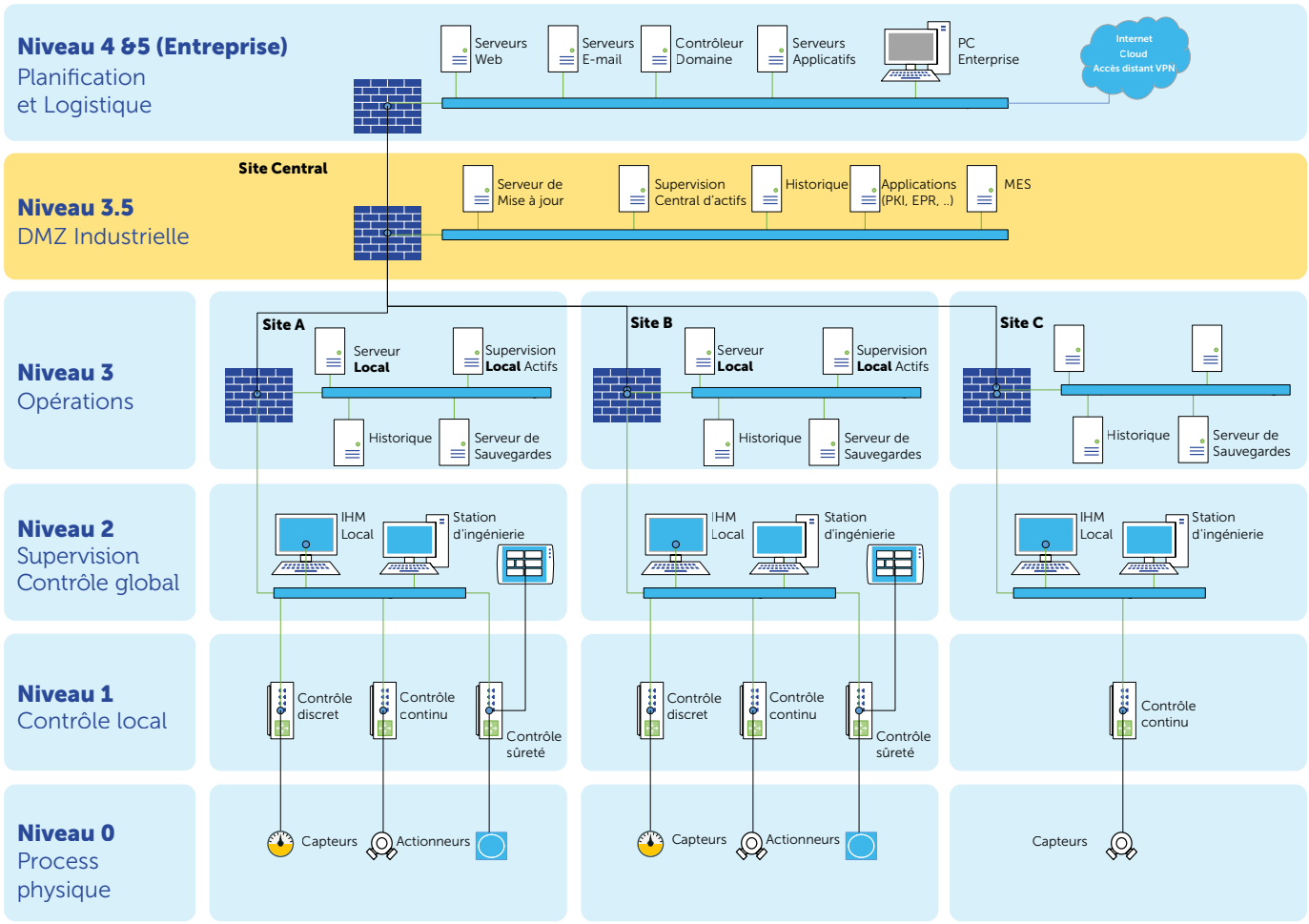


Figure 4 : Modèle Purdue pour organisation industrielle sur plusieurs sites

[15] The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation - Theodore J. Williams - 1992 (sciencedirect.com)

La convergence entre les mondes IT et OT, qui résulte de la transition vers l'Industrie 4.0 et l'adoption massive des systèmes connectés, participe à l'augmentation de la surface d'exposition des systèmes industriels aux cyberattaques. Historiquement, les environnements OT étaient isolés (air-gapped) et déconnectés des réseaux externes, ce qui leur offrait une protection relative contre les menaces IT. Cependant, l'intégration croissante des systèmes IT avec les systèmes industriels expose désormais les infrastructures critiques aux mêmes menaces que l'IT, tout en ajoutant des risques supplémentaires dus à l'interdépendance des systèmes.

GOUVERNANCE ET MODE D'ORGANISATION

Dans le domaine IT, la gouvernance et le mode d'organisation reposent généralement sur une structure claire et centralisée, où la DSI (Direction des Systèmes d'Information) et/ou le RSSI (Responsable Sécurité des Systèmes d'Information) supervise à la fois le Maintien en Condition Opérationnelle (MCO) et le Maintien en Condition de Sécurité (MCS). Cela signifie que la responsabilité des actifs et leur cybersécurité sont gérées sous un même contrôle.

Cependant, dans le monde industriel de l'OT, la gestion des actifs est plus complexe, avec de nombreux intervenants impliqués, notamment pour la gestion du MCO et du MCS. Les responsabilités sont fragmentées entre différentes parties prenantes : les responsables d'actifs, les responsables de la maintenance, les équipes cybersécurité, et parfois même les responsables de la production lorsque les actifs impactent directement les processus critiques. Cette segmentation entraîne une distribution des responsabilités entre plusieurs entités, avec des rôles et des responsabilités qui varient d'une organisation à l'autre.

Dans les environnements OT, les équipes travaillent souvent en 3/8 (trois équipes se relayant sur une période de 24 heures), et de plus on trouve la présence de nombreux intervenants externes (fournisseurs, intégrateurs, opérateurs, sous-traitants, etc.) ce qui exige une coordination rigoureuse. Le schéma de gouvernance devient ainsi moins centralisé que dans l'IT, ce qui peut poser des défis en matière de sécurité et de suivi.

Cela souligne l'importance cruciale de la coordination entre les différents acteurs. Chaque groupe ayant des cultures et des objectifs différents, il devient indispensable de mettre en place des mécanismes de communication et de suivi bien définis pour garantir l'efficacité du MCS. Un manque de synchronisation entre les équipes peut entraîner des lacunes en matière de sécurité, ce qui pourrait avoir des conséquences graves dans un environnement industriel. La coordination entre les différentes parties prenantes doit donc être renforcée à travers des processus de collaboration et des structures organisationnelles adaptées.

L'image ci-après illustre la répartition des rôles et responsabilités entre les équipes IT, OT, et les fournisseurs/intégrateurs dans le cadre de la gestion de la cybersécurité industrielle. Chaque acteur joue un rôle précis dans l'identification des besoins de maintenance, la gestion des vulnérabilités, et la mise en œuvre des plans de remédiation et de correctifs.

		Utilisateur						Fournisseur / Intégrateur	
		Responsablité IT		Responsablité OT					
		DSI (Équipe IT)	RSSI (Équipe IT)	Resp. Maintenance / contrat	Resp. Exploitation	Exploitant	RSSI (Équipe OT)	Équipe Projet / Déploiement	Resp. Cyber
Gestion client/ fournisseur	Identification des besoins de maintenance		I	C	A	R	C		
	Exécution du contrat de maintenance			A	C	R	I	R	I
Connaître son SI	Cartographie du SI	C	C		A	R	R	C	I
	Consolidation inventaire	C	C		A	R	R	C	I
	Maintenance de la cartographie	C	C		A	R	R	C	I
	Gestion de la configuration	C	C		A	R	R	C	I
	Classification et contextualisation	C	C		A	R	R	C	I
Identification des vulnérabilités et correctifs	Identification des vulnérabilités		R		I	I	A	C	R
	Identification des correctifs		R		I	I	A	C	R
Définition du plan de remédiation	Élaboration du plan de remédiation		I		R	R	A	[R]	[R]
	Application des mesures de durcissement ou d'atténuation du risque		I		R	R	A	[R]	[R]
	Application de correctifs		I		A	R	R	[R]	[R]
	Programme de gestion de la remédiation	C	C		C	R	A		
Application de la remédiation	Application des mesures d'attenuation				C	R	A	[R]	[R]
	Gestion des sauvegardes				C	R	A	[R]	[R]
	Validation de la remédiation				C	R	A	[R]	[R]
	Déploiement de la remédiation				C	R	A	[R]	[R]

R- Réalisateur / A- Approbateur / C- Consulté / I- Informé / [R] : Si responsabilité sous-traitée

Figure 5 : Matrice R.A.C.I. de responsabilités du processus MCS dans une organisation industrielle

COMMUNICATION ET PROTOCOLES

Les protocoles de communication industriels sont conçus pour répondre aux besoins d'environnements critiques qui exigent une fiabilité élevée, une robustesse dans des conditions extrêmes, et des échanges en temps réel entre les équipements (machines, capteurs, actionneurs). Ces exigences diffèrent des protocoles classiques utilisés dans les réseaux informatiques. En OT, il ne s'agit pas uniquement de gérer des flux d'information, mais de garantir le bon fonctionnement de processus physiques souvent vitaux pour la production industrielle.

Ces communications peuvent être réalisées via des supports filaires, optiques, ou sans-fil. Toutefois, lorsque des solutions sans-fil sont utilisées, le risque cyber est accru, car elles sont plus exposées aux attaques telles que l'interception des communications ou les attaques par déni de service. Des mesures de sécurité adaptées doivent donc être intégrées dès la conception pour limiter ces risques et protéger l'intégrité des communications industrielles.

Voici un tableau regroupant les protocoles de communication industriels les plus utilisés, classés en fonction de leur nature (bus de terrain, protocoles Ethernet standard, et propriétaires) :

Bus de terrain	Protocoles standards sur Ethernet	Protocoles propriétaires sur Ethernet
Modbus	Profinet	Siemens S7com et S7com+, UMAS, WAGO, SOFRELT, etc.
Profibus DP	EtherNet/IP	Allen-Bradley Data Highway Plus (DH+)
ASi	Modbus/TCP	Mitsubishi Melsec
CANopen	OPC UA	Omron FINS
DeviceNet	EtherCAT	Beckhoff ADS
BACnet MS/TP	Powerlink	
	IEC 61850 et IEC 60870-5-104	
	BACnet/IP et BACnet/SC	

Table 1 : Familles de protocoles industriels les plus utilisés - liste non exhaustive

Historiquement, les bus de terrain ont été largement utilisés dans les systèmes industriels pour permettre la communication entre les différents équipements. Cependant, ils sont progressivement remplacés par des réseaux Ethernet, qui apportent des avantages en termes de flexibilité et de fonctionnalités supplémentaires. Ethernet permet une gestion plus fluide des flux de données et une intégration plus simple avec les systèmes IT. Mais ces mêmes avantages peuvent aussi présenter des risques si des mesures ne sont pas prises pour réguler l'utilisation des réseaux. L'absence de restrictions pourrait ouvrir la voie à des flux malveillants ou non autorisés qui compromettraient la sécurité des systèmes industriels.

Ainsi, un Maintien en Condition de Sécurité (MCS) efficace est essentiel pour surveiller et contrôler ces réseaux, limitant les risques d'intrusion et d'attaques. Des politiques de segmentation réseau, une gestion stricte des accès et des systèmes de détection d'intrusions doivent être mis en place pour protéger les infrastructures industrielles contre les menaces cyber et garantir la disponibilité et l'intégrité des processus industriels.

MATÉRIELS

Le matériel industriel utilisé dans les environnements OT présente des spécificités notables. Chaque équipement, qu'il s'agisse de hardware ou de software, est conçu pour des usages très précis. Cependant, en raison de leur ancienneté et du fait que ces équipements n'ont pas été initialement conçus avec la cybersécurité en tête, ils intègrent rarement des mécanismes de protection contre les menaces modernes.

L'une des grandes difficultés réside dans l'application des correctifs logiciels. Ces mises à jour, essentielles pour améliorer la sécurité des équipements, demandent une expertise et une expérience spécifiques, car elles peuvent impacter directement la stabilité des systèmes. De plus, les fournisseurs de technologie ont un contrôle exclusif sur les correctifs et les vulnérabilités. Lorsqu'il s'agit de mettre à jour des logiciels (tels que les systèmes d'exploitation Windows ou Linux), les gestionnaires d'infrastructures industrielles doivent souvent obtenir la validation des fournisseurs pour ne pas annuler la garantie des équipements ou risquer une incompatibilité avec les processus industriels.

La diversité technologique est également une source de complexité. Les sites industriels se caractérisent par une hétérogénéité des équipements provenant de multiples fournisseurs et intégrateurs. Cette diversité rend difficile la maîtrise des flux d'information, car les équipements utilisent des protocoles de communication différents. Cette fragmentation technologique ajoute un niveau de complexité supplémentaire pour assurer un Maintien en Condition de Sécurité (MCS) optimal.

En outre, les infrastructures industrielles sont réparties dans des environnements géographiques variés et soumis à des contraintes physiques hétérogènes, comme des conditions extrêmes de température, d'humidité ou d'accès difficile. Le contexte industriel lui-même est caractérisé par des environnements exigeants, où la poussière, l'humidité, la chaleur, et les rayonnements électromagnétiques sont courants. Ces contraintes supplémentaires pour la maintenance et la sécurisation des systèmes, combinées à des exigences de production continue, réduisent considérablement les fenêtres de temps disponibles pour la maintenance, rendant la sécurisation des infrastructures OT encore plus complexe.

Enfin, la réglementation apporte aussi son lot de contraintes, différentes selon les secteurs. Les secteurs comme la pharmacie (GXP, FDA), le nucléaire (code de l'environnement, guides IAEA) ou la chimie sont soumis à des régulations strictes qui influencent directement la gestion des risques et l'application des standards de sécurité. Ces régulations sectorielles s'ajoutent aux normes internationales (ISO 27001, IEC 62443, NIST) et aux règlements nationaux et européens en matière de cybersécurité, comme la Loi de Programmation Militaire (LPM), la Directive NIS et sa mise à jour NIS 2.

GESTION DES INCIDENTS ET DES ÉVOLUTIONS

La gestion des incidents dans les environnements IT et OT présente des différences majeures. Dans le monde IT, les incidents sont souvent gérés avec plus de rapidité grâce à la flexibilité des systèmes, qui permettent des correctifs réguliers et, parfois, automatisés.

Dans l'IT, la mise à jour d'applications, de serveurs ou d'ordinateurs peut se faire rapidement car ces systèmes peuvent être mis hors ligne temporairement pour maintenance ou sont redondés. À l'inverse, dans les environnements industriels, toute interruption de la production pour maintenance ou mise à jour peut

entraîner des pertes financières, ce qui complique considérablement la réponse aux incidents.

La gestion des incidents IT se concentre principalement sur la protection des données et des systèmes informatiques contre les cybermenaces, les violations de données et les défaillances système. Les équipes IT suivent des protocoles établis pour contenir, atténuer et récupérer les incidents, souvent avec une approche bien structurée et des ressources disponibles.

En OT, la gestion des incidents est plus complexe car les conséquences peuvent être physiques, affectant non seulement les systèmes mais aussi les machines et processus industriels. Les incidents peuvent directement perturber la production et, dans certains cas, mettre en danger la sécurité des personnes. La remédiation dans ces environnements nécessite souvent une expertise spécifique, et fait appel à plusieurs intervenants, notamment les fournisseurs et intégrateurs, pour rétablir les opérations et limiter les interruptions[16]. Le facteur temps joue un rôle clé, et les fenêtres de maintenance doivent être soigneusement planifiées pour minimiser les impacts sur la production.

La gestion des vulnérabilités dans l'OT se fait également sur un cycle plus long que dans l'IT. Alors que des systèmes IT, comme les versions de Windows Server, sont régulièrement publiés (tous les 3 à 4 ans), des équipements industriels comme les Schneider Modicon ou les Siemens S7 peuvent rester en place pendant plus de 10 ans sans mise à jour majeure. Cette longévité des équipements, associée à des priorités de production, pousse souvent les équipes industrielles à reléguer les correctifs de sécurité au second plan, laissant ainsi des équipements obsolètes et vulnérables aux cyberattaques.

De plus, les processus de validation des équipements IT sont rapides, avec des phases de recette ou de pilote qui s'effectuent en peu de temps. En revanche, dans les environnements OT, et surtout chez les opérateurs d'infrastructures critiques, les processus de qualification ou d'homologation des systèmes sont bien plus longs et consomment davantage de ressources. Cela ralentit l'application des mises à jour et complique encore la gestion des évolutions.

Pour pallier ces difficultés, il est essentiel d'anticiper les fenêtres de maintenance et d'adopter des outils comme les jumeaux numériques, qui permettent de tester les correctifs avant leur déploiement dans l'environnement de production. Cela permet de réduire les risques de perturbation et d'assurer une mise à jour sécurisée des systèmes sans compromettre la production industrielle.

2.3 LE MCS ET LA RÉGLEMENTATION

Outre les contraintes techniques et opérationnelles qui caractérisent les systèmes OT, un autre type de contrainte existe en matière de réglementation. En effet, les systèmes industriels sont encadrés par des normes et des lois visant à renforcer leur sécurité face aux cybermenaces. La nature critique de certaines infrastructures OT, comme les réseaux d'énergie, de transport ou de production, impose aux organisations de respecter des exigences strictes pour assurer la résilience de ces systèmes.

DIRECTIVE NIS, LPM

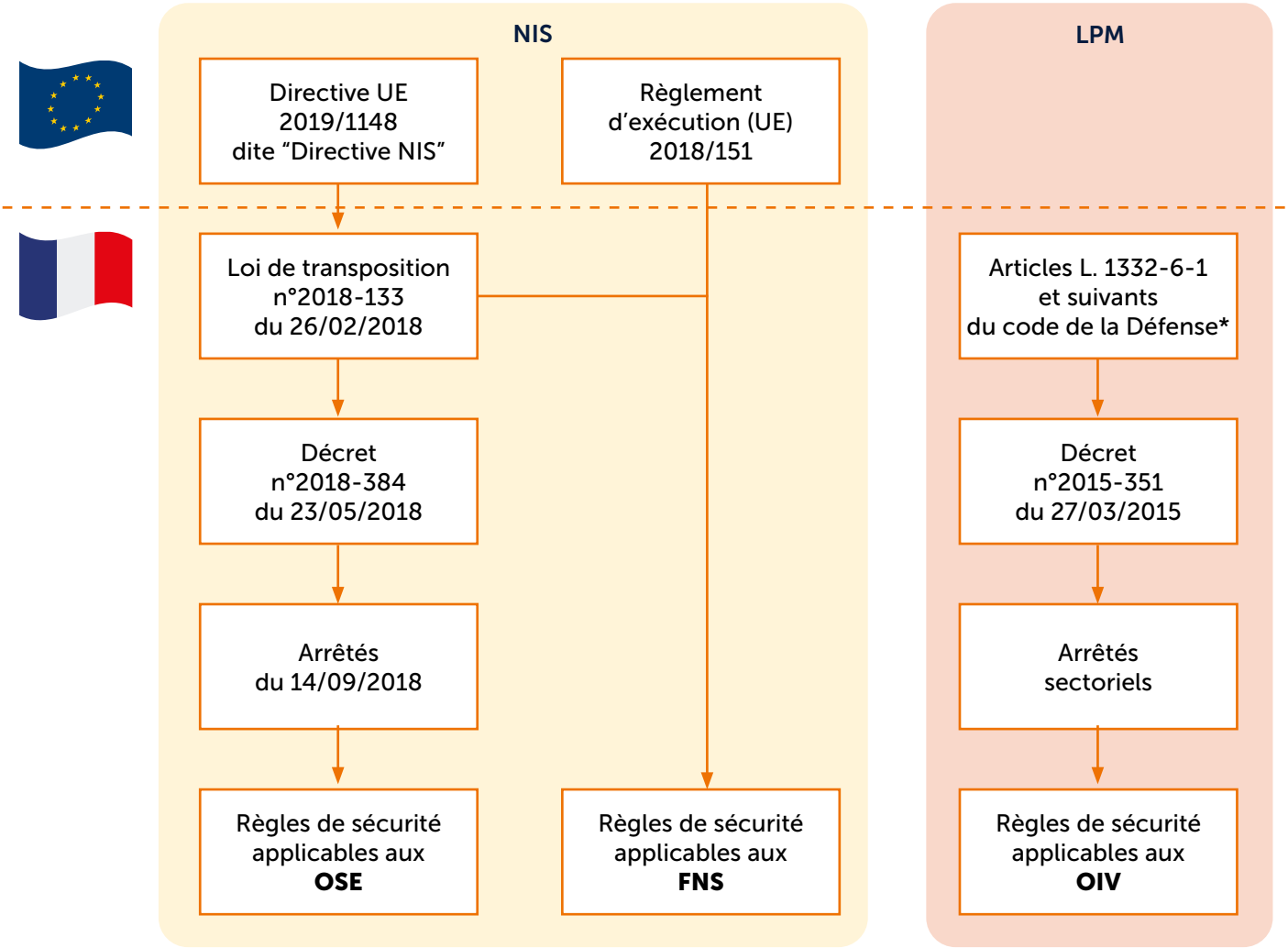
La réglementation relative au MCS en France et en Europe s'appuie sur plusieurs textes clés, principalement la Directive NIS, directive (UE) n°2016/1148 du Parlement Européen et du Conseil du 6 juillet 2016, et la Loi de Programmation Militaire, loi n°2013-1168 du 18 décembre 2013 (dite "LPM"), ainsi que des normes internationales comme l'IEC 62443.

La Directive NIS et la LPM imposent aux organisations la mise en œuvre de mesures de sécurité robustes pour protéger leurs Systèmes d'Information Essentiels (SIE) et Systèmes d'Information d'Importance Vitale (SIIV). Ces textes concernent trois types d'entités :

- **Opérateurs de Services Essentiels (OSE) :** soumis aux règles de la NIS et à la loi n°2018-133 du 26 février 2018[17] de transposition de la directive en droit français.
- **Fournisseurs de Services Numériques (FSN) :** la directive NIS précise que les FSN ne sont pas soumis aux règles applicables aux OSE cependant, ils doivent définir des « mesures de sécurité visant à assurer un niveau de sécurité des réseaux et systèmes d'information qu'ils utilisent », au titre du règlement d'exécution (UE) 2018/151 de la commission du 30 janvier 2018.
- **Opérateurs d'Importance Vitale (OIV) :** soumis aux articles L. 1332-6-1 et suivants du code de la défense, pour sécuriser leurs Systèmes d'Information d'Importante Vitale (SIIV).

[16] Doctrine de détection pour les systèmes industriels (cyber.gouv.fr)
[17] LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (legifrance.gouv.fr)

La figure ci-après publiée par l'ANSSI en décembre 2020 synthétise les cas d'applications de NIS et de la LPM :



* Ces articles sont créés par la loi n°2013-1168 du 18/12/2013 dite "LPM 2014-2019"

Figure 6 : Organisation du dispositif réglementaire NIS et comparaison avec celui applicable aux OIV[18]

Plus précisément, l'arrêté du 14 septembre 2018, qui découle de la loi de transposition n°2018-133 de la Directive NIS en droit français, contient 23 règles spécifiant les exigences en matière de sécurité des réseaux et systèmes d'information pour les OSE et FSN. Parmi ces règles, plusieurs se concentrent spécifiquement sur la mise en place et la gestion du MCS, avec des implications directes pour les opérateurs et fournisseurs :

POLITIQUE DE SÉCURITÉ (RÈGLE 2)

Cette règle stipule que chaque OSE doit intégrer dans sa Politique de Sécurité des Systèmes d'Information (PSSI) une procédure spécifique pour le maintien en condition de sécurité des ressources de ses Systèmes d'Information Essentiels (SIE). Cette procédure doit prendre en compte l'ensemble des composantes matérielles et logicielles, assurant que celles-ci soient maintenues à jour et protégées contre les vulnérabilités identifiées.

[18] Recommandations pour la protection des systèmes d'information essentiels | ANSSI (cyber.gouv.fr)

INDICATEURS DE SÉCURITÉ (RÈGLE 4)

Cette règle exige des OSE qu'ils évaluent et mettent à jour régulièrement des indicateurs de sécurité pour chaque SIE, afin de suivre et mesurer l'état du MCS. Parmi ces indicateurs, on trouve le pourcentage de postes utilisateurs ou serveurs dont les systèmes ne sont pas dans une version logicielle encore supportée par le founisseur ou fabricant.

Cet indicateur permet. de suivre l'état de l'infrastructure et d'identifier rapidement les systèmes devenus obsolètes ou vulnérables.

PROCÉDURE DE MAINTIEN EN CONDITION DE SÉCURITÉ (RÈGLE 16)

Cette règle impose aux OSE de développer, tenir à jour, et mettre en œuvre une procédure de maintien en condition de sécurité (MCS) pour toutes les ressources matérielles et logicielles des SIE. Cette procédure, inscrite dans la politique de sécurité des systèmes d'information, doit inclure :

- les conditions nécessaires pour maintenir la sécurité des ressources des SIE, prenant en compte l'évolution des vulnérabilités et des menaces ;
- la politique de mise à jour des versions logicielles et l'application des mesures correctrices de sécurité (patchs et mises à jour) ;
- les vérifications préalables à l'installation de nouvelles versions ou de correctifs pour s'assurer de leur origine, de leur intégrité, et de leur compatibilité technique et opérationnelle avec l'environnement existant.

L'opérateur, dans le cadre du Maintien en Condition de Sécurité (MCS), a l'obligation de suivre en continu l'évolution des vulnérabilités affectant ses ressources matérielles et logicielles. Cette veille est réalisée notamment grâce aux informations fournies par les fabricants ou via des centres spécialisés comme le CERT-FR. Le rôle du MCS est de s'assurer que ces vulnérabilités sont rapidement corrigées, en installant les mises à jour de sécurité sur des versions supportées des systèmes. Cela garantit que les composants du système restent protégés contre les nouvelles menaces.

Cependant, si des difficultés techniques ou opérationnelles empêchent la mise à jour, l'opérateur doit justifier cette impossibilité. Avant de procéder à toute nouvelle installation de correctifs, il doit vérifier que la mise à jour respecte plusieurs critères essentiels pour la sécurité du système : l'origine de la mise à jour doit être fiable, son intégrité doit être assurée, et son impact technique et opérationnel sur l'environnement doit être évalué afin d'éviter des perturbations.

Lorsque des mesures correctrices sont identifiées, elles doivent être planifiées et appliquées après les vérifications nécessaires, sauf en cas de difficultés justifiées. Si l'application de la mise à jour est impossible, l'opérateur doit mettre en place des mesures alternatives pour atténuer les risques. Ces actions doivent être documentées dans le dossier d'homologation, garantissant ainsi que toutes les vulnérabilités identifiées sont gérées de manière proactive et que le système reste sécurisé malgré l'absence de correctifs directs. Cette documentation est un élément fondamental du MCS, car elle formalise la gestion des risques et des vulnérabilités en continu.

Ainsi, ces règles garantissent que les OSE et FSN mettent en place une approche proactive et structurée pour maintenir la sécurité de leurs infrastructures critiques face aux menaces évolutives.

La LPM (2024-2030) renforce ces dispositions, en imposant un suivi rigoureux des vulnérabilités, des mises à jour, et des mesures correctrices, tout en prévoyant la gestion des exceptions.

DIRECTIVE NIS 2

Plus récemment, la directive NIS 2[19] qui a été publiée en décembre 2022, qui doit être transposée dans chaque pays membre depuis octobre 2024, contient les éléments suivants concernant le maintien en condition de sécurité :

Chapitre	Art.	Titre	Description
IV Mesures de gestion du risque cyber et obligations de rapport	20	**Gouvernance**	S'assurer que le management approuve les mesures de gestion du risque cyber, surveille l'implémentation, prends l'engagement en cas de problème cyber et il est formé régulièrement à la cybersécurité pour identifier les risques et les impacts.
	21	**Mesures de gestion du risque Cyber**	Politiques et procédures pour l'analyse et la gestion des risques en incluant la « supply chain » (1) & (2). Ces politiques doivent aussi définir l'usage de la cryptographie et du chiffrement.
			- Approche basée sur l'analyse du risque. - Gestion des incidents. - Continuité du business (sauvegardes, gestion de crises et reprise d'activité). - Sécurité de la chaîne d'approvisionnement. - Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes. d'information, y compris le traitement et la divulgation des vulnérabilités. - Pratiques de base en matière de cyber-hygiène et la formation à la cybersécurité. - Gestion des actifs, sécurité du personnel et la politique des autorisations d'accès. - L'utilisation de pratiques plus avancées en cybersécurité: authentification multi-facteur ou continue, sécurisation des communications.
	22	**Évaluations coordonnées des risques**	Coopérer avec la commission et l'ENISA pour réaliser une évaluation des risques (techniques et non techniques) coordonnée et identifier les services, les systèmes et les produits critiques et leur chaînes d'approvisionnement.
	23	**Obligations de rapport**	Description détaillée de l'incident, y compris sa gravité et son impact (24H notification + 72H rapport, CSIRT)
			Type de menace ou cause profonde (vulnérabilités exploitées) qui est susceptible d'avoir déclenché l'incident
			Mesures d'atténuation appliquées et en cours
	24 & 25	**Normalisation européenne**	(24) Utiliser des produits, services et process certifiés ou être certifié suivant un schéma européen. (25) Normalisation des spécifications et technologies pour converger dans l'implémentation de l'article 21
VII Supervision et entrée en force	32	**Supervision et application pour les entités essentielles (32) et importantes (33)**	Audit des autorités compétentes : inspections sur site ou hors site, audits réguliers, ciblés ou ad hoc, scans de sécurité objectifs, et accès aux données, documents et preuves de la mise en œuvre de politiques de cybersécurité
	33		Mesures d'application de la directive NIS 2 : avertissements, instructions contraignantes, ordres de mise en conformité, désignation d'un officier de surveillance, publication des infractions et amendes administratives.

Table 2 : Eléments de la NIS 2, relatifs au maintien en condition de sécurité

[19] Publications Office (europa.eu) , La directive NIS 2 | ANSSI (cyber.gouv.fr)

DIRECTIVE REC (RÉSILIENCE DES ENTITÉS CRITIQUES)

En complément de la directive NIS 2, l'Union Européenne a adopté la Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC), qui vise à renforcer la résilience des infrastructures essentielles au sein de l'Union. Entrée en vigueur le 16 janvier 2023, cette directive devait être transposée par les États membres dans leur législation nationale avant le 17 octobre 2024. Les principaux objectifs de cette directive sont les suivants :

- **Renforcement de la résilience des infrastructures critiques :** les entités critiques doivent améliorer leur capacité à anticiper, prévenir, réagir et se rétablir après des incidents graves susceptibles de perturber leur fonctionnement.
- **Harmonisation des règles au niveau européen :** la directive met en place un cadre juridique commun et une approche coordonnée à l'échelle de l'Union pour assurer la protection des infrastructures critiques.
- **Identification des secteurs critiques :** les secteurs concernés incluent l'énergie (électricité, gaz, pétrole), le transport (aérien, ferroviaire, routier, maritime), les banques, les infrastructures du marché financier, la santé, l'eau potable, et l'administration publique.
- **Obligations des États membres :** chaque État membre est tenu d'adopter une stratégie nationale pour la résilience des infrastructures critiques et de désigner des autorités compétentes pour superviser l'application des mesures par les entités critiques.
- **Gestion des risques et rapports :** les entités critiques doivent procéder à des évaluations régulières des risques auxquels elles sont exposées et rendre compte des mesures mises en place pour y faire face.

RÉGLEMENTATION CRA (CYBER RESILIENCE ACT)

Une autre réglementation européenne majeure est le Cyber Resilience Act (CRA)[20], qui établit les exigences légales en matière de cybersécurité que les fabricants doivent respecter pour tout produit contenant des éléments numériques mis sur le marché intérieur européen. Celle-ci a été officiellement approuvée par le Parlement européen en mars 2024 et est entrée en vigueur la même année, avec une application immédiate dans tous les États membres de l'UE. Les fabricants devront s'y conformer à partir de 2027.

Le CRA s'applique aux fabricants, distributeurs et importateurs, qui sont tenus responsables de la cybersécurité d'un produit tout au long de son cycle de vie. Les produits numériques ne pourront être mis sur le marché que s'ils respectent des exigences spécifiques en matière de cybersécurité, telles que l'évaluation des risques, la déclaration de conformité, et la coopération avec les autorités compétentes. Certains utilisateurs finaux et donneurs d'ordres voudront s'assurer que les produits qu'ils sélectionnent sont conformes à cette réglementation.

Le CRA impose des exigences strictes en matière de gestion des vulnérabilités des fabricants, afin d'assurer la cybersécurité des produits numériques. La réglementation exige que les vulnérabilités soient corrigées rapidement, avec publication et notification aux utilisateurs des mises à jour de sécurité. Le fabricant doit identifier et documenter toutes les vulnérabilités ainsi que les composants concernés. Lorsqu'un correctif est publié, la documentation associée doit détailler les vulnérabilités corrigées ainsi que les actions à entreprendre. La réglementation encourage également le partage d'informations sur les vulnérabilités des produits et des composants tiers, et exige une distribution rapide et sécurisée des correctifs.

En outre, cette réglementation améliore la transparence pour les consommateurs et les utilisateurs professionnels quant à la sécurité des produits matériels et logiciels, et prévoit un cadre de surveillance du marché pour s'assurer que les règles sont respectées. Parmi les points à retenir pour le Maintien en Condition de Sécurité (MCS), on peut noter :

- les entreprises doivent effectuer des évaluations des cyber-risques avant la mise sur le marché d'un produit et pendant une durée de cinq ans ou tout au long de son cycle de vie prévu.
- les logiciels susceptibles de bénéficier de mises à jour automatiques doivent être configurés pour appliquer les mises à jour de sécurité par défaut, tout en laissant la possibilité aux utilisateurs de choisir de ne pas les installer.
- les produits jugés critiques devront faire l'objet de vérifications externes indépendantes du fabricant.

[20] Texts adopted - Cyber Resilience Act - Tuesday, 12 March 2024 (europa.eu), Procedure File: 2022/0272(COD) | Legislative Observatory | European Parliament (europa.eu)

- les entreprises doivent notifier l'Agence européenne pour la cybersécurité (ENISA) de tout incident dans un délai de 24 heures après en avoir eu connaissance et prendre les mesures nécessaires pour y remédier.

STANDARDS INTERNATIONAUX DE RÉFÉRENCE

En complément de la réglementation, plusieurs normes et standards internationaux définissent des cadres méthodologiques pour le MCS :

- la norme IEC 62443, notamment ses parties 2 et 3, est largement adoptée pour la gestion de la sécurité des systèmes OT.
- le NIST (NIST SP 800-40 Rev. 4 et NIST SP 800-82 Rev. 3) propose des recommandations sur la protection des systèmes industriels.
- la norme ISO 27001 (version 2022) intègre également la gestion des correctifs et la mise à jour continue des systèmes de sécurité de l'information (SMSI), en fournissant des bonnes pratiques adaptées aux environnements critiques.

Ces normes préparent les entreprises à se conformer aux réglementations actuelles et futures, tout en garantissant par conception que leurs systèmes restent protégés face aux menaces émergentes et aux exigences de sécurité.

Ainsi, les cadres réglementaires et normatifs, tant nationaux qu'internationaux, imposent aux entreprises industrielles de développer une gestion rigoureuse et continue des vulnérabilités et de la sécurité des systèmes critiques.

3 / LA MCS **DANS LE MONDE INDUSTRIEL**

3.1 DÉFINITION DU MAINTIEN EN CONDITION DE SÉCURITÉ (MCS)

Le MCS a pour objectif d'assurer le niveau de sécurité d'un système tout au long de son cycle de vie. Cela inclut les phases de conception, déploiement, exploitation, mise à jour, et va jusqu'au décommissionnement. Le MCS s'assure que les vulnérabilités sont gérées de manière continue et maîtrisée, afin de réduire l'écart entre l'identification d'une faille et l'adoption de mesures correctives adaptées.

Durant la phase de conception, le MCS met l'accent sur le développement sécurisé des produits. Le guide de l'ANSSI sur la protection des systèmes essentiels[21] décrit les bonnes pratiques à suivre pour la mise en œuvre de ces mécanismes de sécurité, en application de la directive NIS et de la Loi de Programmation Militaire (LPM).

Durant la vie du système, l'ANSSI recommande plusieurs règles, notamment dans son guide d'hygiène informatique[22] et dans les règles d'or pour la conception de systèmes numériques[23]:

- mettre en place une politique de mise à jour des composants (Règle 34) ;
- anticiper la fin de maintenance des logiciels (Règle 35).

Le MCS doit s'intégrer à la Politique de Sécurité des Systèmes d'Information (PSSI) de l'opérateur (cf. Le guide d'élaboration de la PSSI[24]), qui inclut des lignes directrices sur la gestion des correctifs, des prestataires externes, de l'obsolescence, et de la criticité des actifs. La PSSI comprend aussi le Plan de Continuité d'Activité (PCA) et le Plan de Reprise d'Activité (PRA), qui garantissent la restauration du SI à son état nominal après un incident grave, en s'assurant que tous les composants sont maintenus à jour et fonctionnent avec les versions logicielles appropriées.

Le MCS repose sur une gestion des risques structurée autour de plusieurs étapes :

1. **Identification des actifs :** repérer tous les actifs OT et leurs vulnérabilités ;
2. **Identification des menaces :** évaluer les cybermenaces potentielles ;
3. **Évaluation des vulnérabilités :** mesurer la criticité des vulnérabilités associées à chaque actif ;
4. **Analyse des menaces et vulnérabilités :** déterminer la probabilité et l'impact des menaces identifiées ;
5. **Atténuation des risques :** mettre en place un plan d'action pour atténuer ou éliminer les risques en priorisant les actions.

Le MCS permet donc une gestion proactive des risques liés aux infrastructures critiques et vise à maintenir un niveau de sécurité constant dans un environnement industriel exposé à des menaces évolutives.

3.2 IDENTIFICATION DES BESOINS DE MCS

Pour bien identifier les besoins MCS, la première étape consiste à définir des objectifs de sécurité qui soient en cohérence avec les indicateurs de production. Si les infrastructures industrielles nécessitent un haut degré de disponibilité, les exigences en matière de sécurité doivent être tout aussi élevées. Il est donc primordial d'évaluer les mesures de sécurité déjà en place pour connaître le point de départ de l'analyse.

Lorsqu'un équipement est en voie d'obsolescence, avec une exposition accrue aux nouvelles vulnérabilités, l'industriel devra évaluer la possibilité de prolonger sa durée de vie en intégrant des mesures de sécurité adaptées. Cela permet de limiter ou différer des investissements en renforçant la protection des actifs vieillissants, au lieu de procéder immédiatement à leur remplacement.

Ensuite, la réglementation joue un rôle clé dans la motivation pour mettre en œuvre un plan de MCS. L'industriel doit donc intégrer le besoin de mise en conformité du MCS par rapport à la régulation, tel qu'évoqué au chapitre 2.3.

Très concrètement, afin d'établir les besoins en matière de MCS, plusieurs étapes sont à suivre :

1. ÉVALUER LE CONTEXTE DES ACTIFS

Il s'agit d'attribuer un niveau de sécurité et de criticité attendu à chaque groupe d'actifs. Il faut ensuite établir la position de ces actifs dans le processus industriel pour déterminer leur importance relative. De plus, il est crucial d'évaluer le degré d'obsolescence et la durée de vie des actifs. Les systèmes ayant une longue durée de

[21] La cybersécurité des systèmes industriels
[22] Guide d'hygiène informatique (cyber.gouv.fr)
[23] 10 règles d'or pour la conception et la mise en œuvre de services numériques | ANSSI (cyber.gouv.fr)
[24] PSSI — Guide d'élaboration de politiques de sécurité des systèmes d'information | ANSSI (cyber.gouv.fr)

vie nécessiteront une attention particulière en matière de MCS afin d'assurer leur protection à long terme.

2. IDENTIFIER LES RESPONSABILITÉS DE MAINTENANCE

La responsabilité de la maintenance peut être intégrée à un contrat avec un fabricant ou un intégrateur. Ces contrats incluent souvent le Maintien en Condition Opérationnelle (MCO), mais pas toujours le MCS. Il est donc important de vérifier si le MCS est couvert dans les contrats existants, ou si des besoins spécifiques doivent être définis. En complément du MCO, le MCS assure la protection contre les cyberattaques et garantit la sûreté de fonctionnement. Il est également nécessaire de clarifier les responsabilités des différents acteurs intervenant sur les actifs (voir tableau RACI).

3. ÉTABLIR UN PLAN D'APPLICATION DE LA MAINTENANCE

Il convient de définir les périodes d'arrêt d'activité pour effectuer les opérations de maintenance, en incluant idéalement le MCS dans le planning de maintenance MCO afin d'éviter des interruptions supplémentaires. Toutefois, cela n'est pas toujours réalisable et nécessite parfois des ajustements.

4. DÉFINIR LE PÉRIMÈTRE DES ACTIVITÉS DE MCS

Ce document décrit un processus de MCS structuré en quatre piliers, mais il revient à l'industriel de décider quelles activités peuvent être mises en œuvre immédiatement, et celles qui devront être reportées à un cycle ultérieur, selon les priorités de sécurité.

5. POLITIQUE DE REMÉDIATION

Il est essentiel de clarifier la politique de remédiation de l'organisation. Certaines mises à jour peuvent ne pas être réalisables pour des raisons techniques ou opérationnelles. Il convient également de définir les politiques de gestion des accès aux applications, ainsi que les mesures de durcissement, de contrôle d'accès et de segmentation préconisées par la PSSI.

Ces différents éléments permettent à l'industriel de mieux cerner ses besoins en matière de MCS, et d'orienter la création d'un cahier des charges détaillé, que ce soit pour des interventions internes ou pour le recours à un prestataire externe. Une fois les besoins identifiés et le cadre de MCS défini, la prochaine étape consiste à prendre en compte le MCS dès la conception des nouvelles solutions. Ce principe permet d'intégrer la cybersécurité dès le début du cycle de vie des systèmes et d'éviter les vulnérabilités potentielles.

6. DÉFINITION DES KPI DE SUIVI

Pour piloter l'efficacité des actions de sécurité, il est important de définir des KPIs spécifiques. En voici quelques exemples :

- nombre de vulnérabilités détectées et corrigées
- nombre de vulnérabilités critiques non corrigées
- temps moyen de correction des failles (MTTR)
- niveau de conformité aux politiques de sécurité
- nombre de correctifs appliqués ou non

3.3 PRISE EN COMPTE DU MCS POUR LA CONCEPTION DES NOUVELLES SOLUTIONS

DEVSECOPS : UNE APPROCHE INTÉGRÉE AU MCS

Lors de la conception de nouvelles solutions industrielles, il est essentiel d'intégrer le Maintien en MCS dès le début du développement. Le MCS ne doit pas être une simple étape de fin de cycle, mais doit faire partie intégrante du processus de développement pour garantir que la cybersécurité est prise en compte à chaque phase. Cette approche proactive permet non seulement d'assurer une protection continue des infrastructures critiques (en réduisant les vulnérabilités et en améliorant la résilience des systèmes face aux cybermenaces), mais aussi de réduire les coûts et les complexités liés à la sécurisation des systèmes en phase d'exploitation.

Le DevSecOps est un cadre méthodologique qui combine le développement, la sécurité et les opérations dans une démarche continue. En OT, cette approche est particulièrement pertinente car elle permet d'intégrer la sécurité tout au long du cycle de développement des systèmes. Le DevSecOps en OT permet :

- l'identification précoce des risques pendant la phase de conception ;
- l'automatisation des tests de sécurité tout au long du développement ;
- la mise en place de correctifs rapides sans perturber les opérations industrielles critiques.

Les systèmes OT doivent être conçus pour faciliter le suivi des vulnérabilités et permettre des mises à jour de sécurité efficaces sans perturber la production, conformément aux exigences spécifiques des environnements industriels.

Les architectures micro-services offrent un excellent exemple de conception adaptée au MCS dès le départ. Contrairement aux architectures monolithiques, où chaque modification ou mise à jour nécessite des tests sur l'ensemble du système, les micro-services permettent de segmenter les fonctionnalités en modules indépendants. Chaque module peut être sécurisé, testé et mis à jour individuellement sans affecter les autres composants du système.

Cette modularité présente plusieurs avantages :

- **Flexibilité et rapidité des mises à jour :** grâce à leur nature découplée, les micro-services permettent d'appliquer des correctifs de sécurité ou des mises à jour fonctionnelles sans nécessiter un arrêt complet des opérations, ce qui est crucial dans les environnements OT où la disponibilité est prioritaire.
- **Isolement des failles :** en cas de vulnérabilité dans un service, elle peut être corrigée sans risque de propagation à d'autres services, réduisant ainsi l'impact d'une potentielle attaque.
- **Facilité d'intégration des mesures de sécurité :** chaque micro-service peut intégrer des fonctionnalités de sécurité spécifiques (authentification, chiffrement, journalisation des événements) tout en restant cohérent avec l'architecture globale.

L'adoption d'une architecture micro-services permet ainsi de mieux prendre en compte le MCS dès la conception, en facilitant la maintenance et les mises à jour continues de sécurité, en ligne avec les approches DevSecOps.

NORME IEC 62443 : SÉCURITÉ PAR CONCEPTION

La norme IEC 62443 régit la cybersécurité des systèmes industriels et met l'accent sur deux points clés :

- Sécurité dès la conception (Security by Design) : selon la section IEC-62443-4-1, les exigences de sécurité doivent être définies dès la phase initiale de développement, avec une analyse des risques et des vulnérabilités intégrées au cycle de vie du produit. Cela garantit que la sécurité fait partie des fonctionnalités essentielles, au même titre que la performance et la disponibilité.
- Développement sécurisé des logiciels : selon la section IEC-62443-4-2, des pratiques de codage sécurisé doivent être appliquées pour réduire les failles connues. Les outils automatisés de détection de vulnérabilités, ainsi que des tests de pénétration réguliers, doivent être utilisés pour garantir que les correctifs sont appliqués de manière proactive et conforme aux contraintes opérationnelles.

EXIGENCES DU CYBER RESILIENCE ACT (CRA)

Le Cyber Resilience Act (CRA) impose de nouvelles obligations aux fabricants de systèmes numériques, y compris ceux destinés à l'OT. Il renforce la nécessité d'inclure la sécurité tout au long du cycle de vie des produits :

- **Cybersécurité dès la conception :** le CRA exige que les systèmes soient conçus avec des fonctionnalités de sécurité de base et la capacité à recevoir des mises à jour tout au long de leur durée de vie.
- **Obligation de maintenance :** les fabricants sont tenus de fournir des mises à jour de sécurité pendant une période définie. Cela impose la création de systèmes OT capables de recevoir des correctifs sans impact majeur sur la production, renforçant l'importance de l'approche DevSecOps.
- **Gestion des vulnérabilités :** les systèmes doivent surveiller continuellement les risques de sécurité et faciliter la mise en conformité automatique grâce à des pipelines de mise à jour continue (CI/CD), alignés avec les pratiques de gestion des risques prévues par la norme IEC 62443.

BONNES PRATIQUES DE CYBERSÉCURITÉ ET HYGIÈNE INDUSTRIELLE

En complément des cadres normatifs, les recommandations du Guide de l'ANSSI Cyber Industrielle[25] sur les principes d'hygiène informatique des systèmes industriels doivent être intégrées dès la conception des nouvelles solutions :

1. séparation des réseaux IT et OT pour minimiser les risques de propagation des attaques ;
2. contrôle d'accès strict pour garantir que seuls les utilisateurs autorisés accèdent aux systèmes critiques ;
3. gestion régulière des vulnérabilités et planification des correctifs compatibles avec les cycles de maintenance industriels ;
4. segmentation réseau interne pour limiter les déplacements latéraux d'éventuelles menaces ;
5. surveillance continue des systèmes et journalisation des activités pour détecter et analyser rapidement les anomalies.

En définitive, l'intégration du MCS, de l'approche DevSecOps, des bonnes pratiques d'hygiène industrielle, et des obligations du CRA permet de créer des systèmes résilients face aux cybermenaces tout en répondant aux exigences réglementaires et opérationnelles spécifiques aux environnements OT. Ces éléments, appliqués dès la conception, garantissent un haut niveau de sécurité tout au long du cycle de vie des produits industriels, avec un impact minimal sur la continuité des opérations.

3.4 LES QUATRE PILIERS D'UN PROGRAMME DE MCS

Pour toutes les raisons évoquées dans les chapitres précédents, la mise en place d'un programme de MCS dans les environnements industriels requiert une méthodologie spécifique. Contrairement à la MCO, le MCS se concentre sur la gestion des vulnérabilités et des menaces cyber. Il doit être anticipé et structuré dès la conception et l'intégration des systèmes industriels, en s'appuyant sur des procédures rigoureuses et des moyens techniques adaptés, conformes aux exigences réglementaires ou internes.

Un programme de MCS efficace repose sur quatre piliers fondamentaux :

1. CONNAISSANCE DE SON SI

Le premier pilier du MCS est la connaissance approfondie du système d'information. Il est impossible de protéger efficacement un environnement industriel si l'on ne maîtrise pas pleinement l'ensemble des actifs qui le composent. Chaque équipement, logiciel, ou composant non identifié constitue une potentielle faille de sécurité. Une gestion rigoureuse des actifs est donc essentielle pour assurer une visibilité complète de l'environnement industriel et identifier les éléments vulnérables à sécuriser en priorité.

2. IDENTIFICATION DES VULNÉRABILITÉS ET CORRECTIFS

La deuxième étape consiste à surveiller continuellement les vulnérabilités associées aux différentes versions logicielles installées dans l'infrastructure. Il est crucial de comprendre comment ces vulnérabilités peuvent augmenter l'exposition aux risques cyber dans le contexte spécifique de l'industriel. Ce suivi implique également la surveillance des publications de correctifs fournis par les éditeurs de logiciels ou fabricants d'équipements.

La plupart des fournisseurs disposent d'équipes spécialisées, comme les PSIRT (Product Security Incident Response Team) ou les CERT-CSIRT (Computer Emergency Response Team), dont la mission est d'identifier, évaluer et corriger les vulnérabilités affectant leurs produits. Ils communiquent les découvertes et les solutions via des canaux dédiés, tels que des newsletters, auxquelles les industriels peuvent s'abonner pour être informés rapidement des nouvelles menaces et des correctifs disponibles.

3. DÉFINITION DU PLAN DE REMÉDIATION

La troisième étape consiste à évaluer et décider de la remédiation à appliquer pour réduire l'exposition aux cybermenaces. L'application des correctifs est généralement recommandée par les fournisseurs, mais dans certains cas, des mesures de réduction des risques peuvent être mises en place en attendant l'installation d'un correctif ou pour pallier une vulnérabilité jugée moins prioritaire. Cette phase de décision doit également tenir compte des contraintes opérationnelles et des exigences réglementaires. En effet, avant de déployer une mise à jour ou un changement de configuration,

[25] La cybersécurité des systèmes industriels | ANSSI (cyber.gouv.fr)

il est impératif d'évaluer les effets potentiels sur les processus industriels pour éviter des perturbations non souhaitées.

L'établissement d'un plan de remédiation structuré est essentiel pour coordonner les efforts. Ce plan doit inclure les actions spécifiques à entreprendre, les délais, les responsables, et les ressources nécessaires. Il est crucial de définir des étapes mesurables pour suivre les progrès et d'intégrer des contrôles réguliers pour garantir que les correctifs sont déployés efficacement

4. APPLICATION DE LA REMÉDIATION

Enfin, une fois la remédiation choisie, il faut s'assurer que sa mise en œuvre soit réalisée avec soin. Cela implique de prendre en compte plusieurs paramètres, tels que la planification des interventions pour minimiser les interruptions de production, la garantie que le comportement des processus industriels ne sera pas altéré, et la réalisation de sauvegardes complètes des systèmes et des configurations avant toute intervention. L'objectif est de garantir une mise en œuvre sécurisée et contrôlée, tout en préservant la continuité des opérations industrielles.

Les prochains chapitres se consacreront à l'analyse approfondie de chacun des quatre piliers du programme de MCS, en commençant par la connaissance de l'environnement.

Ces quatre piliers forment la base d'un programme de MCS solide et permettent de répondre efficacement aux risques et menaces en milieu industriel. Ils garantissent que les systèmes critiques soient non seulement maintenus en état de fonctionnement, mais aussi protégés face aux cyberattaques.

4 PREMIER PILIER : CONNAITRE SON SI

4.1 CARTOGRAPHIER LE SI

OBJECTIFS DE LA CARTOGRAPHIE

La cartographie du SI vise à représenter de manière détaillée les éléments qui composent le système d'information d'une organisation. Selon la complexité du SI, la cartographie peut être plus ou moins détaillée, mais elle doit toujours offrir une visibilité suffisante pour suivre les vulnérabilités, les menaces et les correctifs applicables. Cette vision est essentielle pour garder une vue à jour d'un réseau d'actifs en perpétuelle évolution, garantissant ainsi une meilleure protection face aux cyberattaques.

MÉTHODES DE CARTOGRAPHIE

Afin de concevoir efficacement la cartographie de son système d'information, l'ANSSI propose une guide d'élaboration en 5 étapes[26] :

1) Identification des enjeux, partie prenantes, périmètre et la cible ;
2) Collecter les éléments nécessaires et définir un modèle de cartographie ;
3) Définir les outils à utiliser ;
4) Réaliser l'inventaire du système d'information et construire les différentes vues cartographiques ;
5) Comment pérenniser la cartographie.

STRUCTURE DE LA CARTOGRAPHIE

La cartographie peut être organisée en trois visions complémentaires, selon les recommandations de l'ANSSI :

1. VISION MÉTIER

La vision métier se compose de deux aspects complémentaires : la vue de l'écosystème et la vue métier du système d'information.

La vue de l'écosystème cartographie l'ensemble des entités et systèmes qui interagissent avec le système d'information, y compris les partenaires, les fournisseurs et les clients. Elle permet de définir les limites de la cartographie et de saisir les interconnexions externes qui pourraient impacter la sécurité du SI.

Quant à **la vue métier**, elle se concentre sur les processus métiers internes de l'organisation, décrivant le rôle de chaque acteur dans ces processus, indépendamment des technologies et des systèmes utilisés. Elle est cruciale pour repositionner les éléments techniques dans leur contexte métier, offrant ainsi une meilleure compréhension de leur importance et de leur rôle au sein de l'organisation.

2. VISION APPLICATIVE

La vision applicative fournit une représentation détaillée des solutions logicielles qui supportent les processus métiers. Elle met l'accent sur les applications, les bases de données, les systèmes d'exploitation, ainsi que les échanges d'informations entre elles. Cette vue permet de visualiser les flux d'information à travers les différentes applications, en s'intéressant particulièrement aux flux critiques pour la sécurité numérique.

Elle inclut également **la vue de l'administration**, qui répertorie les périmètres de gestion des droits et les niveaux de privilèges des administrateurs. Cette partie est essentielle pour identifier qui a accès à quoi, et ainsi définir les politiques de gestion des accès et des privilèges. Dans les systèmes où la gestion des droits est centralisée, elle peut se traduire par une représentation schématique des périmètres d'administration ; dans les autres cas, elle prend la forme de listes précises des comptes et des niveaux d'accès pour chaque équipement.

3. VISION INFRASTRUCTURE

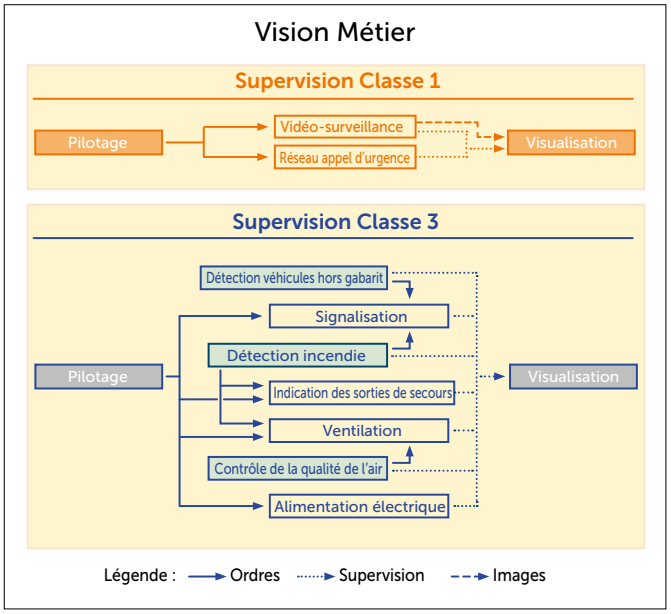
La vision infrastructure se divise en deux sous-parties : les infrastructures logiques et les infrastructures physiques.

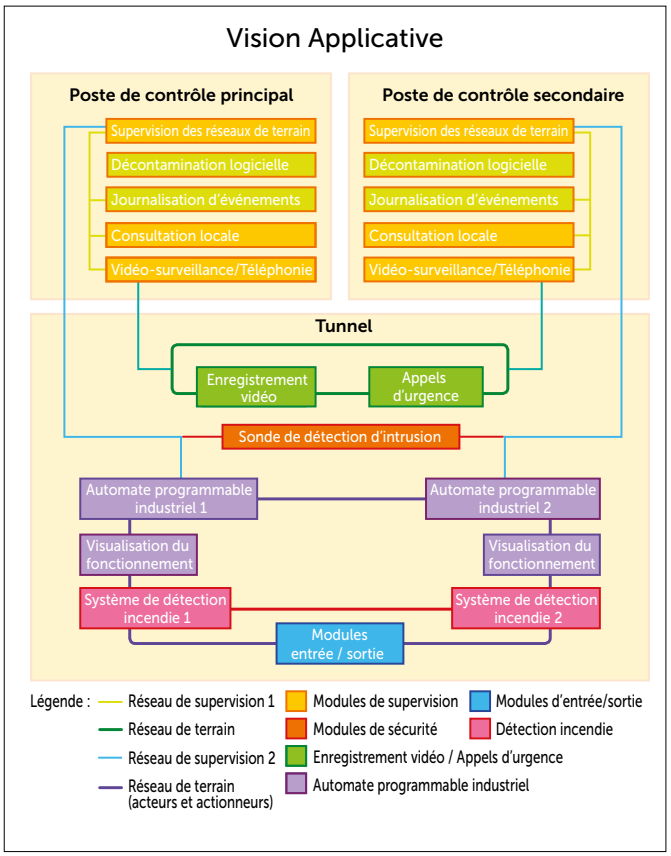
La vue des infrastructures logiques décrit la répartition et le cloisonnement des réseaux internes (zones de sécurité, segmentation, etc.), ainsi que les équipements réseau tels que les pares-feux, les commutateurs et les sondes de sécurité. Elle permet de visualiser les relations entre les différentes zones de sécurité et de comprendre comment les flux de données circulent à travers ces zones, ce qui est crucial pour identifier les points de vulnérabilité potentiels.

La vue des infrastructures physiques, quant à elle, recense les équipements physiques sur l'ensemble des sites de l'organisation. Elle montre la disposition géographique des serveurs, des routeurs, et des autres dispositifs sur les différents sites industriels. Cette représentation géographique aide à planifier les interventions de maintenance et à mieux comprendre la répartition des actifs critiques sur le territoire, en

[26] Cartographie du système d'information (cyber.gouv.fr)

tenant compte des contraintes physiques de chaque site (accès, sécurité physique, environnement).





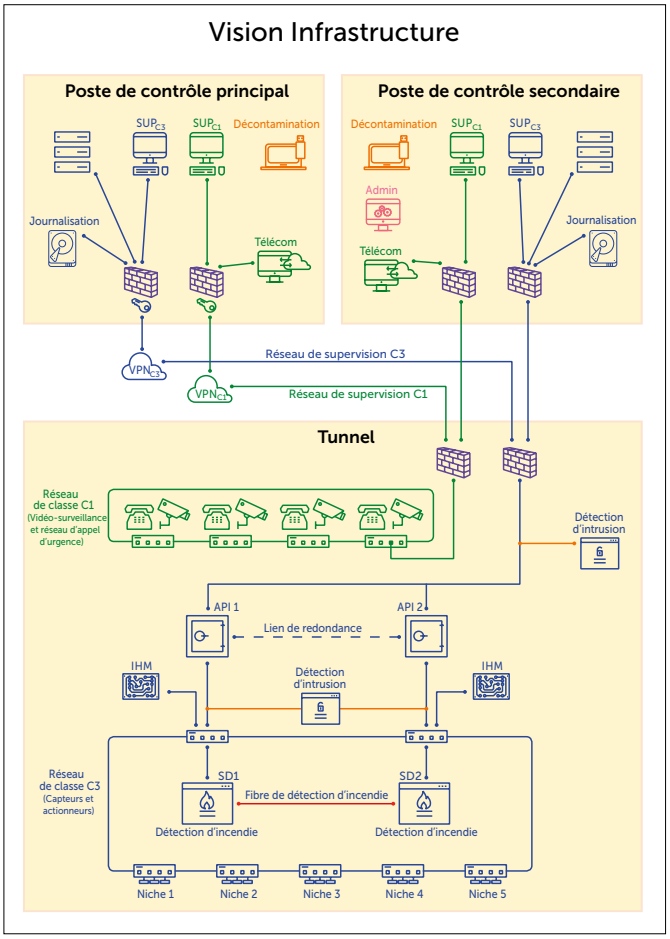


Figure 7 : Exemples de trois visions différentes pour cartographier un SI[27]

[27] Cartographie du système d'information (cyber.gouv.fr)

4.2 CONSOLIDER L'INVENTAIRE

PÉRIMÈTRE DE L'INVENTAIRE

La consolidation de l'inventaire des actifs constitue une étape clé pour assurer une gestion efficace de la sécurité dans les environnements industriels. Selon les recommandations du NIST[28], un inventaire complet des actifs doit inclure plusieurs types d'informations essentielles pour garantir un suivi rigoureux :

- **Identificateurs uniques :** chaque actif doit être pourvu d'un identifiant unique afin de le différencier et de le suivre tout au long de son cycle de vie, facilitant ainsi la traçabilité des équipements.
- **Inventaire du matériel :** cette catégorie regroupe les informations détaillées sur chaque appareil, incluant le fournisseur, le modèle, le numéro de série, les détails relatifs à l'achat, ainsi que des renseignements sur la fabrication et la construction. L'emplacement géographique de l'appareil est également important pour localiser les actifs sur les sites industriels.
- **Inventaire des logiciels et micrologiciels :** outre le matériel, il est crucial de tenir à jour les informations sur les logiciels et les micrologiciels installés sur chaque équipement. Cela comprend les numéros de version, les informations de localisation, ainsi que la nomenclature des logiciels (SBOM - Software Bill of Materials), permettant de mieux connaître les composants utilisés. Le SBOM est une liste détaillée de tous les composants logiciels et dépendances utilisés dans un produit. Il permet de mieux connaître la composition des logiciels déployés, d'identifier rapidement les composants vulnérables, et de faciliter la gestion des mises à jour et des correctifs
- **Renseignements sur le fournisseur :** l'inventaire doit inclure des informations sur les fournisseurs, comme les points de contact, les conditions de garantie, les rappels de produits, ainsi que les informations sur les mises à jour de sécurité. Cela permet de faciliter la communication et la gestion des mises à jour critiques avec les fabricants.
- **Rôles et responsabilités documentés :** il est également indispensable de définir clairement les rôles et responsabilités associés à chaque actif. Cela concerne les personnes, équipes ou groupes qui en détiennent la propriété et ceux responsables de l'exploitation, de la maintenance, ainsi que des aspects de cybersécurité. Une documentation claire de ces responsabilités permet d'assurer une meilleure coordination et une répartition efficace des tâches de sécurité.

TYPOLOGIE, IMPORTANCE ET CLASSIFICATION DES ACTIFS

Pour établir un inventaire complet et pertinent, il est essentiel de répertorier tous les actifs impliqués dans les processus industriels. Cela inclut aussi bien les éléments matériels que les logiciels : stations de travail, serveurs, équipements réseau (routeurs, commutateurs, pare-feu), automates programmables (PLCs), systèmes de contrôle distribué (DCS), stations HMI, machines virtuelles, conteneurs, bases de données, annuaires LDAP, et autres équipements critiques. L'inventaire doit également prendre en compte les actifs de remplacement utilisés pour la maintenance, car ils assurent la continuité de service en cas de défaillance.

Les actifs répertoriés présentent des connectivités variées, telles que des connexions à des réseaux de gestion ou industriels, des actifs isolés (air-gap), ou encore des actifs hébergés dans le cloud. La diversité de ces connectivités influence la manière dont les actifs sont exposés aux menaces et doit être prise en compte dans la gestion de la sécurité.

Au-delà de la simple identification, une classification approfondie des actifs est nécessaire pour prioriser les efforts de sécurisation. Cette classification repose sur plusieurs critères, comme le groupe d'appartenance, le système d'exploitation, le type de matériel, ou encore le rôle de chaque actif au sein du système d'information (SI). Les équipes responsables, en collaboration avec les métiers, doivent comprendre le fonctionnement des procédés industriels et la place de chaque actif dans la chaîne de production. Cela permet de définir la criticité de chaque actif et de mieux cibler les efforts de sécurité.

Cette contextualisation des informations d'inventaire permet également de fixer les niveaux d'exigence en termes de confidentialité, intégrité et disponibilité.

MÉTHODES DE CONSOLIDATION

Pour créer et maintenir cet inventaire, il est essentiel de s'appuyer sur une combinaison d'outils automatisés et de procédures manuelles. Dans les environnements industriels, tous les actifs ne sont pas détectables via les protocoles classiques (par exemple, Profibus,

[28] §6.1.1 de Guide to Operational Technology (OT) Security: NIST Requests Comments (csrc.nist.gov)

Modbus RTU, LLDP, ...), ce qui complexifie la détection automatique.

Ainsi, une découverte automatisée à l'aide de solutions spécialisées est souvent une première étape. Ces outils permettent de recenser les actifs connectés aux réseaux et de mettre à jour les informations de manière continue.

Cependant, selon le niveau d'accessibilité des actifs, des procédures de découverte manuelle peuvent être nécessaires pour compléter cet inventaire. Cela concerne particulièrement les actifs non connectés (air-gapped), pour lesquels il est nécessaire de relever directement les informations sur site. Une approche hybride, alliant compétences IT et OT, est recommandée pour garantir une vision complète de l'ensemble des actifs.

Deux approches principales se distinguent :

- **Analyse passive :** reposant sur des sondes d'écoute, cette méthode identifie les actifs sans interférer avec leur fonctionnement. Les informations des sondes correspondent à l'utilisation réelle des équipements sur site. Elle est particulièrement adaptée aux environnements sensibles, mais nécessite un travail régulier pour ajuster le placement des sondes et garantir une couverture complète.
- **Analyse active :** cette approche consiste à utiliser des outils interagissant directement avec les actifs (avec ou sans agent). Les requêtes sécurisées (« safe queries ») sont à privilégier pour éviter tout risque de perturbation des systèmes lors des analyses.

Il n'existe pas d'outil unique capable de réaliser un inventaire exhaustif des actifs OT. En pratique, il est nécessaire de combiner plusieurs approches, notamment les méthodes actives et passives. L'analyse active permet, en outre, de mieux identifier les vulnérabilités existantes sur le produit si la version n'est pas accessible par la recherche passive. L'analyse passive évite d'interférer avec le système en régime nominal, les sources d'informations existantes telles que les bases CMDB (Configuration Management Database), ainsi que des inventaires manuels. Cette combinaison permet d'obtenir une vue claire et fiable de l'inventaire des actifs, essentielle pour une gestion efficace de la cybersécurité OT.

Enfin, en intégrant un SBOM dans le processus d'inventaire, les organisations s'assurent de disposer d'une vision claire de tous les composants logiciels présents dans leur infrastructure. Cela devient essentiel pour identifier rapidement les vulnérabilités lorsqu'un composant logiciel est signalé comme vulnérable, et pour mettre en œuvre les correctifs nécessaires sans délai, renforçant ainsi la résilience de l'ensemble de l'écosystème industriel face aux menaces.

4.3 GESTION CONTINUE DES ACTIFS ET DES CONFIGURATIONS

MISE À JOUR DE LA CARTOGRAPHIE ET DE L'INVENTAIRE

La mise à jour régulière de la cartographie et de l'inventaire des actifs est essentielle pour garantir une posture de cybersécurité robuste dans un environnement industriel en constante évolution. Une cartographie précise permet de suivre les nouveaux actifs intégrés, les équipements retirés, ainsi que les modifications de configuration ou de version logicielle. Un inventaire obsolète représente un risque majeur, car il peut laisser des vulnérabilités non détectées, augmentant ainsi l'exposition aux cyberattaques.

Dans les environnements industriels dynamiques, où les équipements ou les configurations changent fréquemment, une surveillance de l'inventaire à une cadence hebdomadaire ou bi-hebdomadaire est recommandée. Cette régularité permet de réagir rapidement aux évolutions. En revanche, pour les environnements dits « qualifiés », les cycles de mise à jour peuvent être plus espacés, parfois de plusieurs mois, en raison de la stabilité des configurations et des exigences de conformité.

Pour assurer la mise à jour continue de l'inventaire, il est crucial de centraliser les informations des actifs connectés et non connectés sur une même plateforme. Cette centralisation offre une vue d'ensemble des vulnérabilités potentielles. Les actifs connectés, qui peuvent être découverts et surveillés automatiquement, sont plus simples à maintenir à jour. Pour les actifs isolés (« air-gapped »), leur mise à jour peut nécessiter des interventions sur site pour relever manuellement les informations, une démarche indispensable pour inclure tous les actifs dans la stratégie de sécurité.

GESTION DE LA CONFIGURATION DES ACTIFS

La gestion de la configuration vise à garantir que chaque composant de l'infrastructure (systèmes, serveurs, applications, périphériques réseau, etc.) reste dans un état conforme aux exigences de sécurité et de performance. Ce processus assure la continuité des opérations, même après des modifications au fil du temps, telles que des mises à jour logicielles, des changements de paramètres ou des remplacements d'équipements.

Les outils de gestion de configuration facilitent cette tâche en permettant de centraliser les opérations de modification, d'assurer la traçabilité des changements et de déployer de nouveaux paramètres sur l'ensemble des systèmes concernés. Ces outils automatisent également l'identification des configurations obsolètes ou non conformes et la priorisation des actions correctives. Cela contribue à maintenir la cohérence de l'infrastructure et à réduire le risque de dysfonctionnements.

Les entreprises peuvent ainsi appliquer des correctifs issus de catalogues de standards, gérer les mises à jour des configurations de manière sécurisée et suivre l'état des équipements en temps réel. Cette gestion proactive des configurations, en lien avec la mise à jour régulière de la cartographie, permet de mieux anticiper les risques et d'assurer un maintien en condition de sécurité sur le long terme.

La sécurisation des configurations joue un rôle fondamental dans la réduction des risques liés aux cybermenaces. En combinant le renforcement des configurations, qui consiste à désactiver les services inutiles, modifier les paramètres par défaut et appliquer des mesures de durcissement adaptées, avec des tests réguliers de conformité basés sur des référentiels reconnus comme les benchmarks CIS, les organisations peuvent maintenir un haut niveau de sécurité. Cette approche proactive garantit que les systèmes, serveurs et équipements réseau restent alignés sur les meilleures pratiques, renforçant ainsi leur résilience face aux attaques potentielles.

4.4 CLASSIFICATION ET CONTEXTUALISATION

La contextualisation des informations d'inventaire est essentielle pour hiérarchiser efficacement les vulnérabilités et prioriser les actions correctives correspondantes.

Tout d'abord, l'équipe en charge du SI, en collaboration avec les responsables métier, doit comprendre le fonctionnement du procédé industriel et ses contraintes spécifiques. Cette compréhension permet d'évaluer la fonction de chaque actif dans le processus industriel global et donc sa criticité au sein de la chaîne de production. Une classification rigoureuse des actifs est alors nécessaire, segmentant ceux-ci par groupes, systèmes d'exploitation, logiciels, matériels, et type d'actif (industriel, bureautique, IT for OT, etc.). Cette classification facilite le filtrage des actifs selon des critères pertinents, comme leur importance pour la sécurité, leur conformité à une réglementation spécifique, ou encore leur impact potentiel sur la production. Ce contexte industriel précis permet de définir des niveaux d'exigences clairs en matière de confidentialité, d'intégrité et de disponibilité, tout en intégrant d'autres paramètres environnementaux, comme ceux reflétés dans le score CVSS.

Ensuite, le moyen d'accès à l'actif constitue un facteur structurant du contexte. Il est crucial d'identifier les vecteurs d'accès : par le réseau, un réseau adjacent, un accès local, ou uniquement physique dans le cas d'actifs isolés. Par exemple, un réseau segmenté et supposément isolé d'Internet peut rester vulnérable si des connexions adjacentes permettent des mouvements latéraux, même à travers des pares-feux. D'autres points critiques incluent les privilèges d'accès (authentifiés ou non) et les interactions utilisateur nécessaires.

Enfin, plusieurs éléments supplémentaires influencent la gestion des actifs, tels que la redondance des équipements, les recommandations des fournisseurs de technologie, et les fenêtres de maintenance disponibles pour effectuer des interventions. En prenant en compte ces dimensions, les organisations peuvent mieux structurer leurs efforts de sécurisation et de gestion des vulnérabilités.

5 / DEUXIÈME PILIER : IDENTIFICATION DES VULNÉRABILITÉS ET CORRECTIFS

L'identification des vulnérabilités constitue le second pilier essentiel pour maintenir la sécurité des systèmes industriels. L'objectif est de recueillir des informations fiables et structurées sur les vulnérabilités et correctifs, permettant une évaluation précise de l'état de l'infrastructure et une prise de décision éclairée quant aux actions de remédiation. La capacité à cibler les informations pertinentes, issues de sources de confiance, est cruciale pour éviter un flux de données superflu et agir efficacement face aux menaces.

Dans le domaine de la cybersécurité industrielle, une base de connaissances efficace se construit en combinant des données publiques disponibles avec des informations spécifiques et souvent confidentielles fournies par les fabricants et les éditeurs de logiciels.

5.1 RECUEIL DES INFORMATIONS SUR LES VULNÉRABILITÉS

Les informations sur les vulnérabilités des systèmes et équipements industriels sont en partie accessibles au public. Généralement, les éditeurs de logiciels et les fabricants rendent ces informations publiques après avoir identifié des correctifs ou des mesures d'atténuation robustes, protégeant ainsi les utilisateurs contre d'éventuelles exploitations avant publication. Cette approche permet de limiter les risques tout en assurant une certaine transparence.

Les vulnérabilités émergentes sont généralement publiées sur des sites de référence tels que :

- CVE pour la base des vulnérabilités communes (https://www.cve.org/) ;
- NVD NIST pour les détails techniques (https://nvd.nist.gov/vuln).

La base de données du NVD publie régulièrement plusieurs centaines de vulnérabilités chaque semaine, rendant essentielle l'agrégation d'informations et la sélection des vulnérabilités pertinentes pour le système d'information industriel. Pour les responsables cybersécurité, l'enjeu est d'agréger efficacement ces informations issues de différentes sources, puis de les croiser avec l'inventaire des actifs afin de filtrer les vulnérabilités pertinentes et agir en conséquence.

Pour optimiser cette sélection et évaluer la gravité et l'exploitabilité des vulnérabilités, les équipes de sécurité peuvent également s'appuyer sur des indicateurs, tels que :

- Le score CVSS pour mesurer la criticité technique des vulnérabilités (notons l'arrivée d'un nouveau standard v4.0 mi-2024, https://www.first.org/cvss/) ;
- Le score EPSS pour évaluer la probabilité d'exploitation d'une vulnérabilité dans les 30 prochains jours ("Exploit Prediction Scoring System", https://www.first.org/epss/) ;
- Les alertes de vulnérabilités exploitées publiées par des agences, comme le catalogue KEV du CISA, les alertes de l'ANSSI CERT-FR (https://www.cert.ssi.gouv.fr/ et cert.ssi.gouv.fr/feed/scada/), d'autres agences européennes : NCSC (UK), CCN-CERT (ES) ou CSIRT (IT) ainsi que des CERT sectoriels comme le CERT Santé en France.

Pour une veille complète sur l'état de la menace et les codes exploitables disponibles en ligne ou sur le dark web, il est intéressant de consulter des sources spécialisées. Des bases de données telles que Exploit Database, Metasploit, et Packet Storm Security fournissent des informations sur les codes d'exploitation connus, permettant une meilleure anticipation des risques.

Enfin, au-delà de la veille en elle-même, lors de sessions de tests d'intrusion (pentest) ou au cours de l'utilisation des systèmes, il est possible de découvrir des vulnérabilités qui ne sont pas encore documentées ou rendues publiques. Ces vulnérabilités, dites « zero-day », sont particulièrement recherchées par les attaquants pour leur valeur stratégique, car elles échappent à la vigilance des gestionnaires de systèmes IT et OT. Lorsqu'une telle vulnérabilité est finalement rendue publique et présente un impact majeur — comme ce fut le cas avec la vulnérabilité Log4j[29] — des actions de mitigation doivent être rapidement mises en place.

5.2 ANALYSE DES DONNÉES DES CORRECTIFS

Les fabricants et éditeurs de logiciels sont de plus en plus proactifs dans la notification des correctifs de sécurité, mais il revient à l'utilisateur final de vérifier la disponibilité des mises à jour applicables et de déterminer leur pertinence. Ce processus de vérification peut être manuel et fastidieux, impliquant des recherches via plusieurs canaux : appels, emails, notes de version, flux RSS, et bases de données en ligne.

[29] [MaJ] Vulnérabilité dans Apache Log4j – CERT-FR (ssi.gouv.fr)

À noter que certains fournisseurs limitent la disponibilité des informations de correctifs à leurs clients sous contrat de maintenance. Heureusement, des outils automatisés permettent d'agréger et de filtrer ces informations.

La lecture des notes de version et l'examen des informations publiées par les fabricants sont essentiels pour déterminer la nature exacte d'un correctif. Les informations supplémentaires sur les correctifs, comme les dates de publication, la nature des changements apportés (correction de failles ou ajout de nouvelles fonctionnalités de sécurité), la liste des vulnérabilités traitées, ou encore le type (cumulatif ou nécessitant d'autres correctifs antérieurs), apportent des indications utiles à la décision d'appliquer ou non une mise à jour.

Parfois, les correctifs sont publiés avant la divulgation complète de la vulnérabilité ; il est donc avantageux de suivre simultanément les bases de données de vulnérabilités et de correctifs et de consolider les informations régulièrement.

Lors d'un téléchargement de correctif, il est impératif de vérifier chaque fichier pour s'assurer de son authenticité, de son intégrité et de l'absence de code malveillant. Les correctifs doivent être stockés dans un dépôt sécurisé et conformes aux standards de sécurité de l'organisation.

L'effort de collecte des données de correctifs auprès de tous les fournisseurs impliqués dans une organisation industrielle exige une planification rigoureuse et des ressources conséquentes. Cette méthodologie centralisée favorise une vision claire et simplifiée des vulnérabilités et correctifs, garantissant une protection optimale et une gestion continue des risques dans un contexte de cybersécurité industrielle.

Il est essentiel de mettre en place un modèle de données structuré, intégré au processus de maintien en condition de sécurité. Ce modèle doit permettre une organisation claire et efficace des informations liées aux correctifs.

Pour chaque correctif, il est nécessaire de :

- Identifier leur disponibilité : assurer un suivi précis des correctifs publiés par les différents fournisseurs.
- Évaluer leur applicabilité : vérifier si le correctif concerne les systèmes et versions spécifiques installés dans l'environnement OT.
- Valider les recommandations du fournisseur : confirmer si le fournisseur recommande l'installation du correctif sur les systèmes concernés.

Les informations fournies par les différents fabricants peuvent être hétérogènes et présentées dans des formats variés. La norme IEC 62443-2-3 définit les informations essentielles pour une gestion rigoureuse des correctifs :

- Identification du fournisseur : nom et informations associées.
- Produit et version : détails précis des systèmes et composants concernés.
- Compatibilité avec d'autres composants logiciels : informations sur l'OS ou autres logiciels nécessaires.
- Applicabilité du correctif : identification des systèmes ciblés.
- Validation des correctifs par le fournisseur : détails sur les tests effectués pour garantir la fiabilité et la sécurité des correctifs.

Pour centraliser ces données, il est recommandé de créer un fichier VPC (Vendor Patch Compatibility). Ce fichier doit structurer les informations selon le schéma proposé par la norme IEC 62443-2-3.

6 / TROISIÈME PILIER : DÉFINITION DU PLAN DE REMÉDIATION

La définition d'un plan de remédiation est une étape clé pour réduire l'exposition aux risques cyber dans les infrastructures industrielles. Après avoir collecté toutes les informations sur les actifs, les vulnérabilités et les correctifs disponibles, il est nécessaire de décider et prioriser les actions à mettre en œuvre. En effet, il est impossible de déployer toutes les mesures correctives simultanément, ce qui exige de se concentrer sur les plus urgentes.

Dans les environnements OT, cette planification est particulièrement complexe en raison de plusieurs contraintes opérationnelles : la nécessité de maintenir la continuité de la production, la disponibilité limitée des équipements, la rotation du personnel souvent en 3x8, ainsi que la qualification des systèmes, la compatibilité logicielle et la gestion des compétences nécessaires pour appliquer les correctifs. Ces facteurs imposent une organisation rigoureuse pour coordonner les actions de remédiation.

6.1 APPROCHE FONDÉE SUR LA GESTION DES RISQUES

Au regard du volume de vulnérabilités à traiter, une approche basée sur la gestion des risques est essentielle. Par exemple, face à une vulnérabilité avec un score CVSS (Common Vulnerability Score System) élevé sur un système non critique et une autre moins élevée sur un système de mesure de CO_2 essentiel à la sécurité des personnels, on privilégiera la correction du système de mesure. Bien que son score CVSS soit plus bas, sa criticité pour les opérations et la sécurité de la production le rend prioritaire. Cette méthodologie permet de hiérarchiser les actions de remédiation en tenant compte des contraintes spécifiques aux environnements industriels.

La gestion des risques constitue le socle de toute planification de remédiation. Elle permet de mieux évaluer l'impact des vulnérabilités et de guider les décisions de manière éclairée. Si une analyse de risques existe déjà, elle doit être exploitée pour ajuster le plan de remédiation en fonction des nouvelles vulnérabilités identifiées. En l'absence d'une telle analyse, il est conseillé de la mener dans le cadre du Maintien en Condition de Sécurité (MCS), en s'appuyant sur des normes reconnues comme ISO 27005, EBIOS-RM[30], IEC 62443-3-2 ou NIST SP 800-82r3.

L'approche basée sur les risques présente plusieurs avantages pour le traitement des vulnérabilités :

- Identifier précisément l'impact d'une nouvelle vulnérabilité sur les systèmes industriels ;
- Évaluer l'efficacité des mesures de sécurité existantes et repérer les zones à renforcer ;
- Estimer l'incidence d'une modification planifiée sur le profil de risque global ;
- Réduire les risques en appliquant des mesures correctives adaptées pour améliorer la cybersécurité ;
- Prioriser les actions de remédiation en concentrant les efforts sur les plus urgentes.

[30] L'ANSSI met à jour la méthode EBIOS Risk Manager | ANSSI (cyber.gouv.fr)

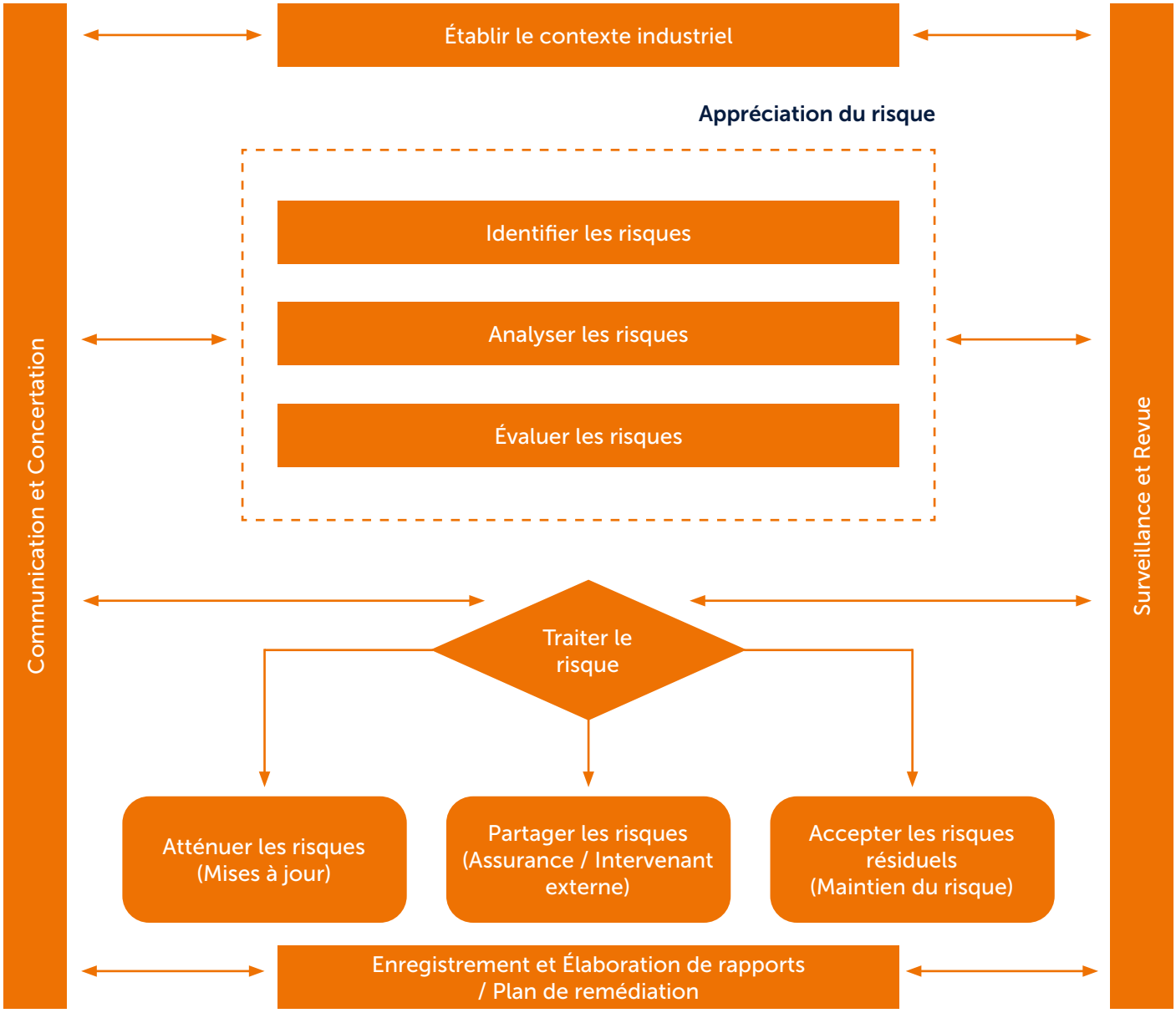


Figure 8 : Processus classique d'analyse et traitement des risques

Une approche basée sur les risques permet de traiter les vulnérabilités de plusieurs manières :

- accepter le risque et ne pas intervenir, lorsque celui-ci est jugé faible ou acceptable ;
- atténuer le risque en appliquant des mesures correctives qui réduisent son impact ;
- éliminer le risque en installant un correctif logiciel ou en désactivant une application vulnérable ;
- transférer le risque en modifiant l'architecture ou en isolant l'actif vulnérable.

Chaque option de remédiation doit être évaluée en termes de coût et de ressources, afin de planifier son déploiement et de s'assurer de sa faisabilité opérationnelle. Les décisions doivent être prises conjointement par les équipes de sécurité, les opérateurs des systèmes et les responsables de la production pour garantir une coordination efficace.

En définitive, pour une gestion efficace des risques, il est essentiel d'impliquer les parties prenantes OT/IT pour évaluer les impacts et valider le plan de traitement. Le traitement des vulnérabilités doit tenir compte de leur pertinence dans le contexte, des conséquences potentielles et de la probabilité des scénarios d'attaque.

Pour gérer les nombreuses vulnérabilités, il peut être intéressant de prioriser en combinant des indicateurs critiques par exemple : le score CVSS (gravité), le score EPSS (exploitabilité). Comme illustré dans la figure ci-dessous, les vulnérabilités qui se trouvent dans la zone sélectionnée combinent un score CVSS > 8 et un score EPSS > 5% et donc celles sur lesquelles il faut focaliser notre analyse.

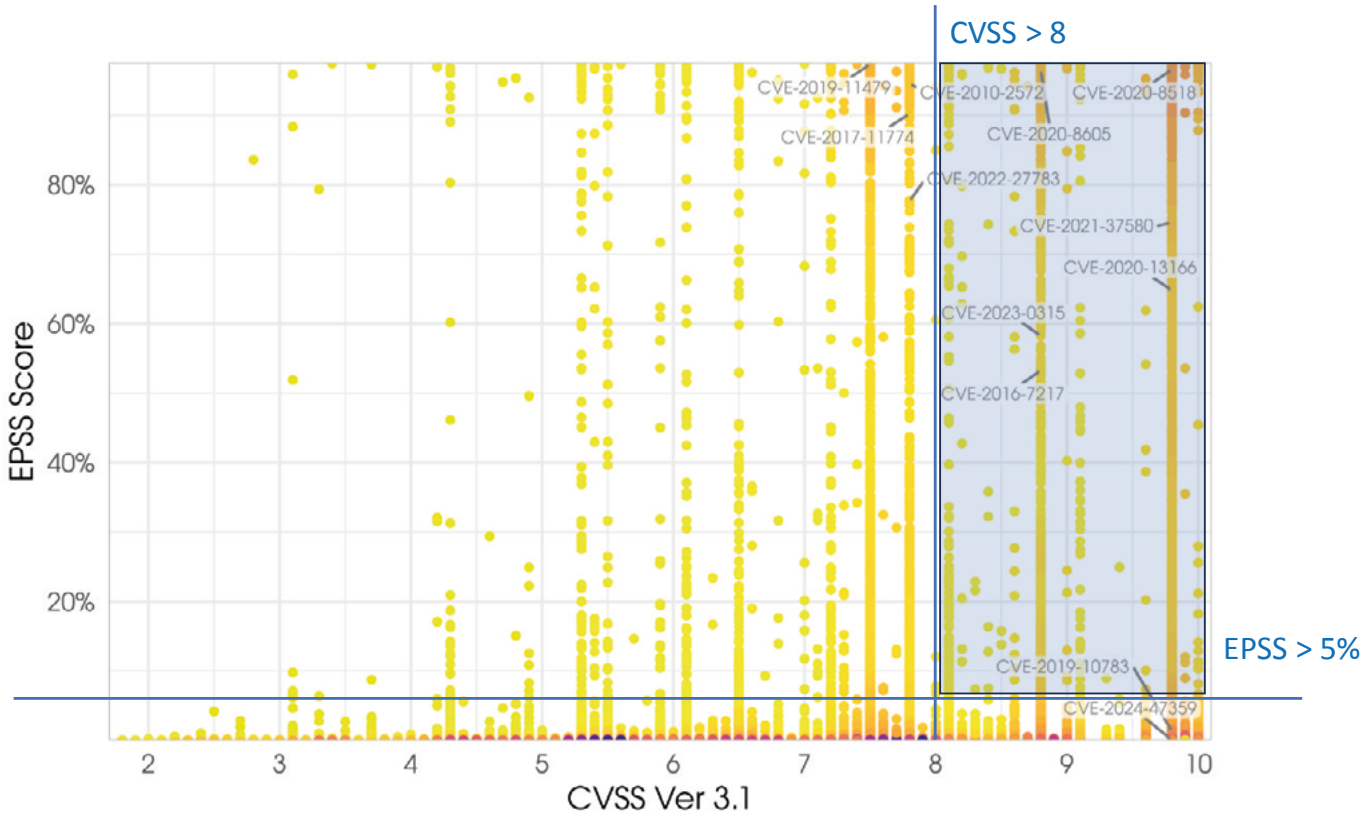


Figure 9 : Combinaison du score CVSS et EPSS pour aider à l'analyse des vulnérabilités[31]

[31] Exploit Prediction Scoring System - EPSS (first.org)

Par ailleurs, l'étude de la chaîne d'attaque est un élément crucial pour élaborer un plan de remédiation efficace. Des méthodologies variées existent, notamment le guide de modélisation de la menace publié par l'agence de cybersécurité de Singapour[32].

La composante environnementale du score CVSS (CVSS-BTE) est également un élément important de décision pour les actions correctives : Par exemple, le mode d'accès aux actifs constitue un autre critère de classification essentiel. Selon le vecteur d'accès, qu'il s'agisse de connexions réseau, de réseaux adjacents, de réseaux locaux, ou d'accès physique uniquement, le niveau de risque varie. Par exemple, un segment de réseau isolé d'Internet mais connecté à un réseau adjacent reste vulnérable aux mouvements latéraux, même si son exposition initiale paraît réduite. D'autres facteurs, tels que la redondance des équipements, les recommandations des fournisseurs, et les fenêtres de maintenance, influencent également la priorisation des actions de sécurité.

6.2 ÉLABORATION DU PLAN DE REMÉDIATION

Le plan de remédiation en cybersécurité est essentiel pour renforcer la sécurité du système d'information d'une organisation après l'identification de vulnérabilités. Voici un résumé et une clarification des étapes clés et des pratiques liées à son élaboration et à son suivi :

ÉTAPE 1 : DÉFINITION DES ACTIONS DE REMÉDIATION

Après l'analyse des processus de sécurité en place dans l'organisation : PSSI, gestion des risques, gestion des correctifs, etc., on peut définir les actions de remédiation par ordre de priorité.

Il convient de définir la méthode de remédiation à entreprendre (application de correctifs, segmentation ou isolation du réseau, mesures de durcissement, etc...) et identifier les actifs concernés par chaque méthode de remédiation.

ÉTAPE 2 : KPIs DE SÉCURITÉ

Ces indicateurs aident à évaluer les progrès du plan de remédiation et à ajuster les actions au besoin (cf. § 3.2 Identification des besoins de MCS.

ÉTAPE 3 : STRUCTURATION DU PLAN DE REMÉDIATION

Le plan doit être détaillé et structuré :

- **Méthodes de remédiation :** choisir les actions à entreprendre (correctifs, segmentation, atténuation) ;
- **Ressources nécessaires :** déterminer les moyens humains, techniques et financiers nécessaires ;
- **Plan d'actions détaillé :** organiser les actions dans un calendrier précis avec des étapes de déploiement basées sur les priorités ;
- **Répartition des responsabilités :** définir clairement les rôles de chaque acteur impliqué dans la remédiation.

6.3 MESURES DE DURCISSEMENT ET D'ATTÉNUATION DU RISQUE

Le durcissement des systèmes OT vise à réduire les vulnérabilités et à renforcer leur résilience face aux cyberattaques. Voici des exemples de pratiques de durcissement applicables :

- **Segmentation réseau :** adopter une architecture en zones et conduits, conformément au modèle IEC 62443, pour isoler les différentes parties du réseau OT et limiter les risques de propagation d'une attaque. L'objectif est de gérer les flux entrants et sortants : par exemple on peut coupler un dispositif de coupure protocolaire physique en amont d'un pare-feu.
- **Contrôle des accès :** restreindre les privilèges d'accès aux seuls utilisateurs et dispositifs indispensables afin de réduire les points d'entrée potentiels. Par exemple éviter les connexions distantes ouvertes en permanence. Maîtriser les accès distants avec des outils et procédures de type intervention "à 4 mains" ou processus "à 4 yeux".
- **Durcissement des configurations :** appliquer des configurations sécurisées sur tous les dispositifs OT, en désactivant les services non essentiels et en renforçant les paramètres de sécurité.
- **Surveillance et journalisation des accès :** mettre en œuvre des mécanismes pour surveiller (Exemple : mettre en place une sonde pour monitorer l'activité du système et remonter des alertes), enregistrer et

[32] Guide-to-cyber-threat-modelling.pdf (csa.gov.sg)

contrôler les accès aux systèmes OT (plateformes SIEM).

Les standards de durcissement, comme ceux fournis par le CIS[33] (benchmarks pour les systèmes Linux, MacOS et Windows), l'ANSSI (sécurisation des Active Directory[34]) ou le NIST (SP 800-53 rev5[35], SP 800-41 rev1[36]), sont des références clés pour appliquer des mesures préventives. Le contrôle d'accès physique est également crucial pour limiter les risques d'accès non autorisé aux systèmes critiques.

Les mesures d'atténuation visent à minimiser les conséquences des cyberattaques lorsqu'elles surviennent. Voici quelques exemples concrets :

- **Plan de réponse aux incidents :** élaborer et maintenir des plans de réponse spécifiques aux systèmes OT, et organiser des exercices réguliers pour entraîner le personnel à réagir efficacement face à un incident.
- **Plans de continuité et de reprise (PRA/PCA) :** préparer des stratégies pour assurer la continuité des opérations et la reprise rapide après un incident.
- **Redondance et résilience :** concevoir les systèmes OT avec des composants redondants afin d'assurer la continuité des opérations en cas de défaillance ou d'attaque.
- **Isolation des systèmes compromis :** prévoir des mécanismes pour segmenter et isoler rapidement les parties du réseau OT affectées, afin d'empêcher la propagation de la menace.
- **Gestion des sauvegardes :** effectuer des sauvegardes régulières des systèmes et des données critiques, et s'assurer de leur disponibilité pour une restauration rapide.
- **Surveillance des anomalies :** configurer des alertes en temps réel pour signaler les activités suspectes ou anormales et permettre une intervention immédiate.
- **Partenariats et collaboration :** participer à des forums ou groupes d'échange sur les cybermenaces OT et collaborer avec d'autres entreprises pour développer des stratégies de défense communes.
- **Formation et sensibilisation :** former le personnel pour mieux gérer les risques de cybersécurité.
- **Tests de pénétration réguliers :** évaluer en permanence les points faibles de l'organisation.
- **Restriction des services :** désactivation des services non nécessaires sur les machines pour limiter la surface d'attaque.

Lorsque les mesures précédentes ne suffisent pas, le remplacement d'un système obsolète par un système à jour peut être envisagé.

Ces approches combinent prévention et réactivité pour renforcer la sécurité des systèmes OT face à des menaces toujours plus sophistiquées.

6.4 APPLICATION DES CORRECTIFS ET MISES À JOUR LOGICIELLES

Lorsqu'un correctif est disponible pour une vulnérabilité, sa mise en œuvre doit être soigneusement planifiée. Les critères à prendre en compte incluent :

- **Contraintes de production :** la possibilité d'appliquer les correctifs lors des périodes d'arrêt planifié de la production doit être vérifiée pour éviter toute interruption non prévue.
- **Systèmes redondants :** la présence de systèmes de secours ou de redondance permet une meilleure gestion des mises à jour sans impact direct sur la continuité des opérations.
- **Défense en profondeur :** ajouter plusieurs techniques de protection cumulés en faisant de la sécurité physique, ajout de pare-feux, appliquer de la segmentation réseau, installer des logiciels antiviraux, sécuriser les applications, les données et même faire de la sensibilisation auprès des utilisateurs.
- **Compatibilité logicielle :** avant d'appliquer un correctif, il est nécessaire de tester sa compatibilité avec les autres systèmes adjacents pour éviter des problèmes d'interopérabilité.
- **Validation du fournisseur :** si un équipement est sous contrat de maintenance, l'approbation du fournisseur peut être nécessaire pour garantir la compatibilité et la continuité de la couverture de garantie.
- **Conformité réglementaire :** dans certains secteurs (comme le nucléaire ou la pharmaceutique), un processus de validation interne ou un audit préalable peut être exigé avant l'application de correctifs.
- **Disponibilité des ressources :** la disponibilité du personnel qualifié et le temps nécessaire pour effectuer la mise à jour doivent être pris en compte pour s'assurer que l'opération peut être menée à bien.

[33] CIS Benchmarks (cisecurity.org)
[34] Points de contrôle Active Directory – CERT-FR (ssi.gouv.fr)
[35] SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC (nist.gov)
[36] SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy | CSRC (nist.gov)

6.5 PROGRAMME DE GESTION DE LA REMÉDIATION

La mise en œuvre d'un programme de gestion de la remédiation est une composante clé de la Politique de Sécurité des Systèmes d'Information (PSSI) de l'organisation. Ce programme vise à planifier, tester, et déployer les correctifs de manière structurée pour assurer la sécurité des systèmes tout en respectant les contraintes opérationnelles spécifiques aux environnements industriels. La norme IEC 62443 2-3 est la norme de référence pour établir un tel programme. Elle fournit un cadre précis pour gérer les correctifs de manière adaptée à la réalité des systèmes industriels.

Les principaux éléments à inclure dans un programme de gestion des correctifs, conformément à cette norme, sont les suivants :

- **Politiques, processus et procédures autour de la gestion des correctifs de sécurité :** il est essentiel de définir clairement les protocoles à suivre pour identifier, évaluer et appliquer les correctifs de sécurité, afin de garantir la cohérence des actions entreprises.
- **Informations sur les fournisseurs de technologie (IACS) :** cela inclut la documentation et le suivi des recommandations des fournisseurs, permettant d'assurer que les correctifs appliqués soient compatibles avec les spécificités des équipements industriels.
- **Sauvegardes avant et après application des correctifs :** réaliser des sauvegardes avant l'application des correctifs permet un retour à un état antérieur en cas de défaillance. Une vérification post-application assure l'intégrité des modifications.
- **Mesures d'atténuation en cas d'impossibilité d'application :** la norme prévoit des alternatives lorsque les correctifs ne peuvent être appliqués immédiatement. Ces mesures peuvent inclure l'isolement des systèmes vulnérables ou le renforcement temporaire de la sécurité.
- **Tests et validation des correctifs avant leur installation en production :** pour éviter les effets indésirables, la norme recommande de tester les correctifs sur un environnement proche de la production avant leur déploiement effectif.
- **Fenêtres de temps planifiées pour les installations :** les correctifs doivent être appliqués durant des périodes planifiées pour minimiser l'impact sur la production, garantissant ainsi que les activités critiques ne soient pas perturbées.
- **Documentation détaillée des opérations :** chaque intervention doit être documentée avec précision, y compris les problèmes rencontrés et les solutions apportées, pour garantir la traçabilité et la continuité des opérations.
- **Politique pour l'application des correctifs de sécurité et des correctifs fonctionnels :** le programme de gestion des correctifs doit inclure une politique claire pour l'application de correctifs de sécurité (visant à réduire les vulnérabilités) ainsi que les correctifs fonctionnels (qui améliorent les fonctionnalités ou corrigent des anomalies). Cette politique définit les priorités et les critères pour chaque type de correctif, assurant une gestion équilibrée entre sécurité et maintien des fonctionnalités.

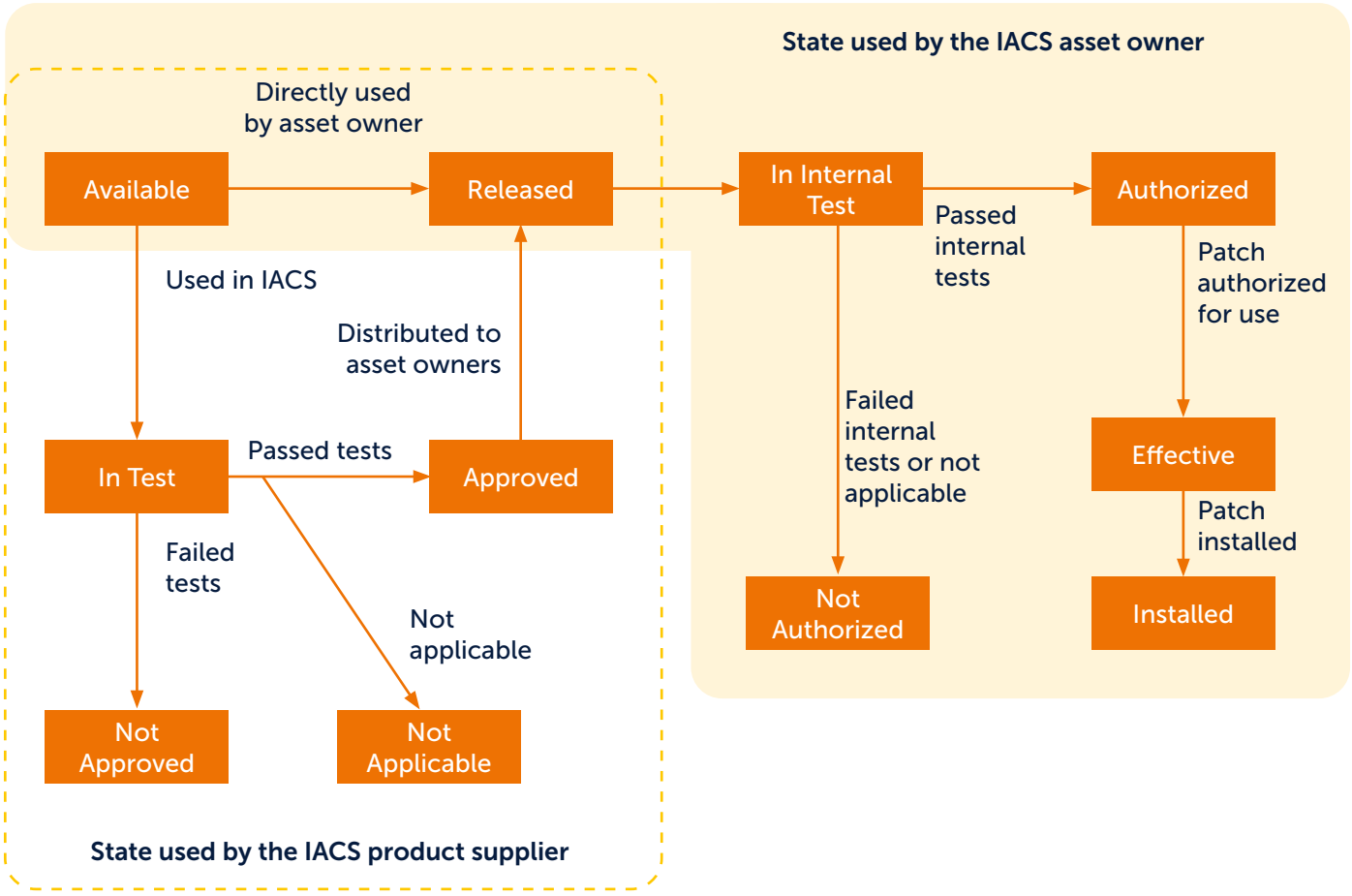


Figure 10 : Modèle de cycle de vie des correctifs proposé dans le standard IEC 62443-2-3

Cette approche permet de structurer le processus de gestion des correctifs en assurant la sécurité tout en maintenant la continuité des opérations industrielles. Cependant, d'autres référentiels apportent des compléments utiles pour gérer les spécificités de certains environnements industriels, tel que celui du Department of Homeland Security (DHS), dans son document sur le Patch Management of Control Systems[37]. Cette approche apporte plusieurs éléments de valeur qui viennent enrichir le cadre défini par la norme IEC 62443-2-3 :

- **Programme de gestion de la configuration :** le DHS insiste sur l'importance d'un suivi documenté et tracé des configurations des systèmes et logiciels utilisés. Cela permet de mieux gérer les dépendances et de maintenir une cohérence des versions des logiciels et des configurations, ce qui est crucial pour comprendre l'impact potentiel des correctifs sur les systèmes. Pour plus d'information sur ce sujet, on peut trouver des informations détaillées sur la gestion de configuration dans le §3 .5 du guide NIST 800-53, Rev 5[38].
- **Plan de gestion des sauvegardes/archives :** bien que la norme IEC 62443-2-3 mentionne la nécessité de sauvegardes, le DHS approfondit cette exigence en détaillant les fréquences de sauvegarde, la création d'archives, les périodes de rétention, ainsi que la gestion physique des supports de sauvegarde. Cela renforce la résilience face aux incidents de sécurité en assurant une restauration rapide et fiable.

[37] Recommended Practice for Patch Management of Control Systems (cisa.gov)
[38] Security and Privacy Controls for Information Systems and Organizations (nist.gov)

- **Test et validation des correctifs sur un banc d'essai dédié :** le DHS met particulièrement l'accent sur la nécessité de recréer des environnements de test proches de la réalité industrielle pour valider les correctifs. Ce processus permet de simuler les interactions entre les différentes applications et équipements avant de déployer les mises à jour, réduisant ainsi les risques d'interruption en production.
- **Plan de reprise d'activité :** le DHS met en avant l'importance de disposer d'une infrastructure de secours qui peut être utilisée pour tester les correctifs. Cela permet de valider les actions correctives de manière sécurisée tout en vérifiant la capacité de reprise à partir des sauvegardes.
- **Application par unités de production :** l'approche du DHS propose une gestion par unités en mode nominal-backup ou production parallèle, permettant ainsi de tester les correctifs sur des unités non critiques avant de les appliquer à celles en production. Cette méthode assure une transition en douceur et minimise les interruptions.

Le cadre de la norme IEC 62443-2-3 fournit une base structurée pour la gestion des correctifs, avec un accent sur la documentation, la gestion des fournisseurs, et la planification des interventions. Le « Department of Homeland Security », quant à lui, enrichit ce cadre en détaillant des aspects opérationnels et techniques, tels que la gestion avancée des configurations et des sauvegardes, ainsi que la création de bancs de tests pour valider les correctifs. En combinant ces deux approches, les organisations peuvent construire un programme de gestion des correctifs plus complet, adapté à la complexité de leurs environnements industriels. Cela permet de répondre efficacement aux exigences de sécurité tout en limitant les risques de perturbation des processus de production.

7 / QUATRIÈME PILIER : APPLICATION DE LA REMÉDIATION

7.1 GESTION DES SAUVEGARDES ET RESTAURATIONS

La sauvegarde des systèmes d'information est depuis longtemps une mesure essentielle pour limiter l'impact des incidents opérationnels, tels que les pannes matérielles ou la perte accidentelle de fichiers. Aujourd'hui, elle joue également un rôle critique dans la réponse aux incidents de sécurité. Par exemple, en cas d'attaque par rançongiciel, des sauvegardes fiables permettent de restaurer rapidement les systèmes, évitant ainsi tout recours à une négociation avec l'attaquant.

Pour garantir l'efficacité des sauvegardes, il est impératif de formaliser une politique dédiée qui couvre les aspects suivants :

- **Identification des données critiques :** liste des informations vitales pour l'organisme (images de clients et serveurs, bases de données, fichiers de configuration) ;
- **Types de sauvegardes :** inclure des sauvegardes en ligne (cloud) et hors ligne (isolées) ;
- **Fréquence des sauvegardes :** planifier des sauvegardes quotidiennes, mensuelles et annuelles selon les besoins ;
- **Procédures d'exécution :** définir les étapes d'administration et d'exécution des sauvegardes ;
- **Sécurisation des sauvegardes :** préciser les lieux de stockage, les restrictions d'accès et les mesures de protection contre les menaces (ex. : chiffrement) ;
- **Tests de restauration :** mettre en place des tests réguliers pour s'assurer de la fiabilité des sauvegardes. Ces tests d'intégrité des sauvegardes doivent être complétés un processus de restauration complet : équipement de rechange, procédures techniques, personnel formé à la procédure de restauration, etc ;
- **Durée de rétention :** déterminer une politique adaptée, comme 15 jours de sauvegardes journalières, 1 an de sauvegardes mensuelles, et 5 ans pour les sauvegardes annuelles ;
- **Destruction sécurisée des supports :** prévoir des procédures pour la destruction des supports en fin de cycle.

L'opérateur de sauvegarde est un administrateur hautement privilégié et de confiance, disposant d'un rôle critique dans la gestion du SI OT. Afin de sécuriser l'infrastructure de sauvegarde :

- Les serveurs de sauvegarde doivent être indépendants des domaines Windows (Active Directory) de production, avec un système d'authentification distinct (comptes locaux ou annuaire dédié).
- Les composants essentiels de l'infrastructure de sauvegarde doivent être clairement définis :
  - Index des sauvegardes : permet d'identifier précisément les éléments sauvegardés ;
  - Agents logiciels : installés sur les actifs à sauvegarder pour faciliter la gestion des flux ;
  - Serveur de sauvegarde : coordonne les sauvegardes avant leur transfert vers un support ;
  - Supports de sauvegarde : disques durs, bandes magnétiques, disques externes USB, etc.

Pour renforcer la résilience des sauvegardes, il est recommandé d'appliquer la règle 3–2–1 :

- 3 copies des sauvegardes pour garantir la redondance ;
- 2 types de supports différents (par exemple, disques et bandes magnétiques) ;
- 1 copie hors ligne pour protéger contre les cyberattaques (rançongiciels, intrusions).

L'ANSSI propose un guide sur les fondamentaux de la sauvegarde des systèmes d'information[39]. Ce document constitue un excellent référentiel pour élaborer une politique de sauvegarde et de restauration conforme aux meilleures pratiques.

7.2 VALIDATION DE LA REMÉDIATION

La mise en place d'un banc d'essai pour valider les mesures de remédiation peut s'avérer coûteuse, mais son utilité reste cruciale. Une approche progressive et méthodique dans l'application des remédiations permet de renforcer la confiance tout en réduisant les risques liés à leur mise en œuvre.

Lorsqu'une nouvelle vulnérabilité est découverte dans un produit (logiciel ou matériel intégrant un logiciel), les fabricants de technologie s'efforcent de corriger rapidement le problème. Cela se fait généralement : soit via une mise à jour logicielle, soit en proposant des mesures de contention visant à atténuer

[39] Sauvegarde des systèmes d'information (cyber.gouv.fr)

temporairement le risque d'exploitation. Cependant, les correctifs et paramétrages proposés par les fabricants sont souvent testés dans des environnements standards, très différents des configurations spécifiques aux environnements industriels.

Il est donc recommandé de réaliser une validation préalable des mesures de remédiation dans un banc d'essai ou simulateur, afin de réduire les risques de dysfonctionnements imprévus susceptibles d'engendrer des coûts financiers importants (perte de production, modes dégradés, retards, pénalités). Cette validation permet aussi de renforcer la confiance des opérateurs et minimiser les imprévus lors du déploiement en production.

Un banc d'essai offre également d'autres avantages :

- **Formation des opérateurs :** permettre aux équipes de se familiariser avec les nouvelles configurations.
- **Préparation des procédures :** élaborer des listes de vérification et valider les processus avant leur application sur les systèmes de production.

Une modélisation proche de l'environnement réel est idéale pour tester les remédiations. Cependant, ce type d'installation nécessite souvent des investissements élevés, rendant cette solution non viable dans des nombreux cas. Les environnements virtuels peuvent réduire les coûts et accroître la flexibilité, mais certains équipements OT (systèmes de contrôle-commande) doivent rester physiques, car leurs versions virtualisées sont rares ou inexistantes.

Les environnements industriels, généralement hétérogènes avec des technologies provenant de plusieurs fabricants, rendent la validation encore plus indispensable. Il est également essentiel de tenir compte des interdépendances avec des modules tiers, tels que les systèmes d'exploitation (Windows/Linux) ou des applications comme Java, SQL, Oracle, .Net, Silverlight, etc.

Pour gérer cette complexité, une expertise spécialisée en intégration et validation est nécessaire, avec une compréhension approfondie des composants logiciels et matériels des solutions de chaque fabricant.

Les principales étapes pour valider l'implémentation d'un plan de remédiation sont les suivantes :

1. identifier les éléments critiques susceptibles d'impacter la production ou les flux financiers ;
2. identifier les fonctionnalités opérationnelles clés et leur criticité ;
3. créer une version minimaliste permettant de tester toutes les fonctionnalités essentielles des logiciels et matériels ;
4. préparer un cahier de tests fonctionnels ;
5. exécuter les tests fonctionnels initiaux (avant remédiation) pour établir une base de référence ;
6. réaliser une sauvegarde de l'état initial avant la remédiation ;
7. implémenter le plan de remédiation ;
8. exécuter les tests fonctionnels après remédiation ;
9. réviser le plan de remédiation en fonction des résultats :
   a. si les résultats sont satisfaisants, passer à l'étape suivante ;
   b. si les résultats sont insatisfaisants, revenir à l'état initial sauvegardé.
10. déployer la remédiation sur le site de production ;
11. effectuer une dernière série de tests fonctionnels post-remédiation.

Dans certaines industries critiques, les logiciels utilisés dans des systèmes sensibles doivent être homologués. Pour chaque modification de version logicielle ou de configuration, l'opérateur est tenu de suivre un processus rigoureux et souvent coûteux de validation approfondie et d'homologation. Ce processus vise à garantir que les modifications apportées n'affecteront pas la sécurité ou la disponibilité des systèmes critiques.

7.3 DÉPLOIEMENT DES MESURES DE REMÉDIATION

La mise en œuvre des mesures de remédiation nécessite la collaboration de toutes les parties prenantes. Les équipes de sécurité et d'exploitation doivent partager leurs préoccupations et contraintes pour définir une approche commune. Le résultat de cette concertation doit servir de base à la recommandation finale à destination de la direction, afin de corriger ou non un système de contrôle industriel.

Les équipes de production et de maintenance, en partenariat avec les fabricants ou intégrateurs

de solutions, sont directement impactées par ces opérations qui peuvent affecter la disponibilité des infrastructures.

Simultanément, les équipes du système d'information et de la cybersécurité jouent un rôle clé dans la mise en œuvre sécurisée et efficace des remédiations.

L'approche préconisée par l'ISA[40] met l'accent sur une gestion structurée des correctifs pour les systèmes OT (Operational Technology), avec les étapes suivantes :

- établissement d'une référence de base (Baseline) ;
- documentation des correctifs installés et processus associés ;
- vérification des correctifs appliqués ;
- préparation d'un plan de retour arrière pour les actifs critiques.

Cette méthodologie assure la sécurité et l'intégrité des systèmes tout en maintenant leur adaptabilité face aux évolutions.

Ensuite on peut envisager la planification et exécution des interventions.

1. PLANIFICATION DES INTERVENTIONS

- Définir les créneaux de disponibilité des systèmes : périodes de maintenance, arrêts de production ou intervention sur infrastructures redondées ;
- Informer et coordonner les équipes concernées.

2. ÉVALUATION DE LA STABILITÉ OPÉRATIONNELLE

- Établir des critères de stabilité, tels que la quantité de produits fabriqués et le temps d'exécution sans défaillance ;
- Surveiller les performances du système corrigé pour garantir l'absence de dégradations.

3. PROCÉDURES DE RETOUR ARRIÈRE

- Préparer un plan de restauration incluant des sauvegardes testées ;
- Conserver des pièces de rechange non corrigées comme solutions de secours immédiates.

Une documentation rigoureuse garantit un suivi optimal des correctifs. La documentation devra consigner les nouvelles versions et configurations et mettre à jour les politiques de sécurité et les procédures de contrôle d'accès pour refléter les évolutions technologiques et réduire les risques.

CAS SPÉCIFIQUE : MISE À JOUR DES ÉQUIPEMENTS DE SÉCURITÉ

1. MISE À JOUR DES SIGNATURES

Les signatures, créées par des équipes de Threat Intelligence, détectent les indicateurs de compromission (IOC) ou d'attaque (IOA).

- **Fréquence :** variable (de plusieurs fois par jour à une fois par heure) ;
- **Processus :** automatisation ou planification manuelle, selon les besoins du client ;
- **Systèmes isolés (air-gapped) :** distribution via un serveur DMZ ou une clé USB.

2. MISE À JOUR DES FIRMWARES

Effectuée ponctuellement par le fabricant avec une planification par l'utilisateur. Effectuer un backup complet de la configuration avant toute mise à jour.

Suivre une procédure détaillée pour maintenir la protection active sur des infrastructures redondées ou multisites.

CAS SPÉCIFIQUE : LES AUTOMATES PROGRAMMABLES

Lors des mises à jour, assurez la cohérence entre les versions des composants (CPU, coupleurs de communication, modules spécialisés). Vérifiez la compatibilité des versions entre le firmware et les composants.

Mettez à jour les plateformes logicielles et les fichiers de configuration si nécessaire.

CAS SPÉCIFIQUE : LES SYSTÈMES OBSOLOLÈTES

Dans le cas où nous avons des systèmes obsolètes (i.e. Windows XP, 7, 2000…) et pour sécuriser ces systèmes malgré leur obsolescence, plusieurs mesures peuvent

[40] §6 du lien : The Top 7 Operational Technology Patch Management Best Practices (isa.org)

être mises en place :

- Installer un logiciel de protection (EDR ou EPP) compatible avec les systèmes anciens, qui soit économe en ressources et capable de fonctionner sans connexion permanente au cloud.
- Déployer des pares-feux industriels pour bloquer les tentatives d'exploitation de vulnérabilités connues sur ces systèmes.

Le succès d'une opération de remédiation repose sur une planification rigoureuse, une documentation exhaustive et une communication efficace entre toutes les parties prenantes.

8 / RETOUR D'EXPÉRIENCE **SUR DES CAS CONCRETS**

8.1 INDUSTRIEL OEM DU TRI BAGAGE

CONTEXTE

Industriel OEM dans le secteur du tri bagage pour les marchés de l'aéroport, des magasins automatisés grande hauteur et des tri-colis dans l'intralogistique, souhaitant enrichir son offre de services maintenance industrielle avec des nouveaux produits et services de cybersécurité.

CHALLENGES / PROBLÉMATIQUE

Les défis auxquels sont confrontés les clients finaux de cet OEM sont principalement les suivants :

- Maintenir la disponibilité des processus (systèmes avec des exigences de disponibilité 24/7).
- Assurer le MCS en plus du MCO pour améliorer la sécurité et être en conformité avec les exigences réglementaires auxquelles les clients sont soumis.
  - maintenir l'inventaire des actifs à jour ;
  - surveillance des vulnérabilités ;
  - maintenir le système information à jour et le faire évoluer ;
  - surveillance de son niveau de conformité réglementaire.

PROCESSUS / OUTILS MIS EN PLACE

Mise en place d'un processus complet de MCS avec plusieurs outils et solutions :

- Solution pour réaliser l'inventaire des actifs sur une base de sondes passives et pour les enregistrer dans la base de données GMAO : version "firmware" et software, suivi des contrats de maintenance des actifs ainsi que définition du niveau de criticité de l'actif. Discussions avec les clients autour de l'utilisation des sondes, la fréquence des inventaires, la gestion de la configuration et le nommage des actifs.
- Solution pour faire l'**analyse des vulnérabilités** avec une capacité pour filtrer les meta-données et ainsi aider à la décision de la remédiation. Notamment **établir une priorisation des vulnérabilités** en fonction de la gravité, l'exploitabilité et la criticité des vulnérabilités qui affectent les différents systèmes.
- Produire un **plan de remédiation** selon les niveaux de risque résiduel, les contraintes de sûreté de l'installation, durée de l'activité OT, le management du changement, les conditions de mise en œuvre, la dette technologique et la gestion de l'obsolescence.
- Mise en œuvre de la correction avec la validation des mises à jour avant déploiement, sur le jumeau numérique process de l'installation industrielle. Puis, déploiement de la correction sur le site de production.

BÉNÉFICES ET CONCLUSIONS

- Les clients finaux ont connaissance de l'inventaire des actifs de leurs installations industrielles.
- Les clients finaux surveillent l'état de vulnérabilités de leurs installations industrielles et ainsi générer des indicateurs de performance clés pour leur conformité de sécurité.
- Ainsi les clients finaux améliorent de manière générale le MCS de leurs installation industrielle et par conséquence leur posture de sécurité.

8.2 INDUSTRIEL DANS LA GESTION DES RESSOURCES ET L'ÉCONOMIE CIRCULAIRE

CONTEXTE

Le client est un acteur clé dans la gestion des ressources et l'économie circulaire. Il exploite des sites de valorisation et retraitement des déchets et de l'eau. Le rythme et les conditions d'exploitation sont soutenus et les coupures de maintenance sont rares. Les opérationnels exploitant les sites n'ont aucune formation initiale à la cybersécurité.

CHALLENGES / PROBLÉMATIQUE

Le client fait face à l'obsolescence des systèmes de contrôle-commande de son site industriel. Ces systèmes vieillissants, malgré des mises à jour, ne répondent plus aux exigences actuelles de performance et de sécurité. Le projet vise à moderniser ces infrastructures, tout en intégrant des mesures de cybersécurité conformément aux normes IEC/ISA 62443. Les principaux défis incluent la sécurisation des flux IT/OT, la mise à jour

des systèmes obsolètes et la formation insuffisante des équipes en cybersécurité.

PROCESSUS / OUTILS MIS EN PLACE

Plusieurs solutions ont été mises en place, telles que :

- la segmentation des réseaux IT/OT ;
- le durcissement des systèmes ;
- la virtualisation des services industriels ;
- la mise en place de la traçabilité des événements.

Ces mesures ont amélioré la résilience du système, réduit les vulnérabilités, et renforcé la conformité aux normes de cybersécurité. En outre, des efforts de sensibilisation ont permis d'impliquer les équipes sur le terrain.

BÉNÉFICES ET CONCLUSIONS

Le succès du projet repose non seulement sur l'aspect technique mais aussi sur une approche humaine, prenant en compte les besoins opérationnels et favorisant une communication fluide avec les équipes, afin de garantir une intégration harmonieuse de la sécurité dans les processus industriels.

En clarifiant les risques concrets (par exemple les attaques pouvant provoquer des arrêts de production ou mettre en danger la sécurité des employés), et en démontrant comment des mesures de sécurité adaptées peuvent prévenir ces scénarios, le consultant aide à faire évoluer la perception de la cybersécurité, qui passe alors d'une contrainte à une nécessité vitale pour la pérennité du site.

Pour nous ce qui a garanti le succès de l'implantation de cette mesure, c'est une orchestration intelligente et adaptée de mesures techniques, humaines et organisationnelles avec notre client sur le site et l'équipe RSSI du groupe.

9 / CONCLUSION

Le Maintien en Condition de Sécurité (MCS) joue un rôle central dans la protection des actifs industriels, des données critiques et des personnes. Au-delà de la sécurisation des infrastructures, il contribue directement à améliorer la productivité de manière performante et maîtrisée. Toutefois, cette démarche exige une réflexion approfondie et une mise en œuvre rigoureuse, excluant toute improvisation.

Pour un MCS efficace, il est essentiel de :

- bien connaître son système d'information (SI) grâce à une cartographie exhaustive et mise à jour ;
- allouer des ressources de veille pour surveiller les vulnérabilités et identifier les mesures correctives adéquates ;
- adopter une gestion proactive des risques, en anticipant les scénarios les plus défavorables lors des opérations de remédiation.

L'application d'un plan de remédiation bien conçu repose sur des bases solides, mais il est également crucial de reconnaître que le MCS est un processus continu. La dynamique des menaces et l'évolution des technologies imposent une vigilance constante et une analyse régulière pour maintenir un haut niveau de sécurité.

Si les ressources internes manquent de formation ou d'expérience pour évaluer et implémenter des mesures de remédiation, l'externalisation peut être une solution rentable. Faire appel à des fournisseurs de services logiciels gérés (Managed Service Providers) permet de confier à des experts la gestion des tâches critiques : correction, configuration, déploiement et restauration des systèmes.

Enfin, le MCS doit être perçu comme un pilier évolutif de la stratégie de sécurité. Cette démarche illustre la nécessité d'une amélioration continue pour répondre aux enjeux actuels et futurs, garantissant ainsi la résilience des environnements industriels et la sécurité des opérations sur le long terme.

10 / GLOSSAIRE

Acronyme	Définition
ANSSI	Agence Nationale pour la Sécurité des Systèmes d'Information. Organisation gouvernementale
Actif	Équipements informatiques (serveurs, postes de travail, équipements réseaux, machines virtuels, terminaux industriels, automates programmables, SCADA, capteurs, actionneurs, etc.)
CERT	Computer Emergency Response Team. Identique CSIRT. Entité qui travaille en anticipation des menaces, investigation, et réponse aux incidents critiques d'une crise cyber
CRA	Cyber Resilience Act. Règles cyber européennes communes couvrant le matériel et le logiciel
CSIRT	Computer Security Incident Response Team. Identique CERT
DMZ	Zone Démilitarisée. Sous réseau intermédiaire, souvent utilisé pour la jonction entre IT et OT
DPI	Deep Packet Inspection. Technique d'analyse des flux encapsulés dans les trames Ethernet pour détecter des intrusions. Analyse possible des protocoles industriels
DSI	Direction (Directeur) des Systèmes d'Information
EDR	Endpoint Detection Response. Logiciel de sécurité qui surveille un terminal (pas le réseau du SI)
forensique	Investigation scientifique d'un SI après une cyberattaque. Permet de produire des preuves nécessaires à une action interne ou au lancement d'une procédure judiciaire
IT	Technologie de l'Information. Se dit généralement du SI bureautique
MCO	Maintien en conditions Opérationnelles
MCS	Maintien en condition de Sécurité
SOC	Security Operation Center. Équipe en charge d'assurer la sécurité de l'information
Mitigation	Mesure pour supprimer ou réduire l'impact de menaces cyber
NIS	Network and Information Security. Directive européenne transposée en droit français
OIV	Opérateurs d'Importance Vitale (activités indispensables pour le bon fonctionnement de la nation)
OSE	Opérateurs de Services Essentiels – EE : Entités Essentielles
OSI	Opérateurs de Services Importants – EI : Entités Importantes
OT	Technologie des Opérations. Se dit généralement ses SI utilisés pour le pilotage et la supervision d'unités de production
PASSI	Prestataire d'Audit de la Sécurité des Systèmes d'Information. Qualifié par l'ANSSI
PCA	Plan de continuité des Activités. Garantir la continuité des opérations en cas de problème
PenTest	Test de Pénétration. Simulation d'une attaque du SI
PRA	Plan de Reprise des Activités. 'BackUp' d'une infrastructure pour reconstruction post sinistre
RSSI	Responsable de la Sécurité des Systèmes d'Information
SI	Système d'Information. Inclut le réseau et les équipements clients/serveurs/automates/ES
SIEM	Security Information and Event Management Outil de management de la sécurité utilisé par le SOC, pour surveiller les infrastructures dans leur ensemble Collecte de données, agrégation et génération d'alertes de sécurité
SOC	Security Operation Center. Équipe en charge d'assurer la sécurité de l'information
XDR	Extended Threat Detection and Response Outil de surveillance endpoint, reseau, cloud
PSSI	Politique de Sécurité des Systèmes d'Information
GMAO	Gestion de maintenance assistée par ordinateur (en anglais : CMMS)

11 / RÉFÉRENCES

Références dans les notes du texte :

1- Global Threat Landscape Report 2H 2023 (fortinet.com)

2- Directive - 2016/1148 - EN - EUR-Lex (europa.eu)

3- La directive NIS 2 | ANSSI (cyber.gouv.fr)

4- Cybersecurity Workforce Study 2023 (isc2.org)

5- Dans l'affaire NotPetya, Merck gagne en appel contre son assureur (lemondeinformatique.fr)

6- Escroquerie bancaire - précisions quant aux conditions du remboursement du client par sa banque (courdecassation.fr)

7- Rapport menaces et incidents - CERT-FR (ssi.gouv.fr)

8- ENISA Threat Landscape 2024 — ENISA (europa.eu)

9- ENISA Threat Landscape 2024 — ENISA (europa.eu)

10- 2024 State of Operational Technology (fortinet.com)

11- ENISA Threat Landscape 2024 (enisa.europa.eu)

12- 2023 Global Threat Roundup Report: Trends in cyberattacks, exploits, and malware (forescout.com)

13- La cybersécurité des systèmes industriels (cyber.gouv.fr)

14- icsmodel.infracritical.com

15- The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation - Theodore J. Williams - 1992 (sciencedirect.com)

16- Doctrine de détection pour les systèmes industriels (cyber.gouv.fr)

17- LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (legifrance.gouv.fr)

18- Recommandations pour la protection des systèmes d'information essentiels | ANSSI (cyber.gouv.fr)

19- Publications Office (europa.eu), La directive NIS 2 | ANSSI (cyber.gouv.fr)

20- Texts adopted - Cyber Resilience Act - Tuesday, 12 March 2024 (europa.eu), Procedure File: 2022/0272(COD) | Legislative Observatory | European Parliament (europa.eu)

21- La cybersécurité des systèmes industriels

22- Guide d'hygiène informatique (cyber.gouv.fr)

23- 10 règles d'or pour la conception et la mise en œuvre de services numériques | ANSSI (cyber.gouv.fr)

24- PSSI — Guide d'élaboration de politiques de sécurité des systèmes d'information | ANSSI (cyber.gouv.fr)

25- La cybersécurité des systèmes industriels | ANSSI (cyber.gouv.fr)

26- Cartographie du système d'information (cyber.gouv.fr)

27- Cartographie du système d'information (cyber.gouv.fr)

28- §6.1.1 de Guide to Operational Technology (OT) Security: NIST Requests Comments (csrc.nist.gov)

29- [MaJ] Vulnérabilité dans Apache Log4j – CERT-FR (ssi.gouv.fr)

30- L'ANSSI met à jour la méthode EBIOS Risk Manager | ANSSI (cyber.gouv.fr)

31- Exploit Prediction Scoring System - EPSS (first.org)

32- Guide-to-cyber-threat-modelling.pdf (csa.gov.sg)

33- CIS Benchmarks (cisecurity.org)

34- Points de contrôle Active Directory – CERT-FR (ssi.gouv.fr)

35- SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC (nist.gov)

36- SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy | CSRC (nist.gov)

37- Recommended Practice for Patch Management of Control Systems (cisa.gov)

38- Security and Privacy Controls for Information Systems and Organizations (nist.gov)

39- Sauvegarde des systèmes d'information (cyber.gouv.fr)

40- §6 du lien : The Top 7 Operational Technology Patch Management Best Practices (isa.org)

41- Operation Black Tulip: Certificate authorities lose authority (europa.eu)

42- Meet 'Flame,' The Massive Spy Malware Infiltrating

Iranian Computers (wired.com)

43- INDUSTROYER.V2: Old Malware Learns New Tricks | Mandiant

44- Chez Saint Gobain, «il y un avant et un après la cyber-attaque» (usinenouvelle.com)

45- TRITON Malware | Attackers Deploy New ICS Attack Framework (mandiant.com)

46- Destructive ICS Malware 'Fuxnet' Used by Ukraine Against Russian Infrastructure - SecurityWeek (ampproject.org)

47- La Russie intensifie sa guerre hybride contre l'Occident (lefigaro.fr)

48- Compromission d'un système de contrôle de haut fourneau (lemagit.fr)

49- Destruction d'un équipement dans l'usine sidérurgique de Khuzestan Steel Company en Iran (scadafence.com)

50- Clusif - 44 fiches incidents cyber SI industriels (clusif.fr)

Autres références intéressantes

- The State of the Industrial Cybersecurity Market in 2023 - Industrial Cyber
- SP 800-40 Rev. 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology | CSRC (nist.gov)
- Recommandations-de-configuration-des-commutateurs-et-pare-feux-siemens-scalance
- Volet_operationnel_cyberattaques et remediation
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- Industrial Control Systems | Cybersecurity and Infrastructure Security Agency CISA
- SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security | CSRC
- Cybersecurity Advisories & Guidance
- Cybersecurity | Homeland Security

12 / ANNEXES

12.1 QUELQUES ATTAQUES EMBLÉMATIQUES SUR DES INSTALLATIONS INDUSTRIELLES

STUXNET : 2007 (ANNÉE D'INITIATION SUPPOSÉE) – 2010 (ANNÉE DE DÉCOUVERTE)

Objectif : Sabotage du programme nucléaire iranien.

Moyens techniques : Stuxnet est un malware d'une complexité sans précédent, conçu pour cibler spécifiquement les systèmes de contrôle industriels (SCADA) utilisés dans les installations nucléaires iraniennes. Il exploitait plusieurs vulnérabilités zero-day non connues à l'époque dans les systèmes Microsoft Windows, ce qui lui permettait de se propager de manière furtive via des clés USB infectées. L'une de ses caractéristiques les plus redoutables était sa capacité à rester invisible aux logiciels antivirus, à éviter la détection lors de la copie de fichiers, et à se désinstaller proprement après avoir accompli sa mission, rendant l'attaque extrêmement difficile à détecter.

Stuxnet était conçu pour prendre le contrôle des systèmes SCADA WinCC/PCS 7 de Siemens, utilisés pour gérer les centrifugeuses de l'installation nucléaire. Il modifiait subtilement les paramètres de fonctionnement des centrifugeuses, les amenant à des vitesses de rotation susceptibles de provoquer des dégâts, tout en falsifiant les données renvoyées aux opérateurs, qui ne se rendaient pas compte des anomalies jusqu'à ce que des dommages irréversibles soient causés.

DUQU[41] ET FLAME[42] : 2011-2012

Objectif : Espionnage à grande échelle et collecte d'informations.

Moyens techniques : Duqu et Flame partagent de nombreuses similitudes avec Stuxnet, en particulier l'exploitation de vulnérabilités Windows, l'utilisation de certificats volés pour éviter la détection, et des mécanismes sophistiqués de propagation autonome. Duqu, découvert en 2011, se concentrait sur la collecte d'informations sensibles, telles que des schémas industriels, afin de préparer de futures attaques potentielles. Flame, révélé en 2012, allait plus loin en intégrant des outils d'espionnage permettant de capturer des conversations audio, de prendre des captures d'écran, et d'intercepter les communications réseau. Ces deux malwares se sont propagés à l'international, touchant plusieurs pays, dont la France, et ont marqué une nouvelle étape dans l'évolution des cyberattaques à des fins d'espionnage à grande échelle.

SHAMOON : 2012 ET 2016

Objectif : Destruction de données et sabotage.

Moyens techniques : Shamoon, également surnommé "Wiper", est un malware destructeur qui a paralysé la société pétrolière Aramco en 2012 en effaçant les données de plus de 30 000 ordinateurs, interrompant ainsi les opérations pendant plusieurs semaines. En 2016, une nouvelle version de Shamoon a frappé à nouveau, ciblant cette fois des infrastructures gouvernementales saoudiennes. Le malware était conçu pour effacer définitivement les données des systèmes infectés, rendant la récupération impossible et causant des dommages opérationnels considérables.

TROJAN (RAT) HAVEX : 2013

Objectif : Espionnage et sabotage des systèmes industriels.

Moyens techniques : Havex est un cheval de Troie d'accès à distance (RAT), découvert en 2013, qui ciblait spécifiquement les systèmes de contrôle industriels, en particulier les SCADA. Il se propageait par des mises à jour logicielles compromises, téléchargées par des victimes à partir de sites légitimes mais infectés. Une fois installé, Havex permettait aux attaquants d'espionner les communications entre les systèmes de contrôle et les équipements industriels. Le malware utilisait des protocoles industriels spécifiques pour intercepter les données et compromettre les opérations, permettant ainsi aux attaquants de surveiller et manipuler les infrastructures ciblées à distance.

BLACKENERGY : 2007 (BE1) - 2015 (BE2, BE3)

Objectif : Sabotage et déni de service des infrastructures critiques.

Moyens techniques : BlackEnergy est un malware dont l'évolution s'est étalée sur plusieurs années, avec trois versions successives : BE1, BE2, et BE3. La première version, BE1, apparue en 2007, était utilisée principalement pour mener des attaques par déni de service distribué (DDoS) en créant un réseau de bots. Ces attaques ciblaient des systèmes en masse pour provoquer des interruptions de service.

[41] Operation Black Tulip: Certificate authorities lose authority (europa.eu)
[42] Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers (wired.com)

Avec l'arrivée de BE2 et BE3, BlackEnergy a gagné en sophistication et a évolué pour cibler directement des systèmes industriels, notamment des infrastructures critiques. En décembre 2015, BlackEnergy a été utilisé lors d'une attaque contre le réseau électrique ukrainien. Les attaquants, après avoir compromis les systèmes SCADA via des emails de phishing, ont utilisé BlackEnergy pour désactiver plusieurs sous-stations électriques, entraînant une coupure d'électricité qui a affecté plus de 225 000 foyers pendant plusieurs heures. Ce malware combinait des techniques de sabotage direct et d'espionnage, permettant de prendre le contrôle des infrastructures tout en restant caché dans les systèmes infectés.

INDUSTROYER : 2016-2017 (INDUSTROYER 2[43])

Objectif : Perturbation des réseaux électriques.

Moyens techniques : Industroyer est un malware découvert en décembre 2016 en Ukraine, où il a provoqué une coupure de 20 % de l'approvisionnement électrique de la capitale, Kiev. Ce malware a été conçu spécifiquement pour attaquer les réseaux électriques en envoyant des commandes malveillantes à travers des protocoles de contrôle industriel utilisés pour la gestion des infrastructures critiques, tels que IEC 60870-5-101, IEC 60870-5-104, IEC 61850 et OPC. En s'attaquant aux SCADA et aux systèmes de contrôle des sous-stations électriques, Industroyer a démontré la capacité des cyberattaques à perturber directement des services publics essentiels.

En 2017, une deuxième version du malware, connue sous le nom d'Industroyer2, a frappé à nouveau le réseau électrique ukrainien. Cette version était plus ciblée et efficace, simplifiant l'adaptation de l'outil à différents environnements industriels. Industroyer2 utilisait un seul protocole de communication – IEC 60870-5-104 – qui permet le contrôle et le monitoring des systèmes de puissance via TCP, ce protocole étant largement déployé en Europe et au Moyen-Orient. Cette version a ainsi optimisé l'efficacité des attaques sur des réseaux spécifiques, réduisant le temps nécessaire pour compromettre les infrastructures ciblées.

2017 : WANNACRY ET NOTPETYA

Objectif : Extorsion financière et sabotage des infrastructures.

Moyens techniques : En 2017, les rançongiciels WannaCry (mai) et NotPetya (juin) ont marqué l'histoire des cyberattaques en mettant en lumière l'importance d'un suivi rigoureux des vulnérabilités connues et de l'application rapide des correctifs. Ces deux malwares ont exploité la vulnérabilité EternalBlue (CVE-2017-0144), une faille d'exécution à distance dans le protocole SMBv1, corrigée par Microsoft en mars 2017 (correctif MS17-010). Malgré la disponibilité de ce correctif, de nombreuses entreprises n'avaient pas encore mis à jour leurs systèmes lorsque les attaques ont eu lieu, permettant à ces malwares de se propager rapidement à travers le monde.

- **WannaCry :** Lancé en mai 2017, WannaCry se propageait à grande échelle en cryptant les fichiers des machines infectées et exigeant une rançon en bitcoins pour les décrypter. Cette attaque a perturbé des grandes entreprises à travers le monde, notamment en France, où Renault a été l'une des entreprises les plus touchées, entraînant la fermeture temporaire de certaines de ses usines.
- **NotPetya :** Un mois plus tard, NotPetya a frappé principalement des entreprises et des organisations en Ukraine, avant de se propager dans le monde entier. Bien que présenté comme un rançongiciel, NotPetya agissait principalement comme un malware destructeur, rendant les machines infectées inopérables même après le paiement de la rançon. En France, des entreprises comme Saint-Gobain, Auchan, et la SNCF ont été sévèrement affectées. Saint-Gobain a estimé ses pertes à 220 millions d'euros à la suite de l'attaque[44].

TRITON[45] (TRISIS) : FIN 2017 - 2019

Objectif : Sabotage des systèmes de sécurité industriels.

Moyens techniques : Le malware Triton (aussi appelé Trisis) a été découvert fin 2017 dans une usine pétrochimique en Arabie Saoudite, où il visait spécifiquement les Systèmes Instrumentés de Sécurité (SIS), utilisés pour protéger les installations industrielles en cas de défaillance. Triton ciblait les automates Triconex SIS de Schneider Electric via le protocole propriétaire TriStation. Le malware manipulait la mémoire des automates de sécurité, provoquant des erreurs de validation et d'intégrité des données, entraînant des arrêts intempestifs des automates de sécurité et perturbant le processus industriel.

[43] INDUSTROYER.V2: Old Malware Learns New Tricks | Mandiant
[44] Chez Saint Gobain, «il y un avant et un après la cyber-attaque» (usinenouvelle.com)
[45] TRITON Malware | Attackers Deploy New ICS Attack Framework (mandiant.com)

Ce qui rend Triton particulièrement dangereux est qu'il s'attaque directement aux systèmes de sécurité, conçus pour prévenir les catastrophes industrielles. En modifiant ces systèmes, Triton aurait pu provoquer des incidents aux conséquences potentiellement catastrophiques pour l'installation elle-même et ses opérateurs.

Bien que le malware ait été découvert en 2017, l'analyse des événements a révélé que les attaques de Triton se sont poursuivies jusqu'en 2019, ciblant à nouveau des infrastructures critiques avec des améliorations du code et des méthodes d'attaque plus sophistiquées. Cette temporalité montre la persistance de la menace et la capacité des attaquants à revenir avec des versions modifiées du malware.

Triton a été attribué au groupe d'attaquants Sandworm, un groupe lié à des acteurs étatiques, probablement russes. Ce groupe est également connu pour avoir orchestré d'autres attaques notoires, comme celles utilisant Stuxnet et Industroyer, démontrant une spécialisation dans les cyberattaques contre les infrastructures critiques.

COLONIAL PIPELINE : 2021

Objectif : Extorsion financière et perturbation des infrastructures critiques.

Moyens techniques : En mai 2021, une attaque par rançongiciel a ciblé Colonial Pipeline, un opérateur majeur qui approvisionne en combustible dérivé du pétrole (essence, gasoil, kérosène) les États de la côte Est des États-Unis. L'attaque a débuté par l'exploitation d'un mot de passe volé permettant d'accéder au réseau interne via un VPN. Une fois l'accès établi, les attaquants ont compromis le système de paiement de l'entreprise, ce qui a incité Colonial Pipeline à arrêter toutes ses opérations pendant 5 jours par mesure de précaution.

L'attaque a provoqué une pénurie d'approvisionnement dans une dizaine d'États américains, entraînant une hausse des prix et des perturbations dans la chaîne d'approvisionnement des carburants. Colonial Pipeline a finalement décidé de payer la rançon d'un montant équivalent à 4,4 millions de dollars en bitcoin pour regagner l'accès à ses systèmes et rétablir les opérations. Malgré la restauration rapide des services après le paiement, l'attaque a démontré la vulnérabilité des infrastructures critiques face aux rançongiciels.

Cette attaque, largement médiatisée, s'inscrit dans une tendance croissante des cyberattaques par rançongiciel, dont le nombre a augmenté de 87 % en 2023 par rapport à 2022. L'impact majeur sur l'approvisionnement énergétique montre à quel point les systèmes industriels, même indirectement touchés, sont sensibles aux cyberattaques, et souligne la nécessité d'une meilleure protection des infrastructures critiques contre ces menaces.

ACIDRAIN (VIASAT) : 2022

Objectif : Perturbation des infrastructures de télécommunication.

Moyens techniques : L'attaque AcidRain visait à perturber les communications par satellite en effaçant les modems utilisés par Viasat, un fournisseur d'infrastructures de communication par satellite. Bien que l'attaque n'ait pas touché directement des systèmes OT, elle a affecté plusieurs infrastructures critiques dépendant des communications satellites. AcidRain a utilisé un malware de type wiper pour effacer les données des modems, rendant les communications inopérantes sur une vaste zone géographique.

CAS PLUS RÉCENTS

Au moment de l'élaboration de ce livre blanc, le conflit entre la Russie et l'Ukraine, génère un grand nombre d'attaques sur des infrastructures critiques et des systèmes industriels : le malware Fuxnet[46] utilisé par le groupe d'origine ukrainienne nommé "blackjack" (origine ukrainien) a récemment provoqué des disfonctionnements dans les systèmes de gestion d'infrastructures russes et notamment dans les passerelles de capteurs industriels. Du côté russe, le groupe "Sandworm" (APT44), est activement engagé dans toute la gamme des opérations d'espionnage, d'attaque et d'influence de l'armée russe visant des infrastructures critiques ukrainiennes. Ce même groupe est également en train de cibler des pays de l'OTAN[47].

Cet historique reprend les attaques les plus célèbres et n'est pas exhaustif : d'autres cas sont intéressants comme la destruction d'un four industriel[48] ou encore la destruction d'un équipement sidérurgique[49] par exemple. Le Clusif propose également une analyse de 44 incidents cyber SI industriels[50].

[46] Destructive ICS Malware 'Fuxnet' Used by Ukraine Against Russian Infrastructure - SecurityWeek (ampproject.org)
[47] La Russie intensifie sa guerre hybride contre l'Occident (lefigaro.fr)
[48] Compromission d'un système de contrôle de haut fourneau (lemagit.fr)
[49] Destruction d'un équipement dans l'usine sidérurgique de Khuzestan Steel Company en Iran (scadafence.com)
[50] Clusif - 44 fiches incidents cyber SI industriels (clusif.fr)

Les systèmes d'informatique industrielle, ou systèmes OT (pour Operational Technology, en anglais) sont à la fois spécifiques, très divers, et souvent méconnus. Dans l'industrie, c'est généralement l'outil de production qui capte l'attention des décideurs, et les principaux financements. Les systèmes OT, périphériques à la production, permettent de l'encadrer, la rendre plus efficiente, et aussi la protéger. Mais lorsque ces systèmes ne sont pas suffisamment considérés, ils peuvent devenir une faille et compromettre l'entreprise, ses produits, et même mettre en danger ses salariés.

Ce livre blanc vise à expliquer la spécificité des systèmes OT, l'intérêt d'en assurer la performance, l'intégrité, la robustesse et la résilience, et les bonnes pratiques pour y parvenir.

S'appuyant sur un corpus normatif et réglementaire de référence, les experts du secteur de la cybersécurité OT proposent ici une approche structurée et pédagogique pour réussir le Maintien en Condition de Sécurité (MCS) de ces systèmes.

GIMELEC

Nous décuplons les énergies

Conception graphique : purplepop