LES INDICATEURS CYBER-SÉCURITÉ DANS LE MILIEU INDUSTRIEL

CESIN

Les Indicateurs cybersécurité dans le milieu industriel

INTRODUCTION

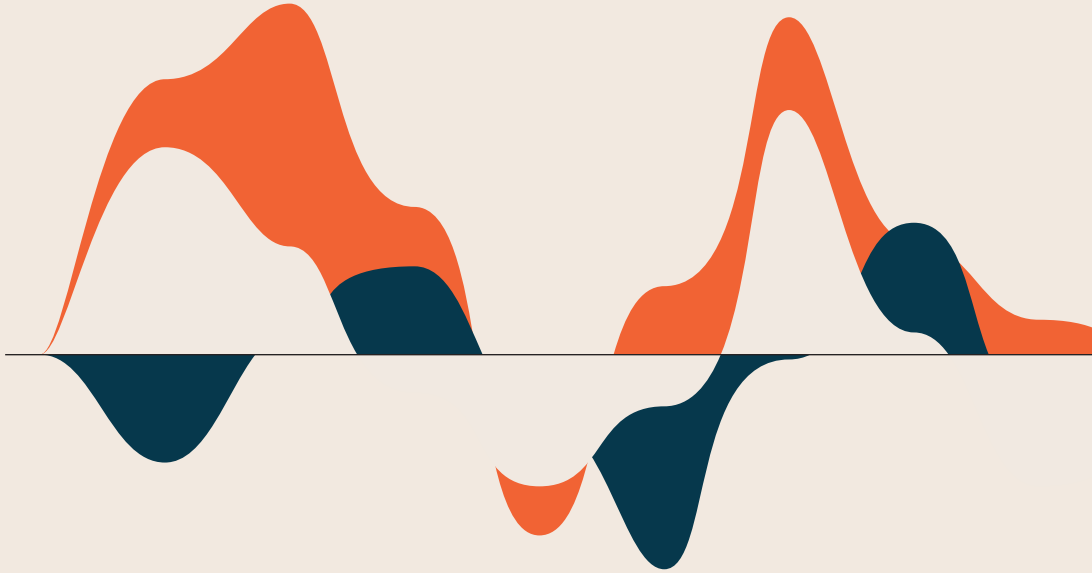
Dans le secteur industriel, une approche pragmatique est cruciale. Les indicateurs évoluent avec la maturité de l'entité : au début, ils se concentrent sur les premières actions de sécurisation, puis s'adaptent pour suivre la conformité aux politiques de sécurité.

Les indicateurs du périmètre industriel contribuent aux indicateurs globaux de cybersécurité de l'entreprise (cf. livrable CESIN du LAB Tableaux de bord intitulé « Tableaux de bord de cybersécurité »).

Les tableaux de bord de cybersécurité sont essentiels pour les RSSI, permettant de suivre et de piloter la sécurité des entreprises. Leur contenu doit être adapté selon les destinataires et les objectifs.

Ce livrable s'adresse aux RSSI du secteur industriel, fournissant des réponses basées sur les expériences du LAB OT du CESIN. Il s'insère dans une série de publications sur les KPIs de cybersécurité, visant à offrir une démarche concrète de mise en place.

POURQUOI METTRE EN PLACE DES INDICATEURS CYBER DANS LE MONDE INDUSTRIEL ?



- Chercher du sponsorship
- Mesurer le risque (ex. taux de click aux tests de phishing)
- Evaluer le niveau de sécurité (ex. niveau de durcissement des serveurs)
- Démontrer une certaine maitrise de la sécurité (ex. vis à vis des assurances pour le calcul de la prime)
- Se positionner et se comparer par rapport à l'état de l'art, au marché ou aux autres sites et entités (ex. score de maturité)
- Piloter des déploiements (ex. déploiement des solutions de sécurité)
- Amener des échanges sur le niveau de cybersécurité
- Chercher du budget
- Embarquer l'ensemble des unités organisationnelles et leurs référents cyber dans un objectif commun
- ...

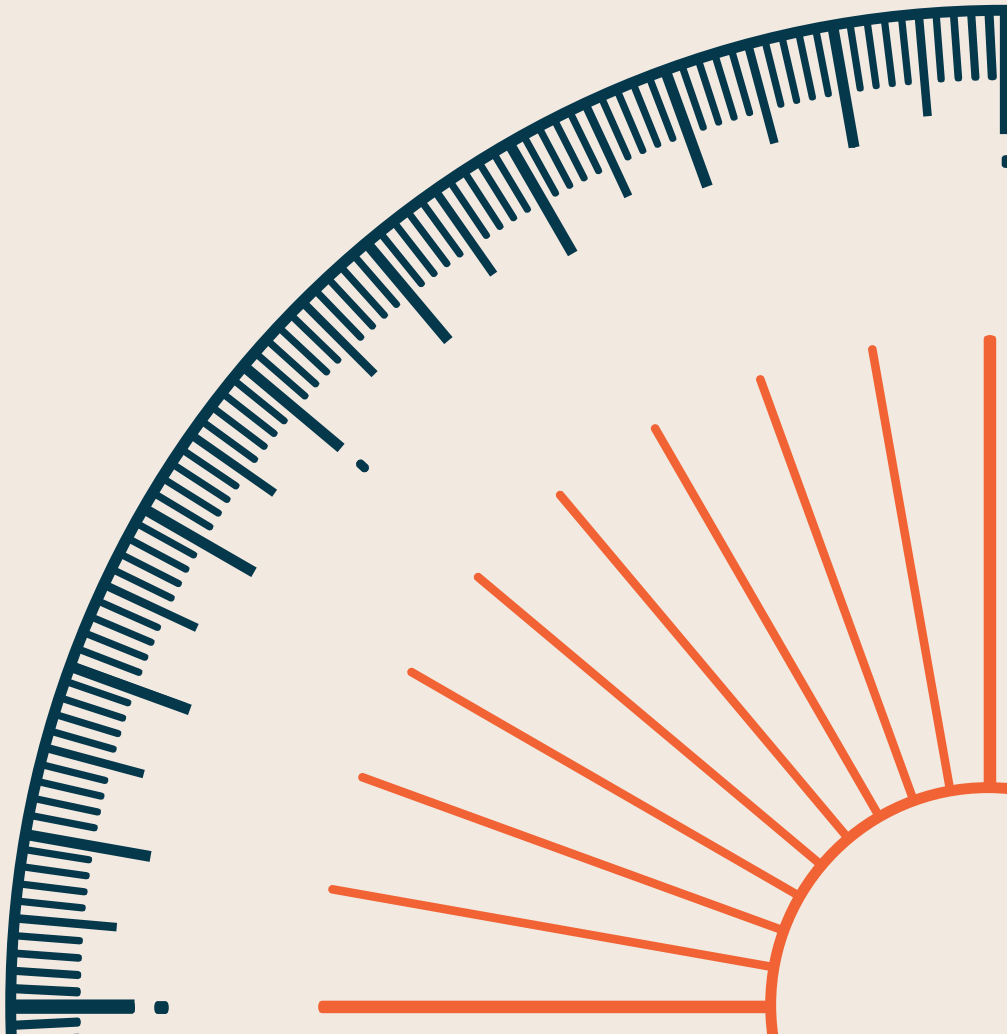
Quel que soit l'objectif recherché, tout indicateur doit permettre d'amener une action qui fera progresser le niveau de protection des sites industriels contre la menace cyber.

POUR QUI ?

Pour embarquer les équipes vers plus de sécurité, l'objectif sera de cibler, via les indicateurs, les équipes opérationnelles et pas uniquement le top management.
Selon les organisations, les interlocuteurs cibles sont : les référents cybersécurité des unités organisationnelles, les responsables des sites, les responsables de maintenance, les responsables des pays, le responsable IT local, les responsables des opérations industrielles, le RSSI en charge du périmètre industriel, le top management, etc.
Pour couvrir cette multitude d'interlocuteurs, privilégier la construction d'un ensemble d'indicateurs qu'il sera possible de regrouper ou de dissocier selon l'interlocuteur et le niveau de détail souhaité.

· **Ainsi, pour le Comex, les indicateurs seront limités en nombre, simples et synthétiques.** L'objectif est d'afficher en un temps réduit une météo représentant l'état du risque (vert, orange, rouge) et une tendance dans son traitement (progression ou régression). Se référer au livrable CESIN « Tableaux de bord cybersécurité ».

· **Pour les équipes opérationnelles, les indicateurs pourront être plus précis et plus détaillés** selon le périmètre à couvrir et selon le niveau de maturité souhaité sur le périmètre.



PAR OÙ COMMENCER ?

Pour mener à bien le chantier d'identification des indicateurs, des prérequis doivent être remplis :

· Disposer d'une évaluation des risques métier ayant pour origine la cybersécurité (cf. livrable CESIN « L'analyse de risque d'un système industriel… en 2h chrono»).

· Formaliser des objectifs de sécurité clairs (par exemple à travers une politique) et partager ces objectifs (ex. les périmètres prioritaires, les cibles…).

Obtenir le sponsorship adéquat de la part du management sur l'atteinte de ces objectifs et le traitement des risques.

· Clarifier la gouvernance sécurité sur les sites industriels.

Le choix des indicateurs se fait en fonction :

• **Des risques cybersécurité identifiés** (exemple : arrêt de production à la suite d'une cyberattaque due à un manque d'hygiène de sécurité)

• **Des objectifs prioritaires de sécurité fixés** pour le traitement de ces risques (exemple : installation de sonde de sécurité, segmentation du réseau, recertification des comptes externes, mise en place de sauvegardes…)

• **Des contrôles de sécurité récurrents à maintenir.** En effet, une fois un objectif de sécurité atteint, il convient aussi de le maintenir et d'en vérifier l'efficacité (exemple : les postes utilisés ont-ils toujours un bon niveau de durcissement ; quel est le volume et le type d'incidents rencontrés…).

• **Du niveau de maturité de l'entité** en se basant sur un référentiel de l'entreprise ou du secteur.

Les indicateurs peuvent être de deux types :

• **Indicateurs de type « Build »** : Ils mesurent la mise en place de processus, politiques ou solutions de sécurité via un taux d'avancement (0 à 100%). Une fois l'objectif atteint, ils peuvent être intégrés aux indicateurs de « Run » pour vérifier le maintien du niveau de sécurité.

Indicateurs de type « Run » : Ils évaluent l'état opérationnel, l'efficacité ou les risques, souvent mesurés comme des indicateurs type météo.

Il est crucial de choisir des indicateurs réalistes pour les sites industriels, en commençant par des indicateurs simples et atteignables. Ces indicateurs devraient être progressivement complétés pour couvrir des objectifs plus complexes. Cela maintiendra une dynamique positive, en équilibrant les indicateurs faciles à réaliser et ceux plus avancés.

COMMENT FAIRE ADHÉRER LES PARTIES PRENANTES ?

Le sponsorship est un point de départ essentiel. Le top management, et en particulier les responsables industriels, doivent avoir conscience des risques de cybersécurité qui pèsent sur leur périmètre. Une fois cette conscience en place, le déploiement des outils et processus de sécurité sur les sites sera vu comme une nécessité.

Il faudra également **une organisation et une gouvernance claire.** Cela passe par la définition des responsabilités sécurité sur le périmètre industriel et par l'identification des interlocuteurs clés et porteurs avec lesquels interagir.

Lors de la construction des indicateurs, le RSSI doit rester dans un rôle d'accompagnant et être force de proposition. Il doit **coconstruire avec le métier les indicateurs pour permettre une meilleure appropriation et un engagement. L'indicateur devra être parlant pour les équipes opérationnelles** en charge de l'implémentation des objectifs. En d'autres termes, l'indicateur doit être lié à leurs activités et aux outils manipulés (ex. gestion de l'obsolescence, installation d'outils de sécurité sur les postes de contrôles...).

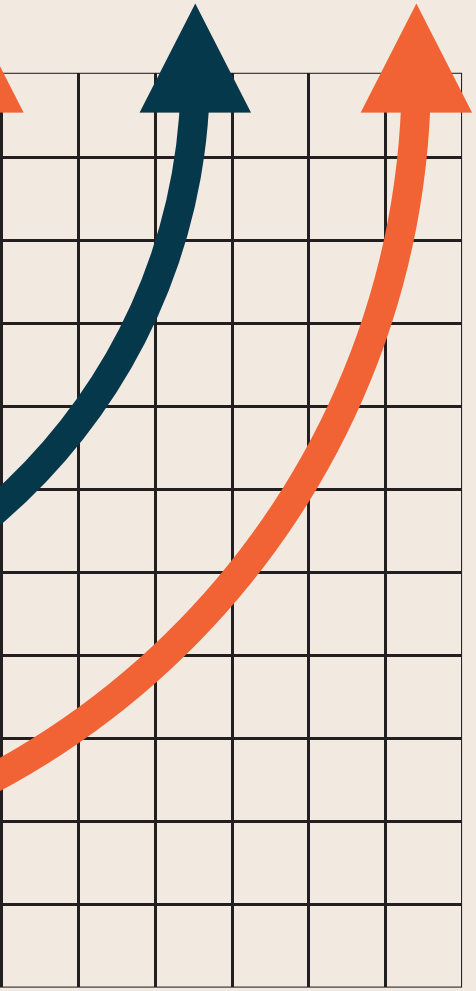
Rester pragmatique sur l'objectif, car certains indicateurs n'atteindront probablement jamais 100%. Par exemple, la gestion de l'obsolescence des machines industrielles peut prendre plusieurs années. L'indicateur reste intéressant mais il doit rester réaliste. **Penser indicateurs SMART** (Spécifique, Mesurable, Atteignable, Réaliste, Temporel).

Un autre moyen de faire adhérer les différentes parties prenantes est de **créer une communauté des référents sécurité industrielle** et de partager avec eux de façon régulière les résultats des indicateurs. Cela permet le partage d'expérience, de solutions et la mise en place d'une cohésion de groupe.

Veillez également à ce que pour chaque indicateur, **des recommandations** soient fournies sur comment atteindre l'objectif. Cela donnera ainsi un cadre clair aux interlocuteurs en charge de leur implémentation leur permettant de **construire un plan d'actions.**
En effet, le rôle du RSSI n'est pas seulement de définir et relever les compteurs, il doit aussi appuyer les équipes afin de les aider à atteindre les objectifs de sécurité.

Idéalement, pour plus d'impact, les objectifs de sécurité et les indicateurs clés associés doivent être **intégrés aux entretiens annuels des équipes** et des responsables et être objectivés par le management de ces équipes.

Point d'attention, lorsque le secteur d'activité de l'entreprise est encadré par une réglementation cybersécurité (ex. NIS 2, LPM...) ou sectorielle, l'étendue des indicateurs à mettre en place est imposée et l'adhésion est généralement déjà en place. Cependant, il est important de ne pas se laisser submerger par les indicateurs de conformité et s'assurer que les indicateurs gardent pour objectif la réduction du risque métier.



LES LIMITES DES INDICATEURS ET QUELQUES POINTS D'ATTENTION

Ajuster le fond / la forme (choix pourcentage ou valeur, durée d'observation, progression...) **en fonction du message souhaité.** En effet, parfois les objectifs fixés ne sont pas atteints mais la progression et la tendance par rapport à la situation initiale peut être positive.

Attention à ne pas s'arrêter au résultat mais de s'assurer de sa pertinence. Analyser l'indicateur pour comprendre le contenu, la valeur, la tendance pour montrer la progression. Par exemple : l'indicateur de taux de sensibilisation des collaborateurs ne progresse pas ? Cela pourrait être dû à la fiabilité de la donnée source (départs des collaborateurs, accès aux outils de sensibilisation, le périmètre est-il stable...).

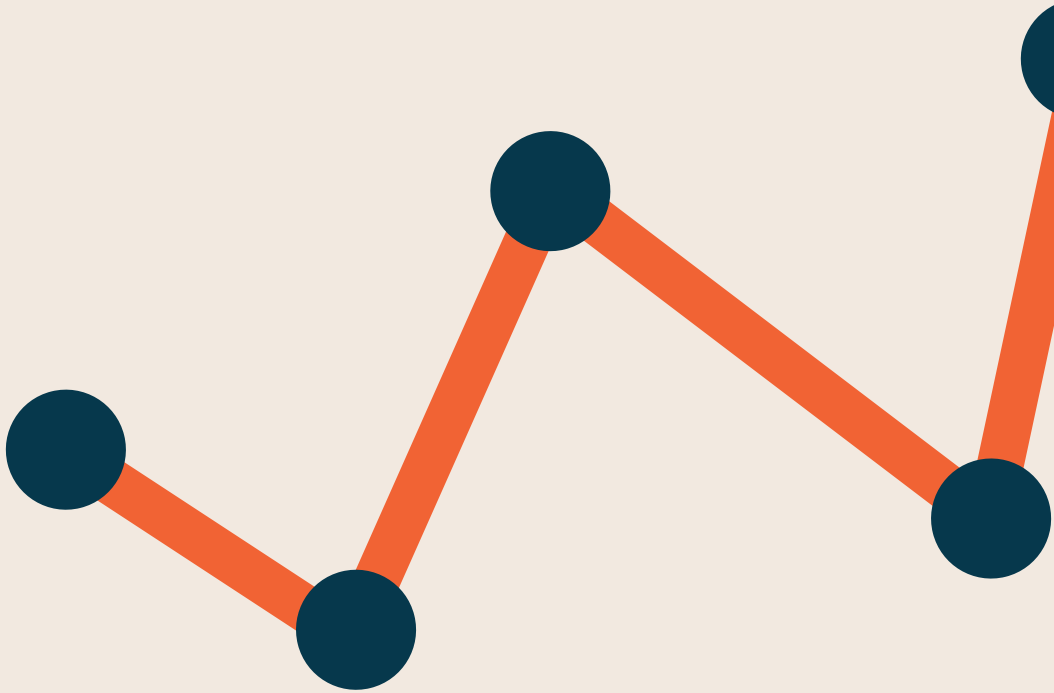
Essayer de ne pas décourager les équipes qui essayent de faire remonter les indicateurs : mettre des indicateurs irréalistes ou qui n'évoluent plus depuis plusieurs mois peut décourager les équipes.

La gestion des indicateurs via Excel peut vite atteindre ses limites. Il faut avoir la capacité de mesurer et de produire les indicateurs de façon régulière et automatisée. Mettre en place des outils de collecte et de traitement de données peut apporter une meilleure précision et une meilleure efficacité. Cela sera possible progressivement avec la mise en place des outils de sécurité (sondes, EDR, AD, outils de scan...).
De plus, des outils comme PowerBI ou Tableau permettent d'apporter une meilleure visibilité et une lisibilité plus claire ; il peut donc être intéressant de progressivement migrer vers ce type de solutions, sans être une priorité : le fond avant la forme !

COMMUNICATION DES INDICATEURS

La communication des indicateurs au sein de l'entreprise a plusieurs bénéfices. Cela permettra aux différentes entités d'avoir la visibilité sur l'avancement et de bénéficier des retours d'expérience des entités les plus avancées. Aussi, cela permettra de **créer une certaine émulation pour l'atteinte de l'objectif** et valoriser les intervenants.

Il peut être intéressant de créer un classement des entités via un score de sécurité. Cet indicateur sera dans ce cas plutôt à destination du top management. Il permettra de poser les questions sur les moyens et les priorités. De plus, laisser chaque entité voir le résultat de ses pairs peut aussi motiver les responsables d'entités qui n'aiment pas avoir de moins bons résultats que ses pairs.



LA MISE EN PLACE D'INDICATEURS DANS LES GRANDS GROUPES (MULTI-SITES, MULTI-ENTITÉS...)

Dans un grand groupe, les risques et objectifs de sécurité peuvent être différents selon les entités, les sites, les pays.... Pour un pilotage efficace des objectifs de sécurité, la construction des indicateurs se fait généralement à deux niveaux :

• **Au niveau central :** la définition des objectifs globaux et communs à atteindre.

• **Au niveau périmètre spécifique :** la prise en compte de l'objectif commun, sa déclinaison sur le contexte local et l'ajout des indicateurs spécifiques couvrant les risques locaux.
Une possibilité est de **grouper les entités en sous-groupes homogènes** (exemple de groupements : taille, chiffre d'affaires, activité, criticité, équipes ou directions fonctionnelles...) en lien avec l'organisation. Ainsi, des objectifs plus ou moins ambitieux sont fixés pour chaque sous-groupe en fonction de la criticité du périmètre, des risques à couvrir et de la maturité cible à atteindre.

Cela permettra de disposer d'un socle commun permettant de piloter l'atteinte des objectifs de sécurité au niveau global.

EXEMPLES DE KPIS

Chaque contexte étant différent (réglementations, risques et vitesse de maturité...), nous avons pris le parti de construire une liste d'indicateurs possibles sur le périmètre industriel en y intégrant des critères de sélection basés sur les expériences des membres du LAB OT.
Ces indicateurs sont classés par domaine du NIST CSF et les critères de sélection sont :

- **Maturité :** le niveau de maturité de l'entité avec 3 niveaux identifiés
  - **Initial :** indicateur à mettre en place en priorité quand on démarre un chantier sécurité sur les sites industriels.
  - **Intermédiaire :** indicateur nécessitant une certaine maturité et peut avoir une complexité de mise en œuvre. A mettre en place si le niveau initial est suffisamment solide.
  - **Avancé :** indicateur permettant d'aller plus loin dans la maitrise des risques et nécessitant souvent des investissements plus poussés.
- **Collecte :** La difficulté de collecte de l'indicateur.
- **Automatisation :** La difficulté d'automatisation de la collecte.
- **Public :** Le public visé (CODIR, Opérations, DSI...).
- **Remédiation :** La difficulté de remédiation pour faire progresser l'indicateur

Ces indicateurs sont à compléter pour chaque périmètre à couvrir, exemple par site. Et peuvent ensuite être consolidés au niveau global. Point d'attention : penser à récupérer les volumes lors de la consolidation pour éviter que des petits périmètres non conformes impactent les chiffres globaux.

En parallèle à leur mise en place et suivi, il est important de fournir une bonne visibilité sur le périmètre couvert : les utilisateurs (internes, externes...), les assets, les prestataires, les profils et les comptes informatiques, les accès prestataires...

Exemple d'indicateurs pour le niveau initial

Domaine NIST	Thème	KPI	Valeur cible	Collecte	Auto-matisation	Public	Remédiation	Commentaires ou points d'attention
Identify	Gouvernance	Pourcentage des unités organisationnelles ayant identifié au moins un référent cybersécurité	100%	Facile	Difficile	CODIR Opérations	Moyen	L'identification d'un référent est le point de départ de la gouvernance et de la mise en œuvre des mesures de cybersécurité sur le périmètre. Le référent devra être formés régulièrement, et devra avoir une certaine capacité à assigner aux sujets Cybersécurité.
	Gouvernance	Une instance de pilotage opérationnelle est en place permettant de suivre l'avancement des actions de cybersécurité	En place	Facile	N/A	CODIR	Moyen	
	Gouvernance	Les évènements métier redoutés sont identifiés	Oui	Facile	N/A	CODIR Opérations	Facile	
	Inventaires	Niveau de maturité de l'inventaire - 0: pas d'inventaire - 1: inventaire partiel réalisé de façon manuelle - 2: inventaire est vérifié par un référent site couvrant l'ensemble du parc - 3: inventaire automatisé	2	Facile	N/A	CODIR	Difficile	
	Inventaires	Pourcentage des unités organisationnelles disposant d'un inventaire des assets industriels, mis à jour dans les 12 derniers mois	> 80%	Difficile	Moyen	Opérations	Difficile	Il est difficile d'assurer la complétude de l'inventaire sans une action de découverte automatique, l'alternative au niveau initial est que le référent site certifie le contenu de son inventaire. La profondeur de l'inventaire dépend de la maturité et peut évoluer en terme de contenu au fil du temps. Cependant un minimum d'informations est requis (identifiant, localisation, type d'asset, owner, criticité...). La criticité nécessite la mise à disposition d'un guide pour les référents site.
	Inventaires	Pourcentage des unités organisationnelles disposant d'une documentation (cartographie physique et logique avec matrice des flux)	2	Facile	N/A	CODIR	Difficile	Cette action nécessite la connaissance des réseaux et des interfaces. Les cartographies peuvent contenir des données sensibles. Elles doivent être conservées dans un environnement sécurisé et dont les accès sont fournis uniquement sur la base du besoin d'en connaitre.

Domaine NIST	Thème	KPI	Valeur cible	Collecte	Auto-matisation	Public	Remédiation	Commentaires ou points d'attention
Protect	Accès	Part des comptes-génériques-à-privilège(s) justifiés.	100%	Facile	N/A	Opérations	Difficile	La cible est à déterminer en fonction du contexte et l'usage de ces comptes. En effet, certains usages nécessiteront des comptes génériques, tant que l'usage de ces comptes est encadré et tracé, cela permet de les maitriser. Changer les usages pour sortir des comptes génériques est complexe et nécessite une conduite du changement adaptée.
	Fournisseurs	Part des fournisseurs ayant, dans leur(s) contrat(s), les clauses de cybersécurité adaptées à la nature du produit ou service objet du contrat.	100%	Moyen	N/A	CODIR, Opérations	Moyen	Clauses de sécurité minimales : Confidentialité, audit, reporting des incidents, responsabilités et indemnités. Clauses selon le service fourni : Standards techniques à appliquer, processus sécurité attendus (gestion des vulnérabilités / patch, maintenance sécurisée...). La stratégie d'intégration de sécurité dans la relation avec les fournisseurs est à définir au préalable dans une politique. Cette politique définira : les clauses par type de prestation, le RACI, les évaluations nécessaires des fournisseurs...
	Réseau	Toute nouvelle interconnexion du système industriel avec l'extérieur fait l'objet d'une prise en compte des exigences de cybersécurité.	Oui (annuel)	Facile	N/A	CODIR Opérations	Facile	Les interconnexions extérieures peuvent intégrer les interconnexions avec des SI externes ou avec des SI non industriels, selon les définitions de chaque entité dans sa PSSI. La maîtrise des interconnexions est un élément critique pour assurer la sécurité des sites. Les fournisseurs de systèmes industriels sont encore peu matures en cybersécurité, et il n'est pas rare de rencontrer des fournisseurs utilisant des listes excels partagées avec tous les mots de passe de leurs clients. La maitrise de l'inventaire des accès peut être réalisée via la revue des contrats fournisseurs, la mise en place d'un outil de découverte, etc.
	Réseau	La segmentation entre réseau IT et OT est en place	Oui	Difficile	Difficile	CODIR, Opérations	Difficile	Cet indicateur doit être justifié avec la documentation de la segmentation et l'audit de la configuration (ex. une segmentation avec un firewall ayant une configuration autorisant tous les flux sans filtrage ne pourra pas être considéré comme de la segmentation). La vérification de la configuration des firewall peut être automatisable mais ce n'est pas simple car nécessite une bonne connaissance des flux nécessaires.
	Sensibilisation	Pourcentage des collaborateurs sensibilisés à la cybersécurité	> 80%	Moyen	Moyen	CODIR Opérations	Difficile	Un premier niveau de sensibilisation peut être réalisé via des affiches ou via les réunions d'équipes. Il faut veiller à rendre les messages pertinents et applicables aux usages sur le site (ex. la sensibilisation sur le phishing via mail sera moins pertinente sur un site industriel que la sensibilisation sur l'usage de clés USB ou sur la protection des identifiants).
	Vulnérabilités	Part des assets intégrés au processus de remédiation des vulnérabilités (via campagne de patching régulière, via virtual patching, via isolation, acceptation du risque...)	100%	Difficile	Difficile	Opérations	Difficile	Cet indicateur va dépendre de la stratégie de gestion de vulnérabilités et patching en place. En effet, dans le monde OT parfois il n'est pas possible de patcher à un rythme similaire à celui de l'IT. Cet indicateur se base sur une bonne connaissance du parc. L'acceptation du risque doit être formelle et justifiée et associée à un asset spécifique.

Exemple d'indicateurs pour le niveau initial

Domaine NIST	Thème	KPI	Valeur cible	Collecte	Auto-matisation	Public	Remédiation	Commentaires ou points d'attention
Protect / Detect	Supervision sécurité	Pourcentage des assets critiques couverts par le moyen de protection le plus adéquat (ex: AV, EDR, Activation des logs, Scan de vulnérabilités, Scellement...)	> 80%	Moyen	Moyen	Opérations	Difficile	L'évaluation de la criticité dépend : de la classification de l'asset sur la base de l'échelle de classification interne, ou vis-à-vis d'une réglementation. L'objectif est de se concentrer sur un périmètre prioritaire. La criticité des systèmes doit être déterminée par une analyse de risques. L'implémentation des outils de sécurité est pertinente sur les couches hautes du modèle Purdue. En dessous du niveau 3.5 (DMZ) l'installation des outils est à réaliser avec précaution. La fonctionnalité de sécurité va dépendre de l'actif industriel. Les fonctionnalités requises doivent être définies au préalable du calcul de cet indicateur. La valeur cible de cet indicateur pourra évoluer en fonction de la maturité pour une couverture plus complète. Ce type d'objectif est plus simple à mettre en place quand il s'intègre à un projet métier (ex. renouvellement d'architecture, déploiement de nouveaux systèmes...)
Respond	Gestion des incidents	Un plan de continuité par processus métier (PCA) essentiel existe permettant de définir des palliatifs SI et métier afin de fonctionner sans système d'information ou de manière dégradée	Oui	Facile	N/A	CODIR, Opérations	Moyen	Cet objectif est à travailler en collaboration entre le métier et les équipes IT pour couvrir le SI industriel et les interfaces avec le SI de gestion. Il s'agit de la première brique à mettre en place pour se préparer à la défaillance du SI. Lorsque le processus métier dépend d'un fournisseur, il est nécessaire de s'assurer également que le fournisseur dispose d'un plan adéquat et/ou d'une assurance. Le prérequis pour l'atteinte de cet objectif est d'identifier la liste des processus métier essentiels.
	Gestion des incidents	Processus de gestion des incidents et crises cyber formalisé et partagé avec les parties prenantes (ex. fournisseurs, CODIR, opérations, DSI...)	Oui	Facile	N/A	CODIR, Opérations, DSI	Facile	
Recover	Continuité	Pourcentage des assets industriels critiques avec sauvegarde hors ligne en place	> 80%	Moyen	Moyen	CODIR, Opérations	Moyen	La collecte de l'indicateur va dépendre de la qualité de l'inventaire et du niveau de centralisation du système de backup. La collecte automatique ne pourra pas toujours couvrir l'ensemble du périmètre. Lorsque le backup doit couvrir un asset industriel obsolète, la mise en place d'un backup peut s'évérer difficile.
	Continuité	Un processus de reprise (PRA) des processus métier est défini	Oui	Facile	N/A	CODIR, Opérations	Moyen	

Exemple d'indicateurs pour le niveau intermédiaire

Domaine NIST	Thème	KPI	Valeur cible	Collecte	Auto-matisation	Public	Remédiation	Commentaires ou points d'attention
Identify	Gouvernance	Les fiches de mission cybersécurité sont définies et partagées (référent cybersécurité, responsable d'asset...)	oui	Facile	N/A	CODIR	Moyen	Dans l'avenir, grâce au SIRH, il pourrait être possible d'identifier les postes en place dans les différents périmètres et ainsi automatiser l'indicateur, cela à condition qu'ils soient affectés à 100%.
	Gouvernance	Une instance de pilotage décisionnelle (en lien avec la direction) est en place et permet de suivre l'atteinte des objectifs, la gestion des risques et l'adéquation des moyens	oui	Facile	N/A	CODIR	Moyen	
	Gouvernance	Architecture du site mise à jour de façon régulière ou en cas de changement majeur	Oui	Difficile	Difficile	Opérations, DSI	Difficile	Cet indicateur dépend de l'organisation et des compétences en place (centralisées vs décentralisées), de l'existence d'un référentiel à jour.
	Inventaires	Part des interconnexions du système industriel avec l'extérieur prenant en compte les exigences de cybersécurité	100%	Facile	N/A	CODIR, Opérations	Difficile	Les interconnexions extérieures peuvent intégrer les interconnexions avec des SI externes ou avec des SI non industriels, selon les définitions de chaque entité dans sa PSSI. La maîtrise des interconnexions est un élément critique pour assurer la sécurité des sites. Les fournisseurs de systèmes industriels sont encore peu matures en cybersécurité, et il n'est pas rare de rencontrer des fournisseurs utilisant des listes Excels partagées avec tous les mots de passe de leurs clients. La maitrise de l'inventaire des accès peut être réalisée via la revue des contrats fournisseurs, la mise en place d'un outil de découverte, etc.SI non industriels, selon les définitions de chaque entité dans sa PSSI.

Domaine NIST	Thème	KPI	Valeur cible	Collecte	Auto-matisation	Public	Remédiation	Commentaires ou points d'attention
Protect	Accès	Pourcentage des assets (Automate, PC, Serveurs, Applications, AD...) ayant des revues des comptes régulières (comptes utilisateurs, comptes administrateurs, accès...)	> 80%	Difficile	Difficile	Opérations, DSI	Difficile	Asset fait référence à tout ce qui est connecté au réseau. Sur les équipements OT, nous avons des comptes opérateurs et comptes locaux qui doivent être revus que l'asset soit dans l'AD ou pas. Exemple de stratégie de revue : revue tournante par nature d'équipement. Certaines sociétés ont des assets mobiles (équipements qui sont en mouvement ou utilisés uniquement à certaines périodes). Ce KPI est faisable pour des entreprises gérant des assets fixes, la difficulté sera uniquement la fréquence. La faisabilité de cette revue dépend aussi des compétences sur site. Car elle nécessite la capacité à aller voir la configuration et recertifier le compte. La fréquence de revue est à déterminer en fonction de la criticité de l'asset et de l'analyse de risque. Cet indicateur demande une certaine maturité car il nécessite de garder une trace de la revue des comptes au-delà de la réalisation de l'action.
	Accès	Nombre de comptes génériques utilisateur applicatif / Nombre de compte utilisateur applicatif	À déterminer en fonction des usages	Moyen	Moyen	Opérations, DSI	Difficile	La cible est à déterminer en fonction du contexte et l'usage de ces comptes. En effet, certains usages nécessiteront des comptes génériques, tant que l'usage de ces comptes est encadré et tracé, cela permet de les maitriser. L'objectif de cet indicateur sera surtout de mesurer la tendance et éviter une dérive des comptes, car l'usage de comptes génériques dans le monde industriel est parfois inévitable. En cas d'utilisation d'un compte unique sur un ensemble d'assets, cet indicateur peut donner un résultat erroné, il serait dans ce cas intéressant de le combiner à l'indicateur suivant. Si les comptes sont gérés dans l'AD, la collecte et l'automatisation peut être simplifiée.
	Accès	Nombre d'assets utilisant un compte générique / Nombre d'assets industriels	À déterminer en fonction des usages	Moyen	Moyen	Opérations, DSI	Difficile	L'objectif de cet indicateur sera surtout de mesurer la tendance et éviter une dérive des comptes, car l'usage de comptes génériques dans le monde industriel est parfois inévitable. Si les comptes sont gérés dans l'AD, la collecte et l'automatisation peut être simplifiée.
	Accès	Pourcentage assets ne permettant pas une traçabilité de l'authentification	< 10%	Difficile	Difficile	Opérations, DSI	Difficile	Ces assets seront encore dans les usines les 10 prochaines années, donc ils sont à gérer via des mesures compensatoires par exemple via de la sécurité périmétrique ou un moyen différent de traçabilité
	Accès	Pourcentage assets sans possibilité de changer le mot de passe par défaut	< 20%	Moyen	Moyen	Opérations, DSI	Moyen	Certains systèmes anciens ne permettent pas le changement de mot de passe par défaut. Cela peut parfois impacter la garantie sur ces systèmes. De nouveau, des mesures compensatoires sont à identifier. L'automatisation de cet indicateur peut être réalisée via la recherche des comptes par défaut sur les sites de constructeurs et des tests sur les machines.

Domaine NIST	Thème	KPI	Valeur cible	Collecte	Auto-matisation	Public	Remédiation	Commentaires ou points d'attention
Protect	Fournisseurs	Pourcentage des fournisseurs ayant été évalués d'un point de vue posture cybersécurité	> 50%	Difficile	Difficile	CODIR	Difficile	Cet objectif pourrait être mis en place par étape, par exemple en sélectionnant dans un premier temps les fournisseurs pouvant avoir un impact important sur l'entreprise en cas de cyberattaque - Exemple de critères de priorisation : Data (fournisseurs manipulant des données sensibles ou données personnelles), Dépendance (fournisseurs dont l'indisponibilité impacte la continuité business), Interfaces (interconnections logiques et interventions physiques sur site). - Exemple de cibles prioritaires : fabricants de machines, automaticiens, accès aux installations, ayant des données de secret industriel ... Cet indicateur nécessite une organisation adaptée (achats, liste de fournisseurs en place...)
	Sensibilisation	Pourcentage des fournisseurs de services sensibilisés à la cybersécurité	> 70%	Difficile	Difficile	Opérations	Difficile	Il faut que le suivi de la réalisation de la sensibilisation soit effectué par le donneur d'ordre dans l'entreprise. L'intégration d'un fournisseur dans le périmètre dépend de la durée de l'intervention. Cet objectif pourrait être atteint également via la signature d'un engagement de cybersécurité dans le contrat ou lors de l'intervention sur site. Dans le futur, idéalement le fournisseur apporte sa certification cybersécurité lors de son intervention sur site. Cet indicateur nécessite une organisation et une traçabilité des fournisseurs.
	Projets	Pourcentage des projets OT ayant intégré la méthodologie d'intégration de la Sécurité dans les projets	> 70%	Moyen	Moyen	RSSI, CODIR	Difficile	Nécessite une méthodologie en place et communiquée, une capacité à traiter, un référent sur site qui identifie les projets et peut intégrer les réflexes sécurité. Difficulté : recenser les projets. Généralement, les projets sont découverts s'ils impliquent une connexion au reste du SI. De plus il faut que le processus d'intégration de la sécurité dans les projets soit pris en compte au bon moment (et non pas en fin de projet). Pour identifier les écarts en terme d'identification des projets, des audits sur site peuvent être réalisés afin d'identifier les projets non identifier et corriger les processus. L'automatisation de la collecte se fait via des outils de gestion de projet, mais cela nécessite tout de même une intégration manuelle des informations de projet.
	Réseau	Pourcentage des accès distants du site sécurisés (MFA, Bastion...)	100%	Difficile	Difficile	Opérations	Moyen	Les règles par type d'accès distant sont à lister dans la politique de sécurité industrielle. Différents types d'accès distants sont possibles : accès d'administration, accès utilisateurs... Si le périmètre total couvre uniquement les outils d'usine, la cible 100% peut être atteignable. Mais atteindre 100% peut s'avérer difficile lorsqu'on intègre les réseaux auxiliaires au fonctionnement de l'usine (GTB/GTC, surveillance, dispositifs d'accès, gestion des systèmes de protection contre les incendies...), l'objectif sera dans ce cas revu à la baisse. La stratégie de leur sécurisation peut aussi être différente (ex. segmentation). La remédiation nécessite un changement des usages.

Exemple d'indicateurs pour le niveau intermédiaire

Domaine NIST	Thème	KPI	Valeur cible	Collecte	Auto-matisation	Public	Remédiation	Commentaires ou points d'attention
Protect	Réseau	Une revue des interconnexions externes et de leur niveau de sécurité est réalisée régulièrement	> 80%	Difficile	Difficile	Opérations	Difficile	Sur la couche réseau: la surveillance peut être réalisée via des scans externes du plan d'adressage IP. Sur la couche applicative: la connaissance des interconnexions peut s'avérer difficile (identification de la liste des APIs, des accès...). Pour avancer dans la remédiation, il peut être pragmatique de commencer par maitriser les interconnexions réseaux avant d'aller couvrir les interconnexions applicatives. La remédiation nécessite d'identifier le contexte d'utilisation de l'interconnexion puis de mettre en place la solution alternative en collaboration avec les équipes opérations.
	Vulnérabilités	Date de la dernière campagne de remédiation (patching, upgrade, durcissement) de l'environnement industriel (ou nombre de mois depuis la dernière campagne)	< 12 mois selon la stratégie de patching et l'exposition	Moyen	Moyen	Opérations	Difficile	Dans les environnements industriels, cela nécessite souvent un arrêt de la production et se fait dans le cadre de campagnes de maintenance et patching annuelle. Chaque prestataire a une stratégie spécifique : patching, upgrade, durcissement. Cet objectif sera à associer à l'activité de maintenance. La source sera la GMAO. L'utilisation de la GMAO par le mainteneur informatique permettra de centraliser l'information et d'automatiser la collecte de l'indicateur.
	Vulnérabilités	Pourcentage de machines avec un anti-virus à jour (signatures à jour) ou EDR	> 70%	Facile	Facile	Opérations, DSI	Moyen	Ce KPI pourrait exclure les machines non connectées, isolées et scellées ayant une stratégie de sécurité différente. Le prérequis pour cet indicateur est d'avoir une base d'asset en place et une identification d'asset commune entre la base d'asset et l'outil de sécurité. La remédiation nécessite parfois une requalification de l'outil de protection et un échange avec le fournisseur pour s'assurer d'avoir l'autorisation d'utilisation de ces outils sur les machines au risque de perdre le support. La mise en œuvre sera plus simple sur un nouveau parc (contrats négociés, exigences intégrées dès le début des projets...) que sur un parc existant.
	Vulnérabilités	Pourcentage de systèmes obsolètes maitrisés (inventaire en place, plan de gestion d'obsolescence défini, exposition réduite)	> 80%	Moyen	Difficile	Opérations	Difficile	Il est acceptable d'avoir des systèmes obsolètes dans le système industriel du moment où ils sont maitrisés. Certains systèmes industriels même acquis récemment, peuvent être livrés avec des OS déjà obsolètes. Standardiser et moderniser le matériel n'est pas toujours faisable. Le owner du système doit assurer une veille sur l'état des équipements et des solutions. La gestion de l'obsolescence peut se faire par exemple : via un plan de modernisation (en profiter pour standardiser) ; via cloisonnement et gestion des backup, scellement...

Exemple d'indicateurs pour le niveau intermédiaire

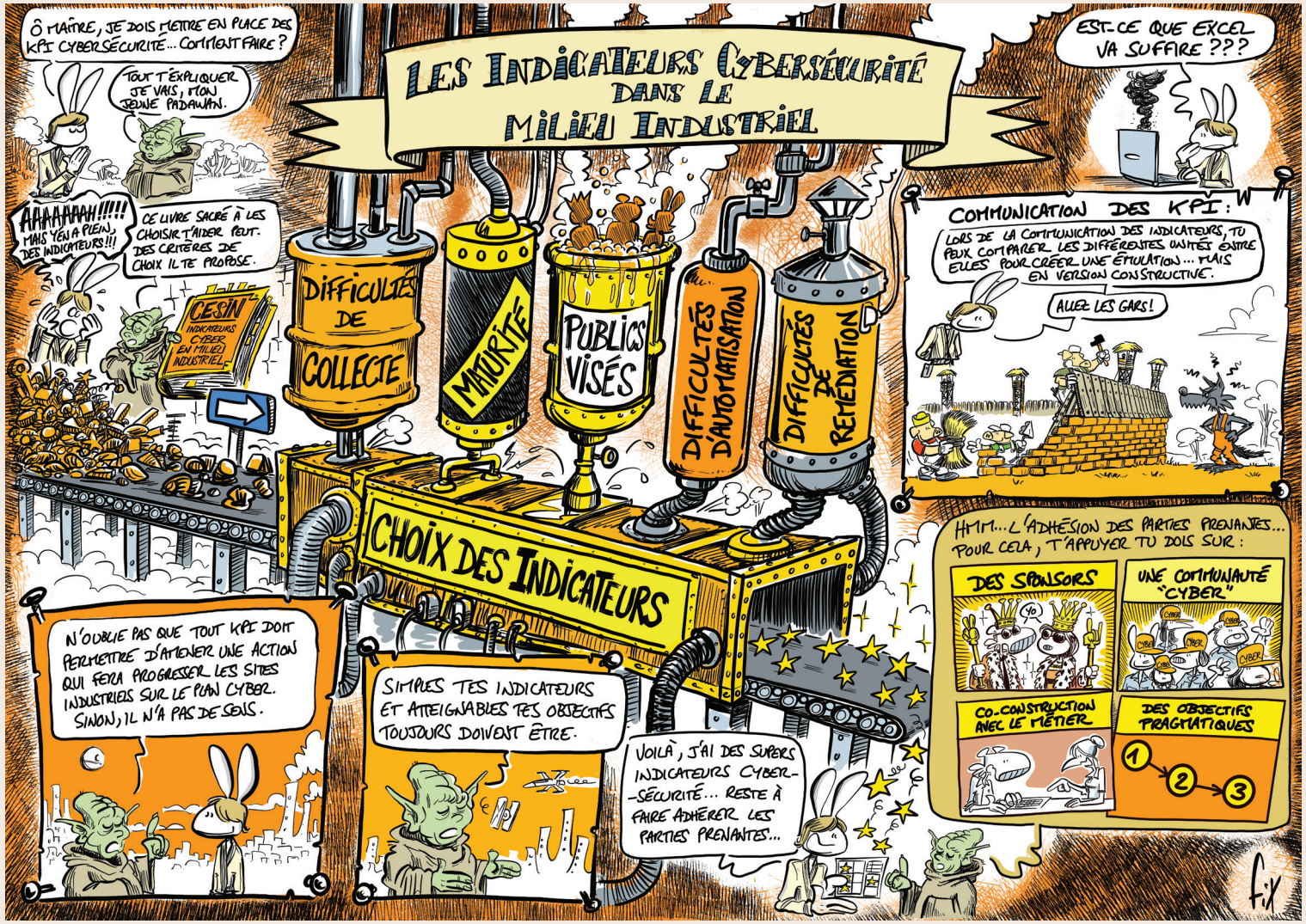
Domaine NIST	Thème	KPI	Valeur cible	Collecte	Auto-matisation	Public	Remédiation	Commentaires ou points d'attention
Detect	Supervision sécurité	Pourcentage des assets dont les logs ont une référence temporelle universelle et identique entre l'ensemble des assets	> 80%	Difficile	Difficile	Opérations	Difficile	Une référence temporelle utilisant NTP ou world GPS. Cet objectif est important pour l'analyse fine des incidents, mais il sera complexe de démarrer par cet indicateur au niveau initial car il n'apportera pas de bénéfices immédiats visibles pour le métier.
	Supervision sécurité	Les évènements de sécurité pertinents sont remontés dans un système centralisé et sécurisé (ex. puit de log, SIEM)	> 80%	Facile	Facile	RSSI, DSI, Opérations	Moyen	Le volume des évènements ne permet pas de remonter tous les logs. Par exemple, il n'est pas forcément pertinent de remonter les logs de l'ensemble des switches, cependant il peut être suffisant de remonter ceux des switches centraux et des firewalls du site. Certains systèmes anciens ont des logs dans une langue locale qui ne peut pas être exploitée par un SOC exerçant dans une langue différente. L'indicateur se concentre en conséquence sur le choix du log et sa centralisation. La collecte de l'indicateur nécessite de vérifier que les logs adéquats sont configurés. Il est possible de vérifier cela en comparant le périmètre couvert par le SIEM et le périmètre connu. Les acteurs (et le public visé) va dépendre de qui a la main sur le déploiement des outils de sécurité et la configuration des logs.
Respond	Gestion des incidents	Pourcentage des parties prenantes essentielles à la gestion de crise formées au processus de gestion d'incidents et de crises	> 90%	Facile	Moyen	CODIR, Opérations, DSI	Facile	Les parties prenantes essentielles intègrent notamment : responsables opérationnels, DSI, CODIR, l'équipe communication, le service juridique, les équipes RH... Les fournisseurs et partenaires essentiels doivent aussi être pris en compte (ex. via une sensibilisation, via la contractualisation...). L'automatisation peut être réalisée via la mise en place d'un E-learning. Cet E-learning doit intégrer une partie validation des savoirs. Faire progresser cet indicateur demande essentiellement des moyens humains pour sa mise en œuvre (temps de préparer et réaliser les formations)
Recover	Continuité	Pourcentage d'assets avec backup respectant le principe 3-2-1 (3 copies sur 2 supports différents et 1 copie offsite	> 80%	Moyen	Difficile	CODIR, Opérations	Difficile	Il est éventuellement possible d'éviter les deux supports différents en ayant un support dont on garantit l'immutabilité. Dans l'environnement industriel, certains assets sont isolés seront complexes à atteindre pour la remédiation. Il convient dans ce cas de se concentrer sur les assets critiques.

Exemple d'indicateurs pour le niveau avancé

Domaine NIST	Thème	KPI	Valeur cible	Collecte	Auto-matisation	Public	Remédiation	Commentaires ou points d'attention
Identify	Gouvernance	La direction fournit les moyens (humains et/ou financiers) nécessaires afin de pouvoir réaliser les missions confiées	oui	Moyen	Difficile	CODIR	Difficile	Cet indicateur va dépendre de l'organisation de chaque entité et du fonctionnement de l'attribution budgétaire. La direction peut faire référence à une direction locale ou centrale. L'identification et l'alignement sur le budget affecté à la cybersécurité peut s'avérer complexe.
	Gouvernance	Le risque cybersécurité est intégré à l'analyse de risque métier. Cette analyse est réalisée et mise à jour de façon régulière ou en cas de changement majeur	Oui	Facile	N/A	CODIR	Difficile	L'accompagnement métier par des spécialistes cybersécurité peut être nécessaire pour identifier les sources cybersécurité des risques métier. L'automatisation via un outil n'est pas faisable, cependant, il est possible d'avoir un processus systématique via la structure organisationnelle existante (exemple : le risk manager métier intègre la source cybersécurité dans la mise à jour de l'analyse de risque métier). La mise en place de cet objectif nécessite une culture de la gestion du risque. Cette culture sera variable selon les secteurs.
	Inventaires	L'architecture du site est mise à jour de façon automatisée	Oui	Difficile	Difficile	Opérations, DSI	Difficile	L'automatisation complète de l'architecture via des sondes n'est pas possible, il est nécessaire de compléter manuellement. Car la sonde récupère une partie de l'information uniquement (l'information IT), il manquera les informations de contexte. Cet objectif nécessite un investissement important. Il est nécessaire d'évaluer le cas d'usage.
Protect	Fournisseurs	Pourcentage des fournisseurs audités conformément à la fréquence établie	> 90%	Difficile	Difficile	CODIR, Opérations	Difficile	Pour pouvoir auditer les fournisseurs, les exigences à vérifier doivent être présentes dans le contrat. Pour plus d'efficacité, il est recommandé d'aller sur le site fournisseur pour vérifier la mise en place des pratiques et pas uniquement sur base de preuves documentaires. La fréquence de ces audits doit être réalisable et selon le volume de fournisseurs à adresser (ex. tous les 2 à 3 ans) Les fournisseurs à prioriser pour ces audits sont ceux ayant des accès distants. Les points à vérifier notamment intègrent : machines utilisées pour les accès distants, l'utilisation des comptes et gestion des mots de passe.... L'automatisation peut s'appuyer sur des plateformes GRC (ex. TISAX)
	Réseau	La segmentation réseau est conforme aux objectifs de segmentation (ex. VLAN distincts selon l'exposition, selon l'usage, etc.)	Oui	Difficile	Moyen	Opérations	Difficile	Les objectifs ciblés peuvent être différents d'une entité à l'autre. Car chaque société définira des étapes différentes pour aller vers une segmentation appliquant les principes du Purdue. La remédiation (ex. changement d'adressage IP) nécessite des arrêts machine ce qui rend la remédiation difficile.

Exemple d'indicateurs pour le niveau avancé

Domaine NIST	Thème	KPI	Valeur cible	Collecte	Auto-matisation	Public	Remédiation	Commentaires ou points d'attention
Protect	Sensibilisation	Pourcentage des intervenants (internes et externes) sur les systèmes du site formés à la cybersécuritép	> 80%	Moyen	Difficile	Opérations	Difficile	Ces formations peuvent être ciblées selon les activités des populations. Il est recommandé d'intégrer les externes quand ils sont amenés à réaliser des missions de longue durée. Cet indicateur nécessite une organisation sur le site pour enregistrer les interventions et tracer les formations. Il dépendra aussi de la maturité globale de l'entreprise concernant sa gestion notamment de la sécurité physique (et pas uniquement sa maturité cyber).
	Vulnérabilités	Part des assets exposés avec des vulnérabilités critiques ou high (CVSS >7) ou des vulnérabilités activement exploitées, dans son contexte (exposition, criticité...)	0	Difficile	Difficile	Opérations	Difficile	Le prérequis est d'avoir des équipes formées à la gestion des vulnérabilités et le sponsorship adéquat.
Detect	Supervision sécurité	Pourcentage des assets avec des évènements de sécurité supervisés par un SOC (analyse continue et gestion des alertes)	100%	Facile	Facile	RSSI, DSI	Moyen	
Respond	Continuité	Date du dernier exercice de PCA	< 24 mois	Facile	N/A	CODIR, Opérations	Moyen	Sur un site industriel, l'exercice se fera dans un premier temps en mode Table Top
	Gestion des incidents	Date du dernier exercice de gestion de crise	< 24 mois	Facile	N/A	CODIR, Opérations, DSI	Moyen	Sur un site industriel, l'exercice se fera dans un premier temps en mode Table Top
Recover	Continuité	Pourcentage d'assets dont les backups sont testés	> 80%	Moyen	N/A	CODIR, Opérations	Difficile	
	Continuité	Date du dernier test de PRA	< 24 mois	Facile	N/A	CODIR, Opérations, DSI	Difficile	Sur un site industriel, l'exercice se fera dans un premier temps en mode Table Top. Le test d'un PRA complet peut impliquer un coût conséquent. Les jumeaux numériques peuvent offrir une opportunité pour l'atteinte de l'objectif.


LES INDICATEURS CYBERSÉCURITÉ DANS LE MILIEU INDUSTRIEL
Ô MAÎTRE, JE DOIS METTRE EN PLACE DES KPI CYBERSÉCURITÉ... COMMENT FAIRE ?
TOUT T'EXPLIQUER JE VAIS, MON JEUNE PADAWAN.
AAAAAAAH!!!!! MAIS Y'EN A PLEIN, DES INDICATEURS !!!
CE LIVRE SACRÉ À LES CHOISIR T'AIDER PEUT. DES CRITÈRES DE CHOIX IL TE PROPOSE.
CESIN INDICATEURS CYBER EN MILIEU INDUSTRIEL
DIFFICULTÉS DE COLLECTE
MATURITÉ
PUBLICS VISÉS
DIFFICULTÉS D'AUTOMATISATION
DIFFICULTÉS DE REMÉDIATION
CHOIX DES INDICATEURS
N'OUBLIE PAS QUE TOUT KPI DOIT PERMETTRE D'ATTEINDRE UNE ACTION QUI FERA PROGRESSER LES SITES INDUSTRIELS SUR LE PLAN CYBER. SINON, IL N'A PAS DE SENS.
SIMPLES TES INDICATEURS ET ATTEIGNABLES TES OBJECTIFS TOUJOURS DOIVENT ÊTRE.
VOILÀ, J'AI DES SUPERS INDICATEURS CYBER-SÉCURITÉ... RESTE À FAIRE ADHÉRER LES PARTIES PRENANTES...
EST-CE QUE EXCEL VA SUFFIRE ???
COMMUNICATION DES KPI :
LORS DE LA COMMUNICATION DES INDICATEURS, TU PEUX COMPARER LES DIFFÉRENTES UNITÉS ENTRE ELLES POUR CRÉER UNE ÉMULATION... MAIS EN VERSION CONSTRUCTIVE.
ALLEZ LES GARS !
HMM... L'ADHÉSION DES PARTIES PRENANTES... POUR CELA, T'APPUYER TU DOIS SUR :
DES SPONSORS
UNE COMMUNAUTÉ "CYBER"
CO-CONSTRUCTION AVEC LE MÉTIER
DES OBJECTIFS PRAGMATIQUES
1
2
3
FiX

Les Indicateurs cybersécurité dans le milieu industriel

Club des Experts de la Sécurité
de l'Information et du Numérique
contact@cesin.fr
www.cesin.fr