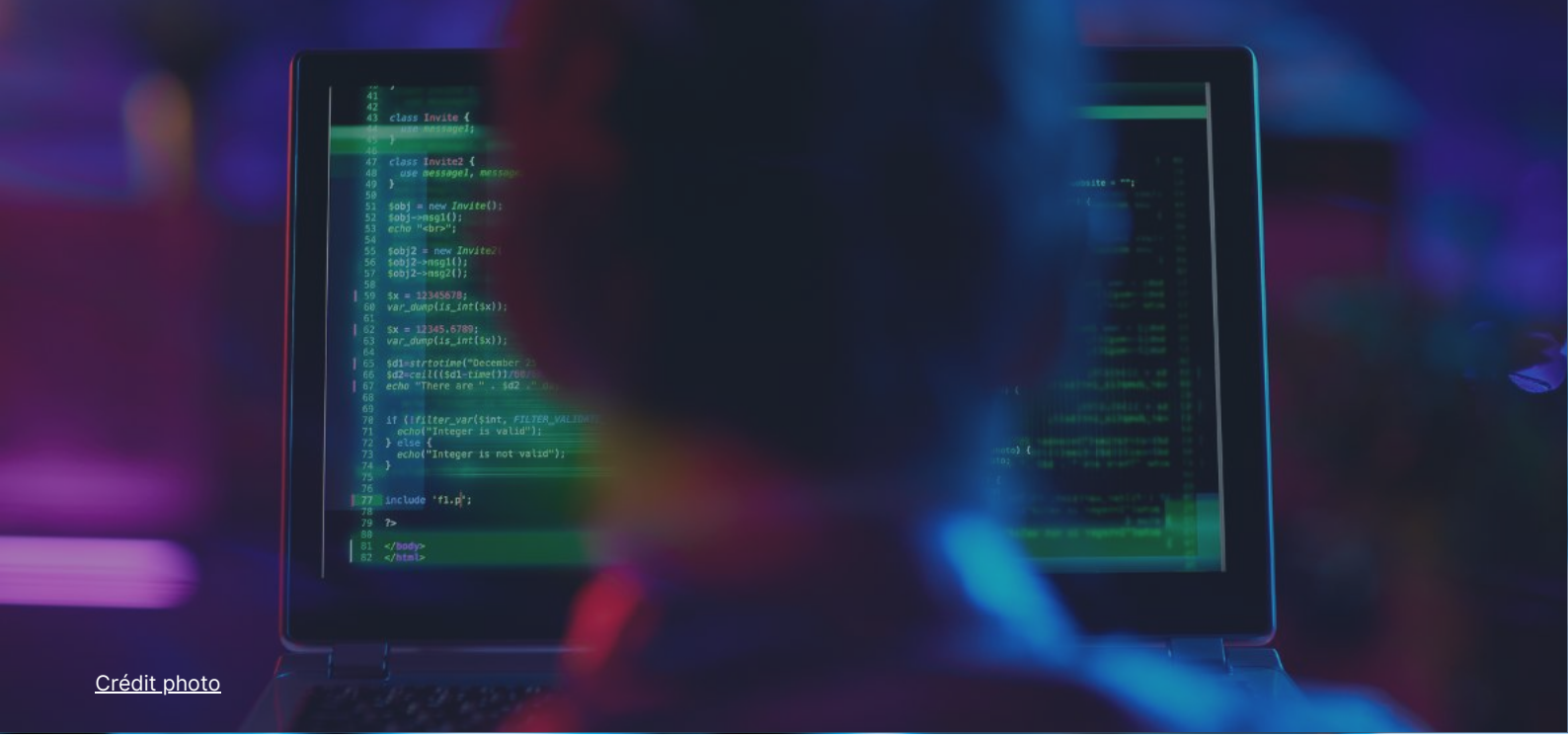
Timly

Cybersecurity Asset Management

Focus sur le registre des actifs pour réduire les risques et sécuriser les audits

Crédit photo

Sommaire



Crédit photo

Avant-propos et objectifs de ce livre blanc

Il est impossible de protéger des actifs dont on ignore l'existence. C'est pourtant la situation de nombreuses entreprises aujourd'hui : elles ont bien un inventaire de leurs actifs informatiques, mais il est éparpillé entre plusieurs outils, jamais à jour et aveugle aux enjeux de sécurité.

La conséquence ? Des angles morts sur la surface d'attaque, des délais dans la réponse aux incidents et des preuves de conformité à rassembler manuellement. Ce livre blanc explique pourquoi un registre des actifs constitue la base opérationnelle d'une cybersécurité efficace, et comment les entreprises peuvent le construire et le maintenir dans la durée.

1.1 Pourquoi la gestion des actifs de cybersécurité est aujourd'hui une priorité

Les surfaces d'attaque des entreprises s'étendent aujourd'hui plus vite que ne peuvent suivre la plupart des modèles de sécurité et d'exploitation. En plus des actifs informatiques traditionnels comme les ordinateurs portables, les serveurs et les composants réseau, le paysage de la cybersécurité inclut désormais les ressources cloud, les applications SaaS, les identités, les prestataires externes, les composants IoT et les systèmes OT connectés.

C'est particulièrement vrai dans des secteurs comme la construction, le facility management, l'industrie manufacturière et l'IT, où des environnements hautement dynamiques se créent en permanence : sites changeants, équipements mobiles, infrastructures temporaires et responsabilités partagées entre l'IT, les opérations et les équipes métiers.

Le problème de fond n'est que rarement un manque de technologie. De nombreuses entreprises disposent déjà d'un parc informatique documenté, mais au travers d'inventaires séparés, peu synchronisés et rarement reliés aux enjeux de cybersécurité. Pourtant, des questions essentielles restent souvent sans réponse : **quels actifs sont réellement critiques pour la sécurité ? Qui en est responsable ? Quel est leur niveau de criticité ? Où en est leur posture de sécurité aujourd'hui ?**

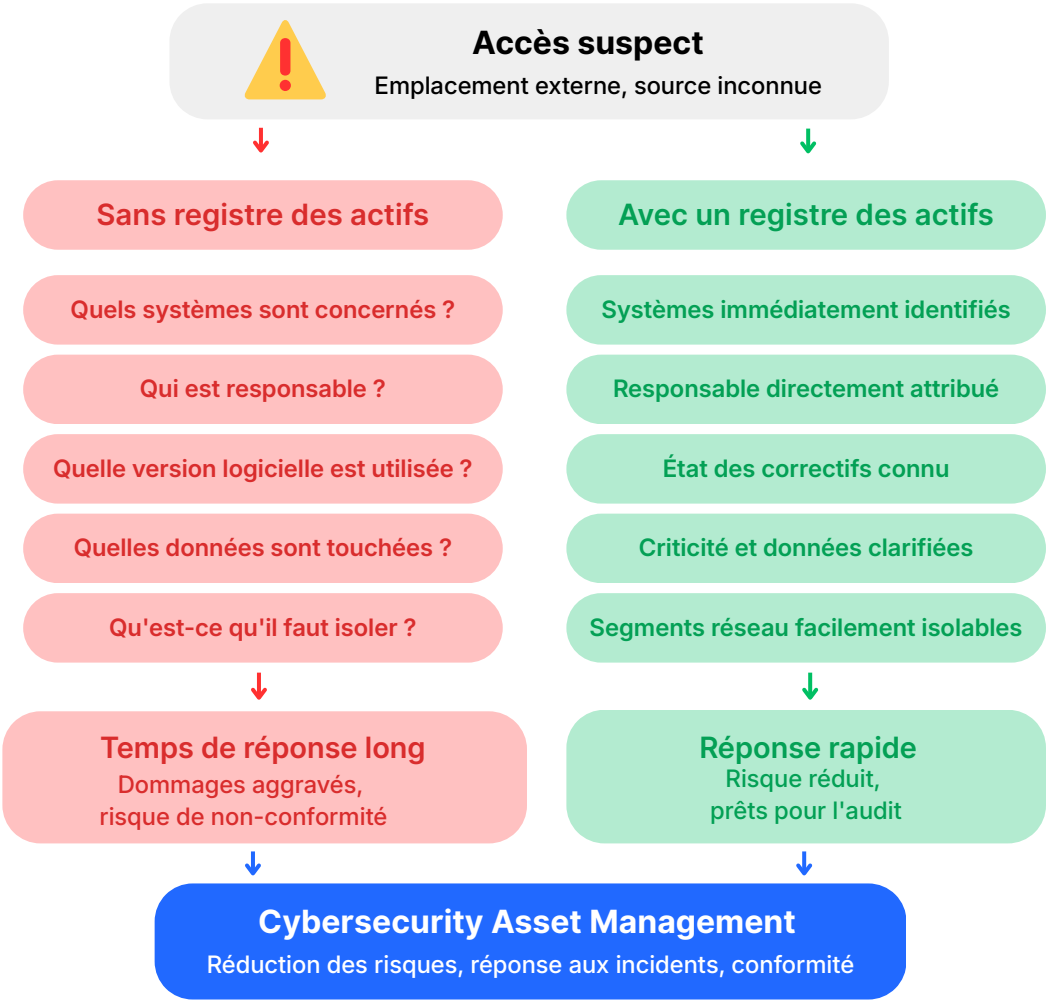
C'est précisément ce manque de réponses qui fait basculer la gestion des inventaires d'actifs d'un simple enjeu opérationnel vers un sujet central de cybersécurité. Son importance se mesure concrètement.

- Selon le Data Breach Investigations Report 2025 de Verizon, 46 % des systèmes compromis contenant potentiellement des identifiants d'accès d'entreprise dans l'un des jeux de données analysés **n'étaient pas intégrés à l'environnement de gestion centralisée de l'entreprise**. [1]
- Le rapport Cost of a Data Breach 2025 d'IBM montre également que 40 % des violations de données étudiées impliquaient des informations réparties sur plusieurs environnements, et que ces incidents nécessitaient en moyenne 283 jours pour être identifiés et contenus.[2]

L'exemple qui suit illustre l'importance de la visibilité : une tentative d'accès suspecte (via un système externe ou un compte cloud mal inventorié, par ex.) met immédiatement en lumière à quel point la transparence sur l'ensemble des actifs est critique. **Sans vue centralisée des actifs, les équipes de réponse aux incidents manquent de réponses claires à des questions comme : quels systèmes sont concernés ? Qui en est responsable ? Quelles données sont impliquées ? Qu'est-ce qu'il faut isoler en priorité ?** Cela retarde les efforts de réponse et augmente le niveau de risque.

À l'inverse, un registre des actifs informatiques, complet, à jour et exploitable par les équipes de cybersécurité permet d'identifier immédiatement les systèmes affectés, de les prioriser correctement et de les rattacher aux responsables adéquats. Ce schéma montre comment des informations telles que l'état des correctifs, la criticité, les segments réseau, les identités, les interfaces et les emplacements peuvent être centralisées, permettant une réponse rapide et prête pour l'audit.

La gestion des actifs de cybersécurité cesse ainsi d'être une discipline d'inventaire de niche pour devenir un prérequis à la réduction efficace des risques, à une réponse opérationnelle aux incidents et à une conformité durable.



1.2 À qui s'adresse ce livre blanc ?

Ce livre blanc s'adresse aux entreprises qui souhaitent structurer leurs processus de sécurité et de conformité dans la base fiable que représente un registre des actifs.

Ce contenu est pertinent pour :

- Les RSSI, responsables de la sécurité de l'information
- Les directions IT et équipes informatiques
- Les responsables OT et de la production
- Les responsables du facility management
- Les professionnels de la conformité, du risque et de l'audit
- Les équipes d'audit interne et de gouvernance

De nombreuses entreprises connaissent déjà les principaux standards de sécurité et exigences réglementaires, comme ISO/IEC 27001:2022, NIS2 ou des cadres spécifiques à leur secteur. **Ce qui manque souvent, en revanche, c'est une approche pratique pour construire et maintenir, au quotidien, un inventaire complet et sécurisé de leurs actifs**.

C'est exactement sur ce point que ce livre blanc apporte des recommandations concrètes.

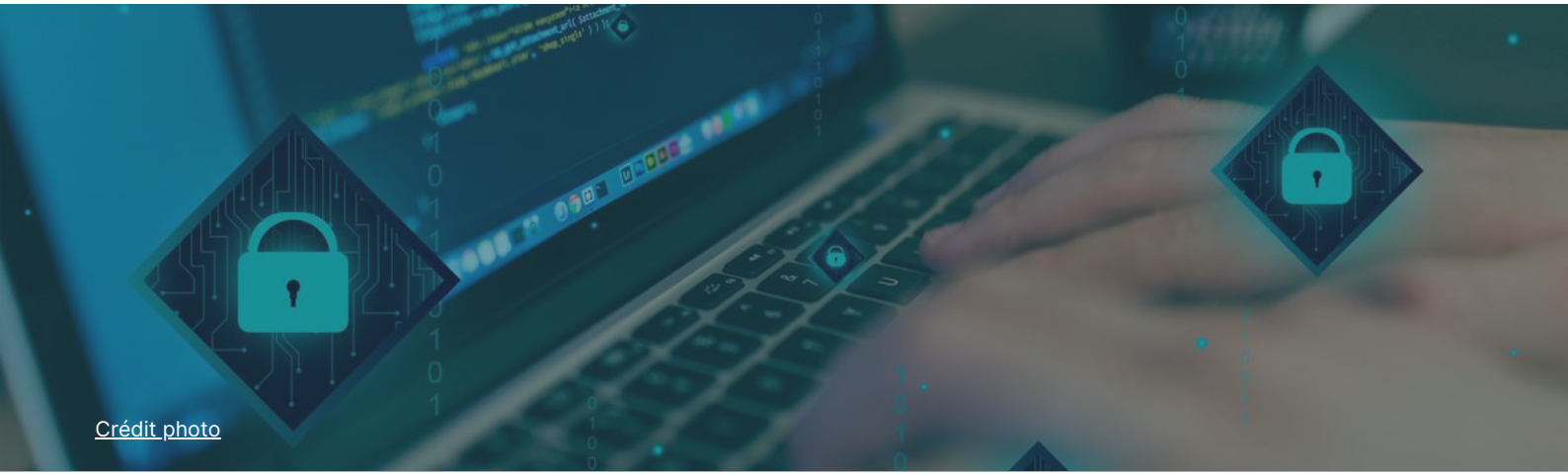
Il croise les perspectives technique, organisationnelle et processuelle pour montrer comment les entreprises peuvent mettre en place un registre d'actifs central comme fondation de leur sécurité.

1.3 Objectifs et structure de ce livre blanc

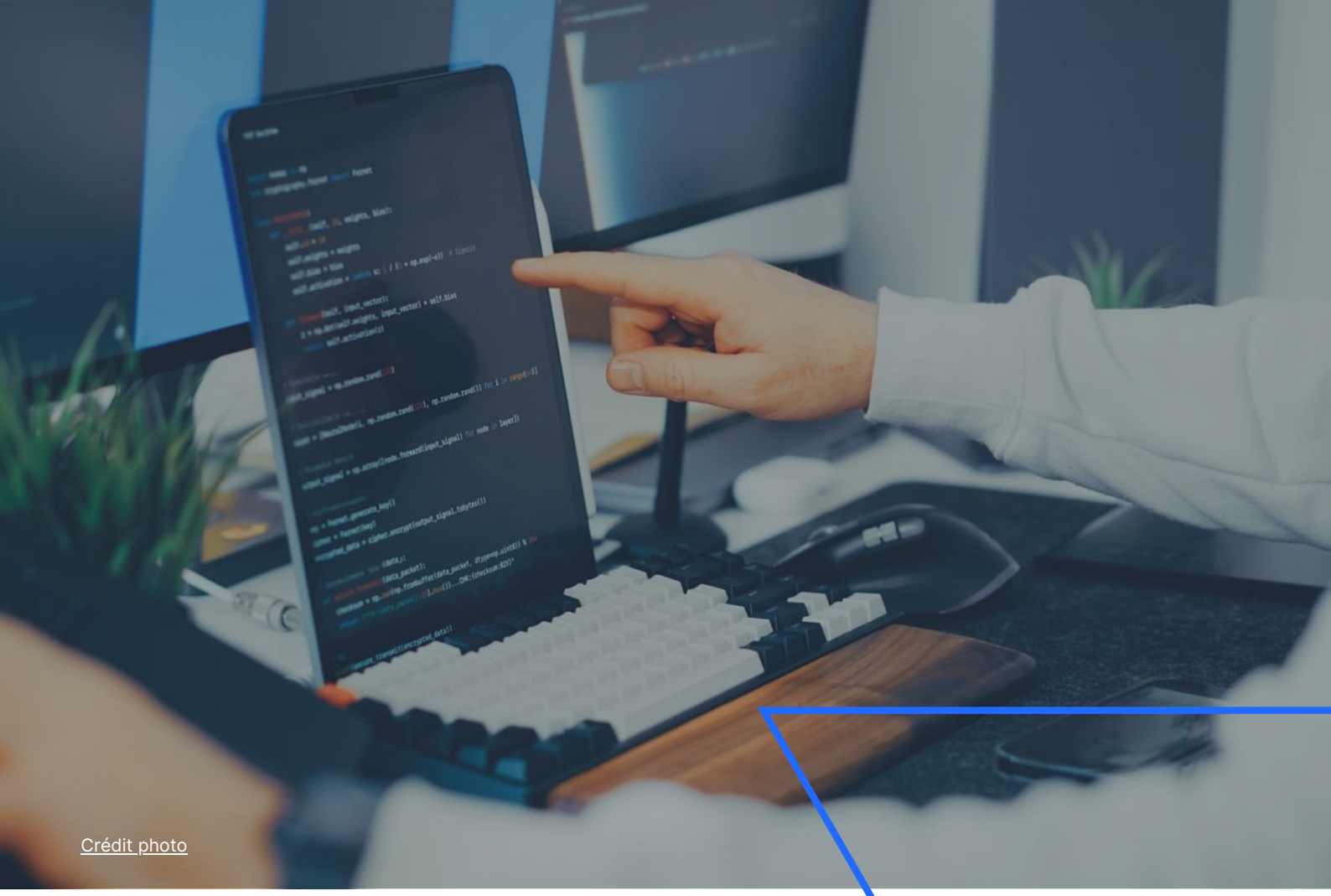
Cybersecurity Asset Management pourquoi un inventaire des actifs incomplet ne constitue pas seulement un problème de gestion, mais représente également un **risque direct pour la cybersécurité et la conformité**. Il montre comment les actifs inconnus, l'absence de responsabilités clairement définies et des données d'inventaire fragmentées fragilisent les processus de gestion des correctifs, la réponse aux incidents, la capacité à réussir les audits ainsi que le reporting destiné à la direction.

Dans un second temps, ce livre blanc présente les **exigences que les normes et les cadres réglementaires imposent** à un registre des actifs fiable. Il propose également une approche pragmatique pour construire un registre des actifs sécurisé, en détaillant les principales catégories d'actifs, les rôles et responsabilités, un modèle de maturité simple, les processus de sécurité essentiels ainsi que des exemples d'indicateurs de performance (KPI).

Enfin, ce livre blanc développe un plan d'action sur 90 jours, que les entreprises peuvent utiliser pour évaluer leur maturité actuelle et hiérarchiser les actions d'amélioration.



Crédit photo



Crédit photo

Qu'est-ce que la gestion des actifs de cybersécurité ?

Définition et scope

Qu'est-ce que la gestion des actifs de cybersécurité ?

Définition et scope

Avant de mettre en place un registre des actifs, les entreprises ont besoin de répondre clairement à une question fondamentale : que comprend précisément la gestion des actifs de cybersécurité, et en quoi se distingue-t-elle de la gestion de parc informatique classique ?

2.1 Définition et différenciation

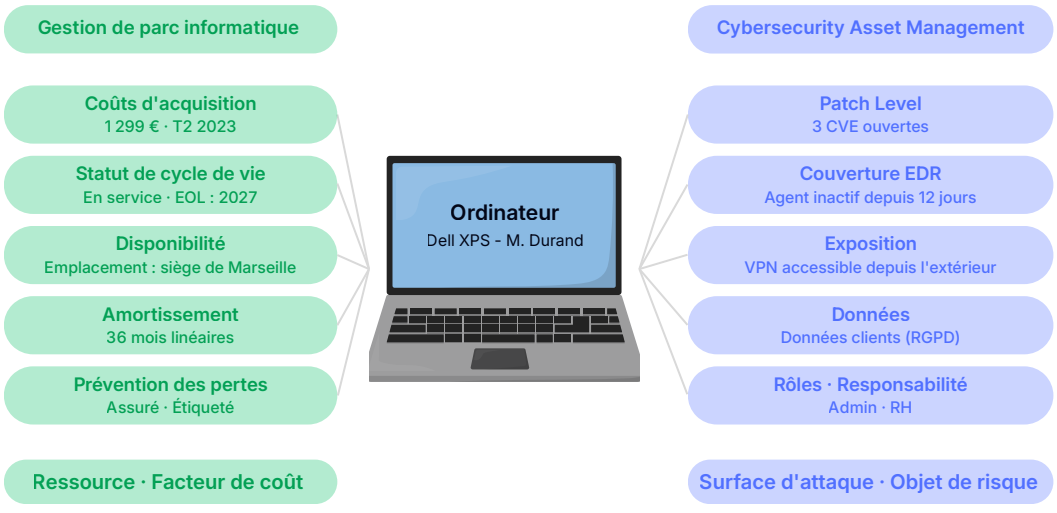
> La gestion des actifs de cybersécurité (Cybersecurity Asset Management) est le processus continu qui consiste à identifier, documenter, classifier, attribuer des responsables et enrichir tous les actifs pertinents pour la sécurité avec des informations de sécurité et de risque.

Contrairement à la gestion de parc informatique, l'objectif principal n'est pas la gestion opérationnelle ou financière du cycle de vie. L'accent est mis sur la compréhension des risques, des dépendances et de la surface d'attaque associés à chaque actif.

Alors que **la gestion de parc informatique considère principalement les actifs comme des éléments opérationnels ou liés aux coûts, la gestion des actifs de cybersécurité élargit cette perspective en y intégrant un contexte de sécurité et de conformité,** incluant notamment : l'état des correctifs, le niveau d'exposition, la criticité, les identités, les vulnérabilités, ainsi que la responsabilité.

Ainsi, un appareil géré devient un objet de sécurité géré.

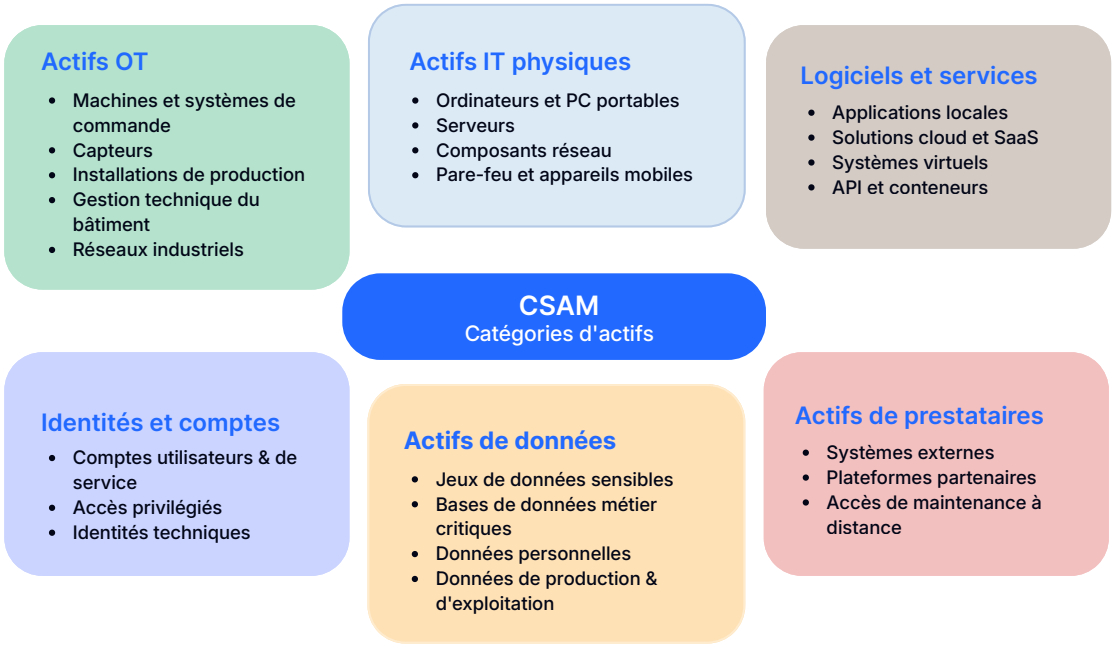
Le schéma qui suit met en évidence ce changement de perspective à travers un exemple concret. Là où un ordinateur portable est avant tout vu, dans un contexte de gestion de parc, comme un équipement opérationnel géré, il est considéré, dans un contexte de gestion des actifs de cybersécurité, sous l'angle de son profil de sécurité et de risque : responsabilité, état des correctifs, niveau d'exposition et mesures de sécurité mises en œuvre.



2.2 Quelles catégories d'actifs sont couvertes ?

Une gestion des actifs de cybersécurité réellement efficace ne se limite pas aux postes de travail et aux serveurs. En réalité, tout ce qui est susceptible de générer un risque de sécurité, de conformité ou d'exploitation devrait être pris en compte.

Exemples de catégories d'actifs couvertes par le CSAM :



L'essentiel n'est pas seulement de savoir qu'un actif existe, mais de disposer de son contexte :

- Criticité
- Responsable
- Statut de sécurité
- Dépendances
- Pertinence pour la conformité

C'est seulement avec ces informations qu'un registre des actifs devient une base fiable pour la cybersécurité.

2.3 Rôles et responsabilités dans un dispositif de CSAM

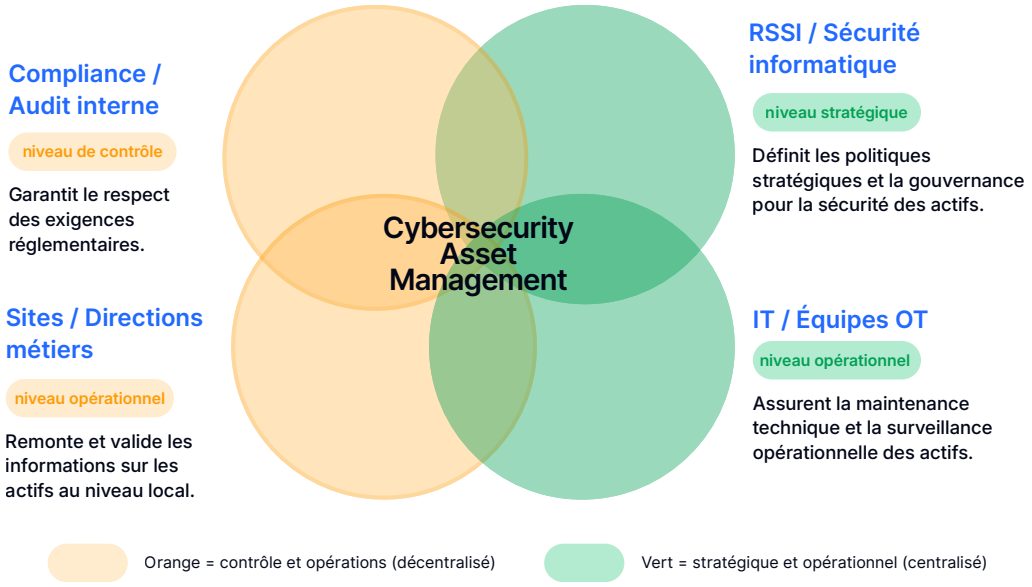
Pour qu'un registre des actifs soit exploitable, les responsabilités doivent être clairement posées. Chaque actif critique pour la sécurité doit avoir un responsable identifié, qu'il s'agisse d'un responsable métier, d'une équipe IT/OT ou d'une fonction support.

Sans cette clarté, la mise à jour des informations est irrégulière et la gestion des changements ou des incidents se fait avec retard. Un Cybersecurity Asset Management efficace répartit les responsabilités de façon délibérée entre trois niveaux : stratégique, opérationnel et de contrôle. Le schéma ci-dessous illustre un modèle de rôles typique, où ces trois niveaux se rejoignent.

Le CSAM crée un cadre commun qui relie le pilotage stratégique assuré par le RSSI et les équipes de cybersécurité aux responsabilités opérationnelles des équipes IT/OT et des métiers, ainsi qu'aux activités de contrôle menées par la conformité et l'audit interne. Dans ce schéma, les zones en orange représentent les responsabilités opérationnelles et de contrôle décentralisées ; les zones en vert, les responsabilités stratégiques et opérationnelles centralisées.

Modèle de rôles en Cybersecurity Asset Management

Le CSAM relie les responsabilités stratégiques, opérationnelles et de contrôle au sein d'un modèle commun.



2.4 Modèle de maturité pour le Cybersecurity Asset Management

Les entreprises se situent à des niveaux de maturité très différents en matière de gestion des actifs de cybersécurité. Avant d'investir dans de nouveaux logiciels, il est donc utile d'évaluer d'abord la situation actuelle de l'entreprise. **Un modèle de maturité simple permet de définir un point de départ réaliste.**

Niveau 1 : Fragmenté

- Les données d'actifs se trouvent dans des feuilles de calcul ou des outils isolés
- Aucune vue complète sur l'ensemble des systèmes IT et OT
- Les responsabilités sont floues ou inexistantes
- Les données sont souvent obsolètes

Question type :
« Sommes-nous vraiment capables de dire quels systèmes existent aujourd'hui dans l'entreprise ? »

Niveau 2 : Consolidé

- Premiers inventaires centralisés ou débuts de structures CMDB
- Découverte des actifs partiellement automatisée
- Informations de sécurité de base intégrées
- Des lacunes et silos d'information subsistent

Question type :
« Nos données sont-elles suffisamment à jour et complètes pour étayer nos décisions de sécurité ? »

Niveau 3 : Maîtrisé

- Processus et responsabilités clairement définis
- Des KPI de sécurité sont suivis activement
- Les données d'actifs soutiennent la gestion des correctifs, la gestion des risques et la réponse aux incidents
- Des contrôles qualité réguliers sont en place

Question type :
« Sommes-nous capables d'identifier rapidement les actifs concernés lors d'un incident ? »

Niveau 4 : Intégré

- La gestion des actifs est pleinement intégrée aux processus de sécurité et de conformité
- Données de haute qualité, mises à jour en continu
- Workflows automatisés et processus de gouvernance en place
- Éléments de preuve prêts pour l'audit à tout moment

Question type :
« Exploitons-nous activement nos données d'actifs pour piloter le risque et la conformité ? »

Crédit photo

Cybersecurity Asset Management

Problème et contexte

Cybersecurity Asset Management: Problème et contexte

Dans la plupart des entreprises, la difficulté ne provient pas d'un manque de données, mais d'un défaut de consolidation. Les CMDB, outils de découverte, portails cloud et inventaires locaux fonctionnent souvent en silos, sans permettre une vue d'ensemble cohérente. Par ailleurs, les environnements IT et OT évoluent plus rapidement que les inventaires ne sont actualisés : nouveaux sites, ressources cloud provisionnées ponctuellement, prestataires externes, terminaux non gérés.

Il en découle des responsabilités insuffisamment définies, une multiplication des angles morts de sécurité et une surface d'attaque difficilement maîtrisable dans son ensemble. Ce chapitre met en évidence les limites des approches classiques ainsi que les risques qui en résultent concrètement.

3.1 La complexité croissante des environnements IT et OT

Les entreprises n'évoluent aujourd'hui plus dans un environnement informatique homogène et centralisé. Leurs infrastructures s'appuient sur un **ensemble hétérogène composé de postes de travail, de services cloud, de terminaux mobiles, de plateformes SaaS, d'identités numériques, d'infrastructures réseau, d'accès partenaires et, selon les secteurs, de composants OT** tels que des machines, des automates, des capteurs ou des systèmes d'automatisation des bâtiments. Cette diversité est particulièrement prononcée dans la construction, le facility management et l'industrie manufacturière.

À cela s'ajoute une **évolution constante des environnements opérationnels**. De nouveaux chantiers voient le jour, des réseaux temporaires sont mis en place, des prestataires se voient accorder des accès, de nouveaux services SaaS sont adoptés sans validation centralisée, des ressources cloud sont créées à la demande et certains systèmes restent en exploitation bien au-delà de leur durée de vie initialement prévue. Les actifs évoluent ainsi en continu, souvent à un rythme supérieur à celui des inventaires centralisés et des processus de gouvernance.

Cette situation entraîne des responsabilités floues et multiplie les angles morts en matière de sécurité. Certains systèmes existent, mais ne figurent dans aucun inventaire central. Des équipements sont recensés, sans responsable clairement identifié. Des applications sont en production, mais leur criticité ou leur niveau de correctifs n'est pas documenté de manière fiable. C'est précisément ce constat qui est à l'origine du Cybersecurity Asset Management.

3.2. Pourquoi les inventaires classiques (Excel, CMDB isolées, outils réseau, portails cloud) ne sont plus suffisants

La plupart des entreprises s'appuient déjà sur de multiples sources d'information : CMDB, outils de découverte, plateformes cloud et endpoint, solutions IAM et diverses briques de sécurité. Dans la pratique, le problème n'est presque jamais le manque d'information, mais le fait que ces données ne sont pas consolidées.

> Les inventaires traditionnels échouent généralement non pas parce que des données manquent, mais parce qu'ils manquent d'actualisation, de cohérence et de contexte de sécurité.

Cybersecurity Asset Management: Problème et contexte

Comme décrit dans la section 2.1, la gestion des actifs de cybersécurité se concentre sur une représentation cohérente et orientée risque des actifs pertinents pour la sécurité. Sur ce point, la plupart des approches traditionnelles restent en deçà de ce qu'elles promettent ; en particulier lorsque les mises à jour sont réalisées manuellement ou lorsque de nouveaux types d'actifs apparaissent en dehors des modèles de données historiques.

Les limites sont particulièrement visibles dans les approches centrées sur une CMDB. Dans des modèles de données statiques ou rigides, les actifs cloud natifs, éphémères, externes ou gérés par les unités métiers peuvent facilement rester invisibles.

Dans le même temps, la visibilité directe sur l'état des correctifs, les vulnérabilités, le niveau d'exposition, les identités, l'historique des incidents ou la criticité des données manque souvent. Les plateformes de sécurité ne fournissent elles aussi, le plus souvent, qu'une vision partielle des actifs et nécessitent donc une consolidation.

Un registre des actifs, **par exemple géré dans une plateforme de gestion de parc comme Timly**, offre une vue cohérente et directement exploitable pour la sécurité, la conformité et la gouvernance.

3.3 Les conséquences pour la sécurité et la conformité

Les hackers ciblent délibérément les systèmes qui ne sont pas surveillés, qui ont été oubliés ou qui sont insuffisamment sécurisés. Les cibles les plus fréquentes sont :

- Les systèmes obsolètes
- Les équipements réseau non recensés
- Les services cloud non documentés
- Les terminaux non gérés
- Les composants OT sans responsable clairement défini

Les conséquences les plus fréquentes :

Allongement des délais de réponse aux incidents

Lors d'un incident de sécurité, les organisations manquent souvent d'informations immédiates sur les systèmes concernés, leurs responsables et leurs dépendances.

Gestion des correctifs incomplète

Certains systèmes restent non corrigés parce qu'ils sont inconnus ou non rattachés clairement à une équipe responsable.

Surface d'attaque élargie

Les actifs inconnus ou non gérés augmentent directement la surface d'attaque.

Nombre élevé d'actifs inconnus

Les entreprises ne sont souvent pas en mesure de déterminer de manière fiable quels systèmes sont effectivement connectés à leurs réseaux.

Lacunes lors des audits et en matière de conformité

Les preuves relatives aux responsabilités, aux mesures de sécurité ou à la couverture doivent souvent être rassemblées manuellement.

Or, une visibilité insuffisante sur les actifs reste l'un des risques structurels les plus lourds dans les environnements IT et OT : elle **freine la détection des menaces, ralentit la réaction et fragilise la conformité**.

Crédit photo

Normes et exigences réglementaires autour du registre des actifs

Normes et exigences réglementaires autour du registre des actifs

Pour beaucoup d'entreprises, la conformité réglementaire sur la gestion des actifs n'est plus un sujet théorique, ni un problème pour plus tard. **La norme ISO 27001, la directive NIS2** et bien d'autres référentiels posent in fine la même exigence : savoir précisément quels actifs on détient, qui en a la charge, et dans quel état de sécurité ils se trouvent.

Le registre centralisé des actifs ne relève donc pas du confort organisationnel : c'est une obligation réglementaire. Ce chapitre précise ce qu'exigent concrètement les grands référentiels et montre où leurs exigences se rejoignent.

4.1 ISO/IEC 27001:2022 : l'inventaire des informations et des actifs

La norme ISO/IEC 27001 souligne que la sécurité de l'information ne peut être mise en œuvre efficacement sans une connaissance précise des actifs à protéger. L'Annexe A 5.9 exige notamment la tenue d'un **inventaire systématique des informations et des actifs associés**, ainsi que l'attribution de responsabilités clairement définies.

Dans ce contexte, un registre des actifs n'est pas un outil optionnel, mais une **condition fondamentale pour l'analyse des risques**, la mise en place des mesures de protection et la définition des responsabilités au sein d'un SMSI.

Au-delà de son existence, c'est la qualité de l'inventaire qui importe. L'annexe A 5.9 part du principe que les inventaires sont tenus de manière **cohérente, restent à jour et sont traçables sur l'ensemble du cycle de vie des actifs**. Dans les faits, cela signifie que le registre doit être correctement maintenu, contenir un socle minimal d'attributs, et être régulièrement rapproché des autres sources de référence.

Un registre des actifs conforme à la norme ISO doit permettre de répondre à ces questions :

- Quels sont les actifs inclus dans le scope du SMSI ?
- Qui est responsable de chaque actif ?
- Sur quelle base la criticité et les exigences de protection sont-elles déterminées et classifiées ?
- Comment les ajouts, modifications et retraits d'actifs sont-ils répercutés dans le registre correspondant ?
- Comment garantit-on que chaque actif recensé reste systématiquement relié aux risques, aux contrôles et aux éléments de preuve associés ?

Les questions d'audit de sécurité les plus courantes :

- Comment garantissez-vous l'exhaustivité et l'exactitude du registre ?
- Comment la responsabilité reste-t-elle clairement attribuée tout au long du cycle de vie d'un actif ?
- Quelles classes d'actifs sont incluses dans le scope du SMSI, et pour quelles raisons ?
- Comment les enregistrements d'actifs sont-ils reliés à la gestion des risques et aux activités de contrôle opérationnel ?

Normes et exigences réglementaires **autour du registre des actifs**

4.2 NIS2 : la gestion des actifs au cœur de la gestion des risques et des incidents

Les exigences réglementaires, notamment celles de la directive européenne NIS2, renforcent sensiblement les attentes en matière de transparence et de pilotage des risques. NIS2 ne prescrit aucun outil ni modèle d'inventaire spécifique, mais impose la mise en œuvre de « mesures techniques et organisationnelles appropriées » pour la gestion des cyberrisques.[3]

Concrètement, cela **nécessite une vision fiable des systèmes**, des services et des responsabilités associées. Sans une vision consolidée des actifs, la mise en conformité aux exigences clés reste partielle, en particulier dans les domaines suivants :

- L'évaluation des risques
- La réponse aux incidents
- La gestion des vulnérabilités
- La continuité d'activité
- Les obligations de reporting

La capacité à **identifier rapidement les systèmes concernés en situation d'urgence** est particulièrement importante. Les entreprises doivent être en mesure de déterminer :

- Quels actifs sont affectés
- Leur niveau de criticité
- Quels emplacements ou sites sont impliqués
- Quelles sont les dépendances entre les systèmes

Dans ce contexte, le CSAM conditionne la résilience réglementaire.

4.3 Normes complémentaires et exigences clients

En complément de l'ISO/IEC 27001:2022 et de la NIS2, de nombreuses autres normes et exigences clients reposent, de manière indirecte, sur une gestion des actifs de cybersécurité structurée dans un registre des actifs fiable. Notamment :

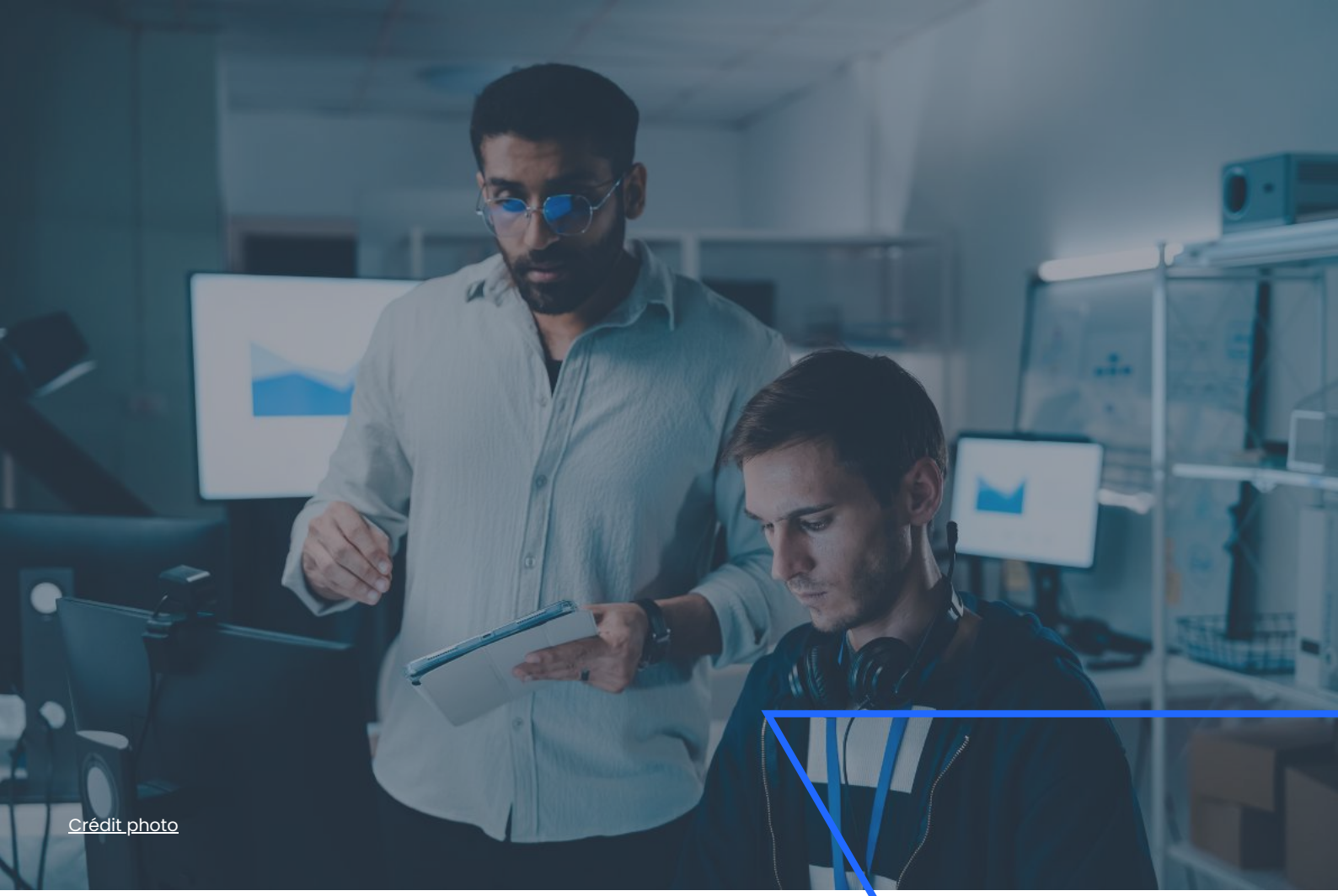
- Les exigences de l'ANSSI
- Les normes de sécurité propres à certains secteurs d'activité
- Les audits réalisés par les clients
- Les référentiels SOC 2 et TISAX
- Les exigences de gouvernance interne des entreprises

Même si ces exigences se présentent sous des formes différentes, la plupart des cadres de sécurité partagent la même prémisse.

Les entreprises doivent être capables d'identifier clairement les systèmes, les données et les points d'accès qu'elles détiennent et qu'elles doivent protéger. Un registre des actifs centralisé et à jour devient donc la fondation commune de la sécurité, de la conformité et du management opérationnel. Les entreprises opérant à l'international doivent également prendre en compte des exigences spécifiques à certains pays, telles que :

- Les exigences BSI/KRITIS en Allemagne
- Les réglementations NIS et dispositifs NCSC au Royaume-Uni
- Les exigences et dispositifs INCIBE en Espagne

Dans ce contexte, les entreprises ont besoin d'un modèle de Cybersecurity Asset Management évolutif et standardisé, capable de soutenir une gouvernance globale tout en intégrant les spécificités réglementaires locales.



Crédit photo

La feuille de route pour bâtir un registre des actifs orienté sécurité en 90 jours

La feuille de route pour bâtir un registre des actifs orienté sécurité en 90 jours

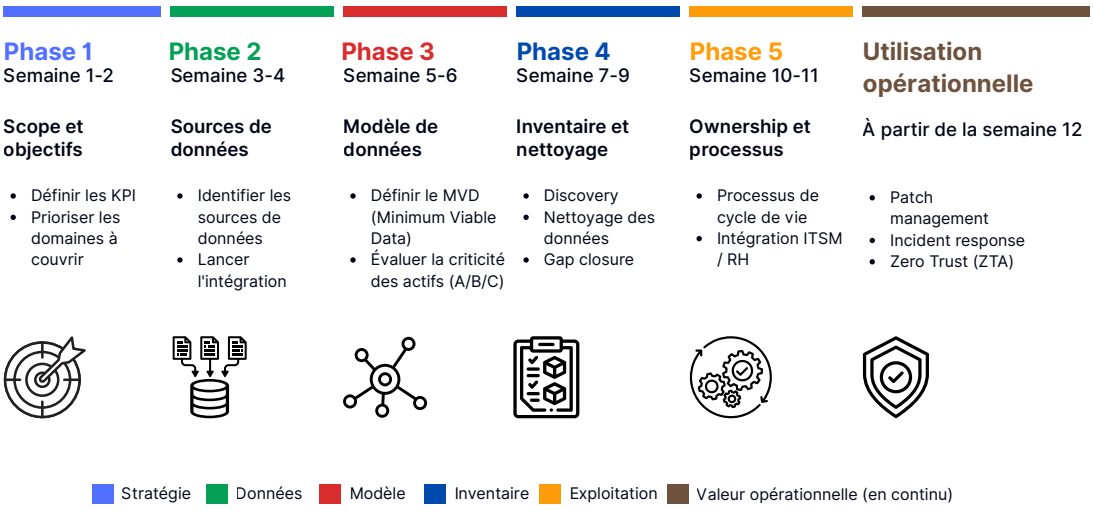
Dans les faits, un registre des actifs orienté sécurité ne se construit que rarement autour d'un seul outil. Ce qui importe surtout, c'est de définir précisément **quels sont les systèmes concernés, quelles sont les sources de données, qui en est responsable**, et comment ce registre est géré au quotidien.

Les actifs inconnus ou non maîtrisés figurent parmi les problèmes de sécurité les plus courants, comme le mettent en évidence Trend Micro et d'autres analyses. [4] Pour cette raison, la création d'un registre des actifs doit être envisagée comme une démarche de sécurité, bien plus qu'un simple inventaire informatique. Les objectifs prioritaires sont les suivants :

- Améliorer la visibilité sur les surfaces d'attaque
- Permettre une réponse aux incidents plus rapide
- Diminuer l'effort consacré aux audits

Cette feuille de route sur 90 jours offre un point de départ pragmatique. Onze semaines, cinq phases : délimiter le périmètre, raccorder les sources de données, bâtir un modèle de données, inventorier les actifs, installer les processus d'accompagnement. À partir de la semaine 12, le registre rejoint les activités de sécurité courantes. L'ambition n'est pas de tout documenter parfaitement dès le premier jour : c'est une **démarche fondée sur les risques**, qui traite en priorité les zones les plus sensibles.

Feuille de route pour bâtir un registre des actifs orienté sécurité en 90 jours



5.1 Phase 1 : Définir le scope et les objectifs (semaines 1 à 2)

Beaucoup de projets échouent avant d'avoir réellement commencé, parce qu'ils cherchent à établir d'emblée un inventaire exhaustif couvrant tous les systèmes, tous les sites et toutes les classes d'actifs. Dans la réalité, cela se traduit par des discussions longues et un niveau d'effort élevé avant d'obtenir des résultats réellement utilisables. Pour un **registre des actifs orienté sécurité, il est donc recommandé d'adopter dès le départ une approche basée sur les risques**.

Pendant les une à deux premières semaines, il convient de **définir un scope clair et des objectifs mesurables**. Il faut accorder la priorité aux systèmes et aux environnements qui sont les plus critiques pour la détection des menaces, la gestion des incidents, le patch management et le respect des exigences de conformité. L'illustration ci-dessous présente des domaines de démarrage typiques qui ont fait leurs preuves dans la pratique.

La feuille de route pour bâtir un registre des actifs orienté sécurité en 90 jours

Les priorités de l'inventaire des actifs

Systèmes informatiques critiques
Serveurs
Bases de données

Terminaux exposés
Appareils mobiles
Appareils sur sites distants

Comptes privilégiés
Administrateurs
Responsables systèmes

Composants réseau centraux
Routeurs
Switches

Systèmes OT proches de la production
Systèmes de pilotage
Capteurs

Services cloud
Données sensibles
Autorisations étendues

> *Au départ, l'exhaustivité ne prime pas : l'essentiel est de relier les informations. Une fiche indiquant le responsable, la localisation et le niveau de criticité suffit pour renforcer la sécurité dès les premiers jours.*
>
> L'ÉQUIPE DE CUSTOMER SUCCESS DE TIMLY

Dans des environnements distribués (par exemple dans la **construction, l'industrie manufacturière ou le facility management), il peut être judicieux d'intégrer dès le début les actifs mobiles ou répartis sur plusieurs lieux**. Ces environnements sont souvent marqués par un manque de visibilité et par des responsabilités floues.

En parallèle, les objectifs doivent être formulés de manière aussi concrète que possible. Des formulations générales telles que « plus de transparence » ne sont pas suffisantes. **Il est préférable de s'appuyer sur un nombre limité d'indicateurs permettant de mesurer les progrès et la valeur opérationnelle de manière objective**. Les KPI sont particulièrement intéressants lorsqu'ils mettent en évidence des faiblesses récurrentes liées à des inventaires incomplets :

- Des actifs inconnus
- Une absence d'attribution des responsabilités
- Un statut incertain des correctifs (patchs)
- Des temps de réaction longs lors des incidents de sécurité

Au départ, **un petit nombre de KPI** suffit pour faire ressortir les lacunes de visibilité et les progrès opérationnels. Ils doivent mesurer à la fois la qualité du registre des actifs et sa contribution réelle aux processus de sécurité.

KPI	Rôle	Objectif
Part des actifs inconnus	Met en évidence les angles morts et la surface potentielle d'attaque pour les hackers	< 5 %
Actifs avec un responsable attribué	Condition préalable pour les actions, l'escalade et les preuves d'audit	> 90 %
Transparence sur le statut des correctifs	Montre pour combien d'actifs le statut des correctifs est connu et fiable	> 95 %
Actifs critiques avec une classification à jour	Base pour la priorisation dans les processus de sécurité et d'audit	> 90 %
MTTR lors d'incidents de sécurité	Mesure la rapidité avec laquelle les actifs concernés sont identifiés et des mesures sont lancées.	< 4 h (incidents critiques)

Ces valeurs ne doivent pas être interprétées comme des seuils de conformité stricts. Elles sont surtout une **orientation pour les 90 premiers jours**. Leur valeur réelle réside dans la capacité à mettre rapidement au jour les principaux écarts et à déterminer si le registre des actifs apporte un bénéfice tangible aux opérations de sécurité.

Conseil pratique

Sans scope précisément défini, les entreprises obtiennent souvent un registre des actifs riche en informations, mais pauvre en valeur pratique. Une approche centrée sur les risques permet de traiter en priorité les écarts de visibilité et de sécurité les plus significatifs.

5.2 Phase 2 : Identifier et consolider les sources de données (semaines 3 à 4)

Une fois le scope de la gestion des actifs établi, la prochaine étape consiste à **connecter les sources de données prioritaires et à les intégrer dans une vue unifiée**. Cette phase est en général réalisée au cours des semaines 3 et 4.

La plupart des entreprises disposent déjà d'une quantité importante d'informations sur leurs actifs, mais celles-ci sont réparties entre différents systèmes : Active Directory, plateformes cloud, outils réseau, systèmes OT et inventaires locaux.

> *Le problème n'est généralement pas l'absence de données, mais l'impossibilité de les rassembler en une vue cohérente.*

Pour démarrer, il est suffisant de **connecter uniquement les sources de données qui apportent le plus de valeur** en matière de sécurité et de visibilité. Il s'agit en général de :

- Active Directory ou fournisseurs d'identité pour les utilisateurs et leurs droits
- Outils de découverte réseau pour les équipements actifs
- Plateformes cloud pour les ressources et services virtuels
- Registres des actifs ou inventaires existants

Ces sources fournissent déjà une part importante des informations pertinentes pour la sécurité et permettent d'identifier les actifs inconnus ou non gérés. La combinaison de méthodes de découverte automatisée, de collecte manuelle de données et de scans QR/barcode est abordée plus en détail dans la phase 4.

Exemple pratique avec Timly

Les solutions comme Timly permettent de combiner les données techniques issues des outils de découverte avec des processus d'inventaire mobiles, la lecture de QR codes/codes-barres et une gestion décentralisée des actifs. Cette approche est particulièrement adaptée aux environnements distribués, comme la construction, l'industrie manufacturière ou le facility management.

L'objectif de cette phase n'est pas de collecter chaque information possible, mais de construire une **vue centralisée et exploitable des actifs les plus importants**. Ce qui compte, ce n'est pas que toutes les données soient regroupées dans un seul système, mais que les informations issues de plusieurs sources puissent être consolidées de manière cohérente.

Conseil pratique

Les entreprises cherchent souvent à connecter un trop grand nombre d'interfaces dès le départ. Pour disposer d'une vue opérationnelle initiale, un ensemble restreint de sources essentielles (par exemple Active Directory, les outils de découverte réseau, les plateformes cloud et les inventaires existants) est souvent suffisant. D'autres sources peuvent ensuite être intégrées progressivement.

5.3 Phase 3 : Définir le modèle de données et les exigences minimales (semaines 5 à 6)

Une fois les principales sources de données consolidées, l'étape suivante consiste à déterminer **quelles informations sont réellement nécessaires pour chaque actif**. Cette phase devrait être achevée au cours des semaines 5 et 6. De nombreux inventaires deviennent inutilement complexes parce que trop de champs sont définis. Des champs qui, au final, ne sont pas tenus à jour dans les opérations quotidiennes.

Pour un registre des actifs orienté sécurité, un modèle de données minimal commun suffit au début. Seules les informations réellement pertinentes pour l'identification, la responsabilité, la priorisation et la gestion de la sécurité doivent être saisies.

Ce principe peut être décrit comme le « **Minimum Viable Data** » : autant d'informations que nécessaire, mais pas plus.

La feuille de route pour bâtir un registre des actifs orienté sécurité en 90 jours

Les données à faire figurer pour chaque actif

Champ	Rôle
ID d'actif ou identifiant unique	Crée une référence claire et évite les doublons
Type d'actif	Permet de distinguer par exemple IT, OT, logiciel, ressource cloud ou identité
Localisation ou contexte logique	Montre où l'actif est utilisé ou à quel scope il appartient
Personne responsable	Clarifie la responsabilité pour l'évaluation, les mesures et l'escalade
Criticité	Permet de prioriser selon le niveau de risque et l'impact sur l'activité
Statut de sécurité	Rend visible, par exemple, le niveau de patch, l'état des contrôles ou les alertes
Statut du cycle de vie	Montre si l'actif est opérationnel, a subi des réparations, est hors service...

Ces champs créent une base commune entre différents types d'actifs. En fonction du contexte, **des informations complémentaires peuvent être ajoutées ultérieurement** ; par exemple le fabricant, le numéro de série, la version du firmware, la classification des données ou les vulnérabilités associées.

Parmi les attributs minimaux clés figure également une **évaluation de la criticité**, permettant de prioriser les actifs de façon cohérente dans les processus de sécurité et d'audit. Pour la plupart des entreprises, un modèle pratique en trois niveaux suffit comme point de départ :

Un tel modèle de classification établit un référentiel partagé pour l'évaluation des risques, la priorisation des correctifs (patchs) et la réponse aux incidents.

La criticité ne se limite pas au type d'actif ; elle dépend aussi du rôle de l'actif dans les processus métier et de sécurité. Deux équipements techniquement similaires peuvent donc être classés différemment si l'un d'eux accède à des données sensibles ou supporte un processus métier critique.

Conseil pratique

Il vaut souvent mieux disposer de quelques champs essentiels, maintenus avec régularité, qu'un modèle de données complexe qui n'est pas géré correctement au quotidien.

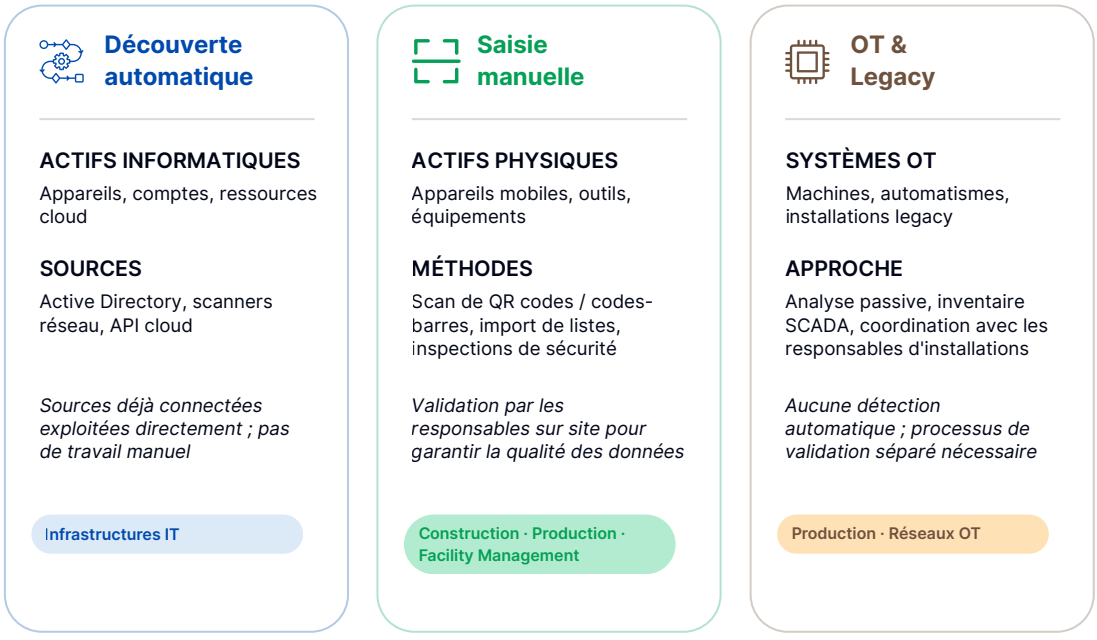
5.4 Phase 4 : Réaliser l'inventaire initial et le nettoyage des données (Semaines 7 à 9)

La phase 4 s'étend en général sur trois semaines (semaines 7 à 9) et constitue l'**étape la plus exigeante du projet** en termes de charge de travail.
Une fois les sources de données connectées et le modèle de données minimal défini, le véritable processus d'inventaire peut commencer.

Pendant cette phase, les **méthodes de collecte de données techniques et manuelles sont combinées**. Des outils comme **l'application de gestion d'inventaire Timly permettent de constituer rapidement un inventaire initial** exploitable.

L'illustration ci-dessous présente les méthodes de collecte de données typiques qui fonctionnent de manière complémentaire au cours de cette phase.

Méthodes de collecte en Phase 4



Une fois la collecte de données réalisée (via découverte automatique, inventaire manuel ou procédures OT spécifiques) il est indispensable de **nettoyer et harmoniser les informations.** Cela comprend notamment :

- L'identification et la suppression des doublons
- Le remplissage des champs obligatoires manquants (responsable, criticité, localisation)
- La correction des incohérences et la fermeture des principaux écarts de données

Le but n'est pas de disposer d'un registre des actifs exhaustif et parfait, mais d'une **base de référence fiable** qui peut déjà servir aux processus de sécurité et de conformité. Les lacunes restantes seront traitées par itérations, une fois que le registre sera intégré dans le fonctionnement quotidien de l'entreprise.

Conseil pratique

L'inventaire initial n'a pas besoin d'être parfait. Un registre couvrant environ 80 % des actifs, avec des données clés bien maintenues, est souvent plus utile que viser 100 % de complétude et retarder le projet de plusieurs mois.

5.5 Phase 5 : Définir les responsables et les processus (semaines 10 à 11)

La phase 5, sur les semaines 10 et 11, vise à clarifier qui est responsable de quoi et à formaliser les processus standards.

Un registre des actifs ne crée une réelle valeur que si les règles définissant clairement **qui est responsable d'un actif et à quel moment les informations doivent être mises à jour** sont clairement établies. Sans responsabilités formalisées, même les registres bien tenus deviennent rapidement incomplets ou obsolètes. C'est pourquoi cette phase ne doit pas seulement définir les responsables, mais également structurer les principaux processus liés au cycle de vie des actifs.

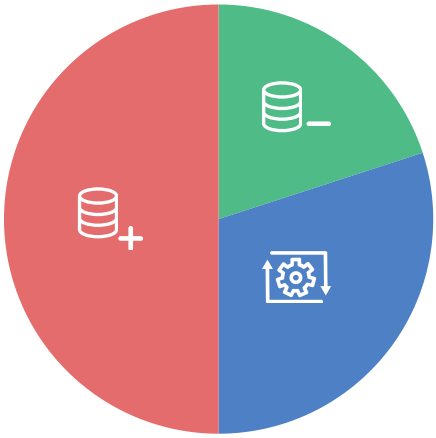
Les trois situations clés :

1. **Onboarding**
2. **Modifications**
3. **Mise hors service**

À chacune de ces étapes, le registre des actifs doit être tenu à jour ; de la création initiale de l'actif jusqu'à ses modifications et sa mise au rebut finale. La maintenance des actifs doit être intégrée le plus étroitement possible aux processus existants d'ITSM, d'achats et de RH, afin que les mises à jour se fassent naturellement tout au long du cycle de vie des actifs.

Le schéma ci-après illustre ces trois moments clés du processus.

Cycle de vie des actifs : les trois moments clés du processus



- **Onboarding**
  Enregistrer l'actif, le taguer, attribuer un responsable, renseigner la criticité.
- **Modifications**
  Actualiser la localisation, l'usage, les responsables et le statut dans le registre des actifs.
- **Mise hors service**
  Retirer l'actif, supprimer les données, documenter les preuves, clôturer l'enregistrement dans le registre.

Exemple pratique avec Timly

Pour garantir la fiabilité des données des actifs sur le long terme, les processus de maintenance doivent s'intégrer étroitement aux workflows existants. Des solutions mobiles comme Timly s'avèrent particulièrement adaptées pour accompagner les équipes décentralisées, les opérations de maintenance et la gestion d'actifs multi-sites.

On observe généralement trois freins récurrents : des responsabilités mal réparties, une mise à jour des données jugée peu prioritaire, et un manque de visibilité sur les gains opérationnels qu'elle génère. Il convient donc de définir précisément, pour chaque événement, la nature de la mise à jour à effectuer et son responsable. **Des responsabilités clairement définies et des processus de mise à jour garantissent la qualité des données.**

Conseil pratique

Pour que la prise de responsabilité fonctionne vraiment, la maintenance des actifs doit s'intégrer aux processus opérationnels déjà en place. C'est notamment le cas lorsqu'elle s'articule avec les workflows d'ITSM, d'achats et de RH.

5.6 Valeur opérationnelle : cas d'usage en matière de sécurité (à partir de la semaine 12)

Après la phase de mise en œuvre (phases 1 à 5, semaines 1 à 11), le registre des actifs entre en usage opérationnel continu à partir de la semaine 12.

C'est au quotidien, dans les opérations de sécurité, qu'un registre centralisé des actifs prend toute sa valeur. Des processus tels que la gestion des correctifs, la réponse aux incidents et le contrôle des accès ne peuvent fonctionner efficacement que si des **informations fiables et à jour sur les actifs concernés** sont disponibles.

Sans cette base, les équipes de sécurité doivent, en cas d'incident, rassembler manuellement les informations provenant de différents systèmes et listes. Un registre géré de manière centralisée permet d'**identifier plus rapidement les systèmes concernés, de les hiérarchiser et de les traiter de manière traçable**.

Les trois cas d'usage suivants illustrent de manière concrète la valeur opérationnelle d'un registre des actifs centralisé.

Gestion des correctifs (Patch Management)

Lorsqu'une vulnérabilité critique est révélée, les entreprises dépourvues de registre des actifs centralisé doivent d'abord trouver des réponses de base : quels systèmes sont touchés, quelles versions sont installées à quel endroit et qui en est le responsable ? Les informations nécessaires se trouvent généralement éclatées entre différents outils, inventaires et équipes.

Avec un registre des actifs centralisé, il devient **possible de filtrer et prioriser immédiatement les systèmes concernés**, par exemple selon la version du logiciel, le site, la criticité métier ou le responsable. On sait alors immédiatement quels systèmes traiter en premier et à qui incombe la remédiation, tandis que le statut des correctifs et la progression des actions restent transparents et facilement auditables.

Réponse aux incidents

Lors d'un incident de sécurité (par exemple une connexion suspecte ou une alerte malware) il est souvent difficile, dans un premier temps, de savoir quels systèmes sont concernés et quelle est la gravité de la situation. Sans source centralisée de données sur les actifs, les équipes de sécurité doivent fréquemment mener des investigations manuelles dans plusieurs systèmes.

La feuille de route pour bâtir un registre des actifs orienté sécurité en 90 jours

Avec un registre des actifs, **le contexte nécessaire est immédiatement disponible** : système concerné, responsable, emplacement, criticité et dépendances potentielles. Cela permet de lancer plus rapidement les premières mesures de confinement et de gérer les circuits d'escalade de manière plus efficace.

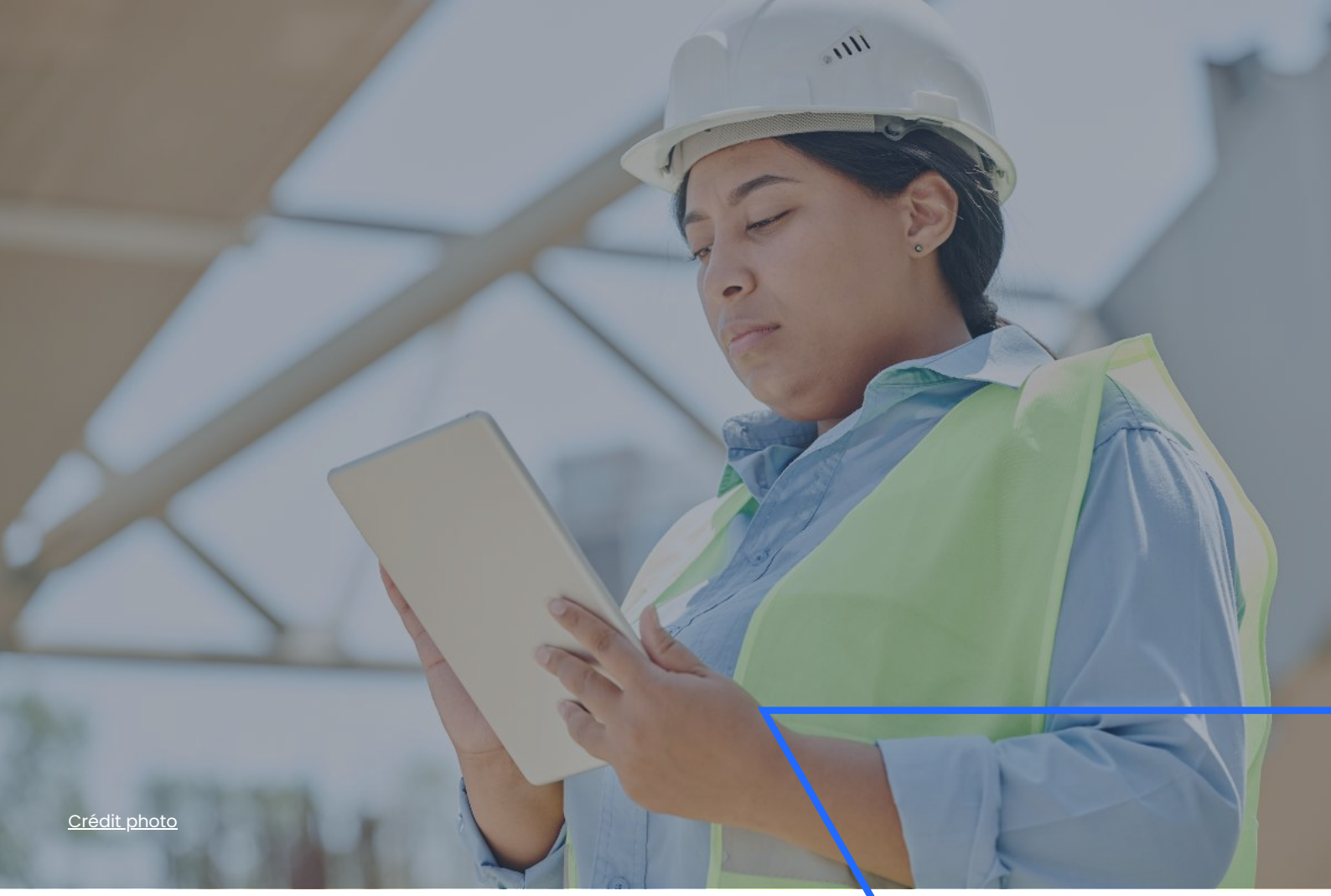
Contrôle des accès & Zero Trust

Dans de nombreux environnements, les décisions d'accès reposent encore sur des hypothèses simples, comme l'appartenance au réseau ou la connexion via VPN. Le contexte autour du système qui demande l'accès est souvent insuffisamment connu.

Un registre des actifs fournit la base nécessaire aux décisions fondées sur le contexte, en apportant des informations comme le **type d'appareil, l'emplacement, la criticité, l'état des correctifs et le responsable**. Cela permet de mettre en place des contrôles d'accès plus granulaires, incluant des restrictions pour les systèmes inconnus ou non conformes.

Conseil pratique

La valeur opérationnelle d'un registre des actifs ne se juge pas au nombre d'entrées qu'il contient, mais à la rapidité et à la fiabilité des décisions qu'il permet de prendre. L'important est que le contexte pertinent soit immédiatement à disposition lors des incidents, des opérations de patch management et des décisions de contrôle d'accès.



Crédit photo

Illustrations concrètes dans la construction, le facility management, l'industrie et l'IT

Illustrations concrètes dans la construction, le facility management, l'industrie et l'IT

Les chapitres précédents ont détaillé, étape par étape, la mise en place d'un registre des actifs conforme aux exigences de la sécurité de l'information. Les exemples qui suivent en montrent la valeur opérationnelle au quotidien pour les divers secteurs concernés.

6.1 Entreprise opérant dans la construction et le facility management

Entreprise opérant dans la construction et le facility management - 400 employés, 30 sites

Actifs mobiles, gestion décentralisée via Excel et e-mails

SITUATION INITIALE

Les responsabilités étaient floues, les sites difficiles à tracer et les audits présentaient régulièrement des lacunes. Plusieurs milliers d'actifs mobiles (outils, appareils de test, équipements informatiques) étaient gérés dans des listes décentralisées, sans visibilité fiable sur leur état ni leur localisation.

MESURES MISES EN PLACE

- Enregistrement des actifs via QR code directement sur le terrain
- Attribution centralisée d'un responsable pour chaque actif
- Intégration avec la gestion des identités et le système de ticketing
- Modèle de criticité A / B / C pour prioriser les interventions de maintenance

RÉSULTATS

Actifs non attribués

~18 % → < 3 %

Temps de réponse aux incidents

Plusieurs jours → < 4h

Préparation aux audits

Complète pour la première fois

Les preuves de contrôle et de responsabilité sont générées directement par le système

« Le moment décisif n'est généralement pas le déploiement lui-même, mais l'inventaire complet. C'est à ce moment-là que l'on voit (très vite) où les responsabilités ne sont pas clairement définies. »

L'équipe de Customer Success de Timly

6.2 Entreprise industrielle spécialisée dans l'OT

Entreprise industrielle spécialisée dans l'OT, basée sur plusieurs sites

Environnements OT complexes, listes d'inventaire parallèles, versions de firmware inconnues

SITUATION INITIALE

Il n'existait aucune vue consolidée sur les installations véritablement critiques, rendant les décisions difficiles lors d'incidents ou d'interruptions. Les inventaires parallèles étaient obsolètes et incohérents, avec des versions de firmware parfois totalement inconnues.

MESURES MISES EN PLACE

- Scope volontairement restreint aux installations critiques de production dans un premier temps
- Utilisation de la découverte réseau comme socle technique obligatoire
- Complément manuel des données OT (version de firmware, fabricant, secteur)
- Définition du responsable et de la criticité A / B / C, avec connexion vers le logiciel de maintenance

RÉSULTATS

Actifs critiques pour la production

> 90 % ont été inventoriés

Versions de firmware inconnues

Niveau élevé → < 5 %

Analyse des vulnérabilités

Désormais priorisable

Les systèmes concernés sont identifiés rapidement et classés selon leur criticité

« Dans les environnements OT, le véritable problème est rarement la technique elle-même, mais l'absence d'une vision commune sur les systèmes réellement critiques. »

L'équipe de déploiement de Timly

Illustrations concrètes dans la construction, le facility management, l'industrie et l'IT

6.3 Prestataire IT / Managed Service Provider

Prestataire IT / Managed Service Provider, 50 clients

Environnements IT hétérogènes, actifs répartis entre système de ticketing, outils de monitoring et fichiers Excel

SITUATION INITIALE

Lorsqu'un incident survenait, il n'existait pas de vue globale et structurée sur les clients, les systèmes concernés et les responsables. Les actifs étaient répartis dans plusieurs outils, et chaque rapport client nécessitait des consolidations manuelles.

MESURES MISES EN PLACE

- Registre central pour les actifs internes et ceux liés aux clients
- Attribution systématique à un client et à un responsable interne pour chaque actif
- Synchronisation automatique via outils RMM et API cloud
- Rapports clients standardisés générés automatiquement à partir du registre

RÉSULTATS

Actifs inventoriés de manière cohérente

> 95 % avec responsable et référence client

Détection des incidents

Plusieurs heures → **Quelques minutes**

Reporting

Totalement automatisé

Les rapports pour les clients ne nécessitent plus de traitement manuel

« La plus grande différence ne vient pas d'un plus grand volume de données, mais du temps gagné lorsqu'il faut retrouver une information en situation d'urgence. »

L'équipe de Customer Success de Timly

Ce qu'il faut retenir

Un constat revient dans tous les cas étudiés : ce n'est pas l'exhaustivité qui crée le plus de valeur, mais la mise en place rapide d'une structure opérationnelle, avec des responsabilités clairement établies et des données de base consolidées. Une fois cette fondation posée, la sécurité opérationnelle et l'efficacité quotidienne progressent nettement.

Crédit photo

Intégration organisationnelle et gestion du changement

Intégration organisationnelle et gestion du changement

Un registre des actifs ne crée pas de valeur simplement parce qu'un outil est déployé. Son efficacité repose avant tout sur son **intégration dans les structures de responsabilité existantes et dans les processus opérationnels**.

Cette intégration permet de transformer le registre d'une simple base de données en un référentiel opérationnel utilisé par la sécurité, les opérations IT et la conformité.

7.1 Gouvernance et modèle opérationnel

La **responsabilité stratégique du registre des actifs relève généralement de la direction informatique ou du RSSI**. Ce rôle définit le scope, le modèle de données minimal, le cadre de criticité ainsi que les liens avec les exigences de gestion des risques et de conformité.

La responsabilité principale à ce niveau ne consiste pas en la maintenance quotidienne, mais dans la définition des règles selon lesquelles les actifs sont classifiés et gérés à l'échelle de l'entreprise.

La responsabilité opérationnelle appartient à ceux qui provoquent les changements :

- Les équipes IT
- Les équipes OT
- Les structures organisationnelles
- Les unités de services techniques

Ces équipes doivent s'assurer que **chaque événement lié aux actifs est immédiatement enregistré dans le système** : déploiement, déplacement, maintenance ou mise hors service.

En réalité, les incohérences proviennent rarement d'un manque de responsabilité, mais plutôt de déclencheurs mal définis. Qui enregistre un changement lorsqu'un appareil est déplacé temporairement ? Qui met à jour le registre lorsqu'une intervention est réalisée par un prestataire externe ? **Un modèle de gouvernance efficace distingue donc à la fois les niveaux organisationnels et les types de responsabilité**. L'illustration suivante présente les trois principales couches de responsabilité d'un registre des actifs.

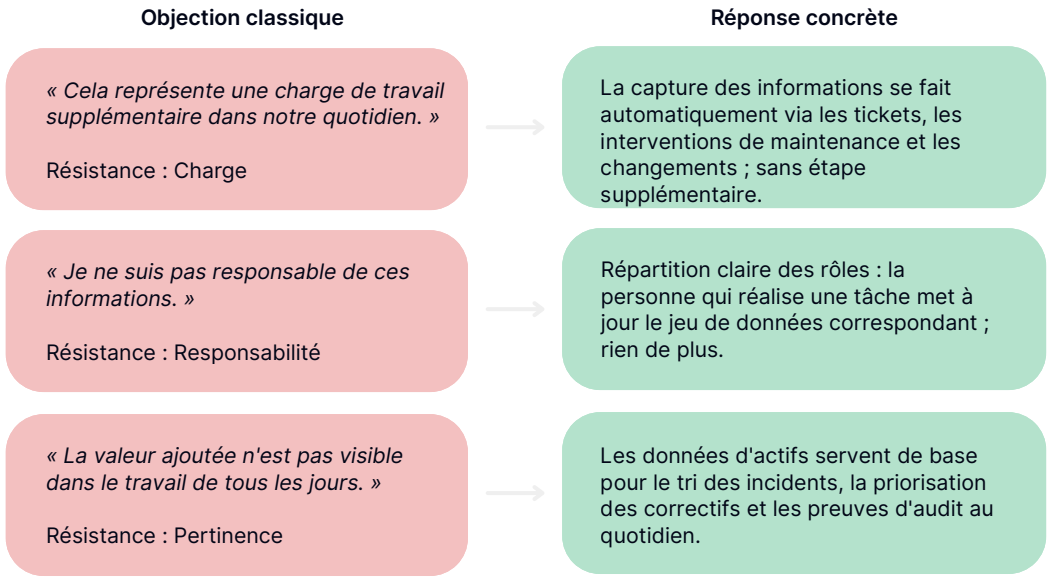
Les niveaux de responsabilité dans le registre des actifs

7.2 Accompagnement et adoption au quotidien

La mise en œuvre d'un registre des actifs échoue rarement pour des raisons techniques. Elle échoue beaucoup plus souvent parce qu'elle **alourdit le travail quotidien des équipes**. Les équipes opérationnelles formulent souvent des objections de ce type :

- « Nous avons déjà assez de travail comme ça. »
- « Ces informations ne relèvent pas de ma responsabilité. »
- « Je ne vois aucun bénéfice concret pour mon équipe. »

L'adoption se produit principalement lorsque les données relatives aux actifs peuvent être maintenues directement dans les flux de travail opérationnels. L'illustration ci-dessous montre **trois objections courantes ainsi que des approches pratiques pour y répondre**.



Le modèle n'apporte de la valeur que lorsque la collecte et la maintenance des données sont intégrées aux processus déjà en place.

En pratique, les informations clés sur les actifs devraient idéalement être générées directement dans les activités opérationnelles courantes ; par exemple lors du traitement des tickets, des interventions de maintenance, des demandes de changement ou des achats.

Les approches les plus performantes sont celles qui réduisent l'effort pour les équipes :

- La **capture mobile de données via scan de QR codes et codes-barres** simplifie les activités d'inventaire et de maintenance au quotidien.
- Un **nombre restreint d'attributs obligatoires** réduit les obstacles à l'utilisation et améliore la qualité des données.
- L'**intégration des informations sur les actifs dans le contexte opérationnel** facilite la prise de décisions concrètes, notamment pour le traitement des incidents, la priorisation des correctifs ou la préparation des audits.

> *« L'adoption ne repose pas sur la formation, mais sur la simplicité. Lorsque les équipes peuvent enregistrer un actif en dix secondes à l'aide d'un code QR et voir immédiatement le résultat apparaître dans un ticket ou un planning de maintenance, la mise à jour des données devient un réflexe plutôt qu'une tâche supplémentaire. »*
>
> L'ÉQUIPE DE CUSTOMER SUCCESS DE TIMLY

Intégration organisationnelle et gestion du changement

7.3 Intégration avec les systèmes de gestion existants

Un registre des actifs crée le plus de valeur lorsqu'il est utilisé comme la référence centrale entre les systèmes opérationnels, de sécurité et de conformité déjà utilisés par l'entreprise.

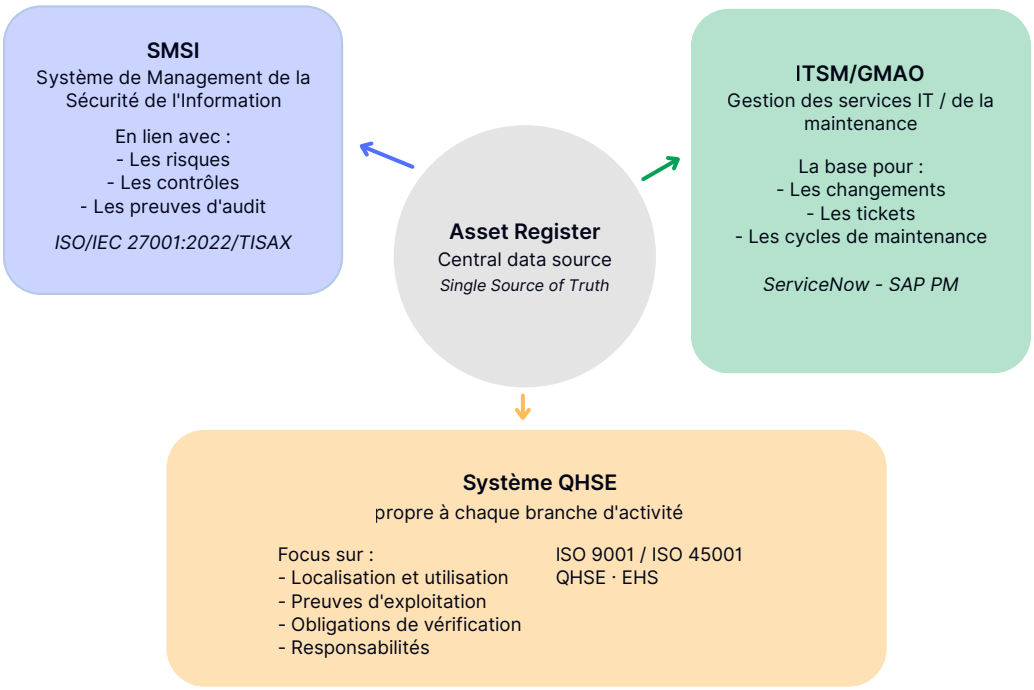
Cette centralisation repose sur des intégrations avec trois types de systèmes :

SMSI relie les actifs aux risques, aux mesures de sécurité et aux preuves d'audit.

ITSM/GMAO
s'appuie sur le registre des actifs comme base pour les demandes de changement, les tickets et les cycles de maintenance.

Systèmes Qualité et HSE
selon le secteur d'activité, ces systèmes garantissent la traçabilité de la localisation, de l'utilisation et des responsabilités.

Comme le montre le schéma ci-dessous, le registre des actifs constitue la **source de données commune à l'ensemble de ces systèmes**.



Il est essentiel d'établir une **attribution claire des systèmes de référence pour chaque catégorie de données**. En l'absence de cette attribution, des incohérences apparaissent rapidement entre les données issues des outils ITSM, du logiciel GMAO et du registre des actifs. Tout l'enjeu repose sur la définition de rôles clairement établis ainsi que sur une articulation explicite entre les systèmes : le registre des actifs constitue la référence centrale, tandis que les systèmes opérationnels alimentent les modifications et les événements du cycle de vie.

Les facteurs de réussite organisationnelle lors du déploiement :

- Des responsabilités de propriété clairement établies tout au long du cycle de vie des actifs, depuis leur intégration jusqu'à leur mise hors service.
- Une articulation cohérente avec les processus d'onboarding, de gestion des changements et de mise hors service.
- Des barrières à l'adoption réduites, grâce à un nombre limité d'attributs obligatoires dans le registre des actifs.
- Des bénéfices opérationnels visibles dès les premières semaines, notamment des audits plus rapides et une baisse des sollicitations internes.

Crédit photo

Principales conclusions et recommandations pour les décideurs

Principales conclusions et recommandations pour les décideurs

Les principales conclusions et recommandations ci-dessous synthétisent les enseignements majeurs de ce livre blanc et indiquent les actions que les entreprises devraient mettre en priorité en œuvre pour bâtir une gestion des actifs de cybersécurité efficace et pérenne.

8.1 Les cinq messages clés

Un bon registre des actifs, rigoureux et structuré, constitue la base opérationnelle des démarches de cybersécurité et de conformité. **Les conclusions suivantes résument les messages clés de ce livre blanc :**

1. Sans **données d'actifs cohérentes et à jour**, la gestion des cyberrisques reste nécessairement incomplète. Les systèmes et appareils mal identifiés ou mal suivis comptent en effet parmi les principales causes de vulnérabilités, de retards dans le traitement des incidents et de failles dans le déploiement des correctifs.
2. **Des réglementations comme NIS2 ou ISO/IEC 27001:2022** imposent désormais une traçabilité des actifs, des responsables clairement désignés et des preuves vérifiables. Or, de simples listes d'inventaire déconnectées des processus métier ne répondent plus aux exigences d'environnements IT et OT en perpétuelle évolution.
3. C'est dans le **quotidien opérationnel** que ce registre révèle sa valeur : centralisé, il améliore directement la réponse aux incidents, la gestion des correctifs, la préparation des audits (et leur bon déroulement) ainsi que le reporting de sécurité.
4. Le succès du CSAM repose ainsi moins sur les outils que sur une **combinaison de gouvernance, de processus intégrés et de gestion continue des données**.
5. Sur le terrain, ce sont les **approches pragmatiques** qui portent leurs fruits : cibler quelques classes d'actifs prioritaires, se concentrer sur un nombre restreint de processus essentiels, et viser des résultats concrets dès les premiers mois.

8.2 Recommandations pratiques pour les 12 prochains mois

Construire un registre des actifs à la hauteur des enjeux de sécurité de l'information ne se résume pas à un projet informatique parmi d'autres. C'est le point de départ d'une bascule progressive vers un fonctionnement pensé autour de la sécurité. **Ce plan d'action synthétique liste les actions qui, dans la pratique, ont porté leurs fruits**.

Premiers résultats (0 à 3 mois)
(phases 1 à 3 de la feuille de route à 90 jours)

- Cadrer le scope et identifier les classes d'actifs critiques
- Regrouper et fiabiliser les principales sources de données
- Fixer un socle minimal de données et clarifier qui est responsable de quoi
- Lancer les premiers indicateurs de sécurité

Consolidation opérationnelle (3 à 6 mois)
(phases 4 et 5 de la feuille de route à 90 jours)

- Relier le registre des actifs aux processus de gestion des correctifs et de réponse aux incidents
- Désigner un responsable clair à chaque étape du cycle de vie des actifs
- Fiabiliser la qualité des données et les processus de mise à jour

Développement stratégique (6 à 12 mois)
(Extension au-delà de la feuille de route initiale)

- Intégrer pleinement le registre des actifs au SMSI
- Automatiser les rapports d'audit et de conformité
- Faire passer à l'échelle le Zero Trust et la prise de décision fondée sur le risque
- Faire évoluer en continu le modèle de maturité et le cadre de gouvernance

Conseil pratique

Mieux vaut ne pas chercher à construire d'emblée un inventaire exhaustif à l'échelle de l'entreprise. Les approches itératives (qui priorisent quelques classes d'actifs clés et s'appuient sur les processus essentiels) donnent, dans les faits, de bien meilleurs résultats.

8.3 Perspectives

Le Cybersecurity Asset Management se transforme progressivement : d'une initiative centrée sur l'inventaire des actifs, il devient un **élément central pour piloter la sécurité, la conformité et la résilience opérationnelle**.

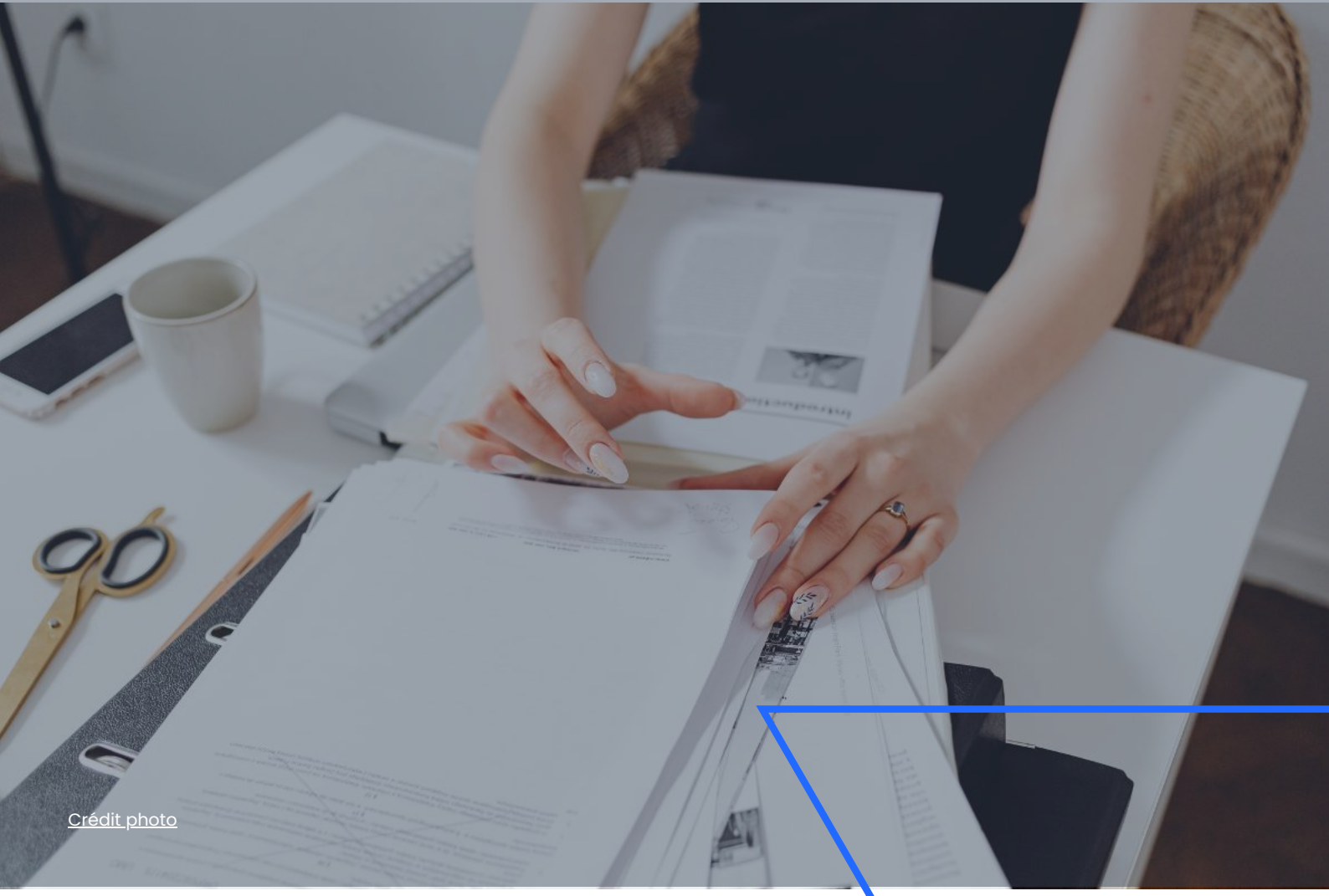
Les réglementations se durcissent (NIS2, ISO/IEC 27001:2022, les exigences de l'ANSSI, ainsi que les référentiels propres à chaque secteur), et les entreprises doivent désormais prouver qu'elles ont une vue d'ensemble sur leurs actifs sensibles. Dans le même temps, les environnements hybrides IT/OT, le cloud, le travail mobile et les accès externes ne cessent de gagner du terrain.

Un registre des actifs fiable est désormais incontournable pour :

- Gérer les risques et la conformité
- Bâtir des architectures Zero Trust
- Automatiser la gestion des vulnérabilités
- Répondre aux incidents et gagner en résilience
- Préparer les audits et gérer les preuves
- Intégrer les processus opérationnels et de maintenance

Sur le long terme, les stratégies de gestion des actifs de cybersécurité tendent vers des **modèles opérationnels intégrés**, capables de connecter les processus de sécurité, IT, OT, maintenance, conformité et ESG dans une seule et même structure unifiée.

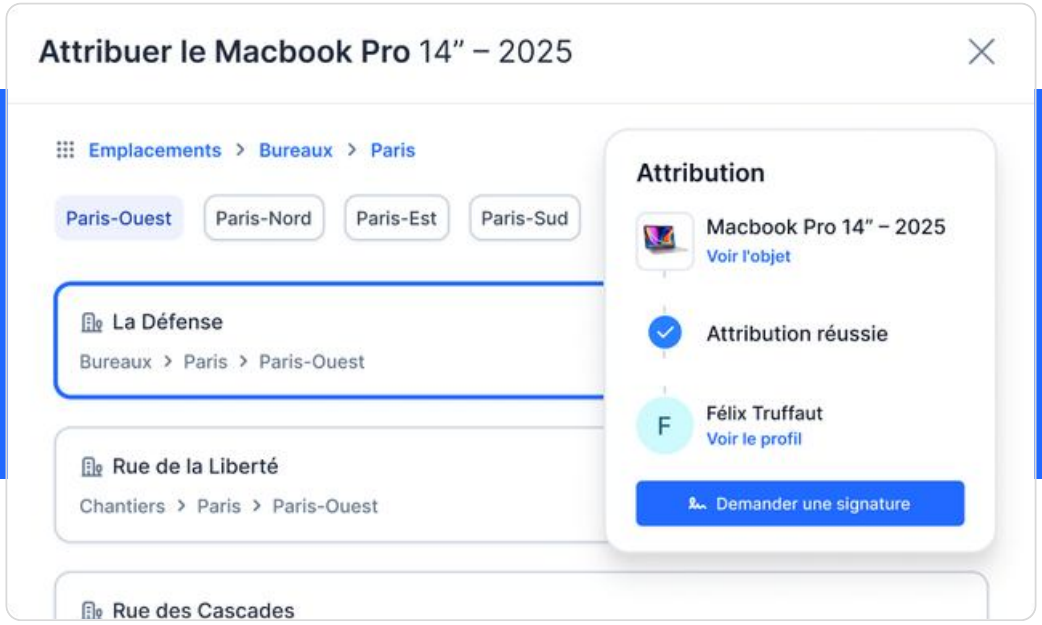
Crédit photo



Crédit photo

Présentation de Timly et de la méthodologie

Timly



Présentation de Timly et de la méthodologie

Avec Timly, les entreprises gèrent leurs actifs physiques, leurs équipements opérationnels et leurs ressources de sécurité depuis un point unique, en toute transparence et directement sur le terrain. Sa plateforme est particulièrement utilisée dans des **secteurs où les actifs sont nombreux, répartis et en mouvement**, comme la construction, le facility management, l'industrie manufacturière et l'IT.

Le cœur de l'approche consiste à relier la visibilité sur les actifs, les processus du quotidien et les exigences de sécurité. Cela inclut :

- La gestion centralisée des actifs physiques et des équipements opérationnels
- La collecte de données sur le terrain, via smartphone ou tablette
- La gestion de parc matériel par QR codes et codes-barres (scanner intégré)
- La prise en charge de sites multiples et d'équipes mobiles
- L'intégration des actifs OT et des équipements techniques
- La gestion du cycle de vie et de la maintenance
- L'attribution des responsabilités selon les rôles

Grâce à cette combinaison de simplicité de saisie, d'usage mobile et de données centralisées, Timly aide les entreprises à **réduire les lacunes en matière de transparence et rendre les données sur les actifs exploitables sur le plan opérationnel** dans les environnements IT/OT, ainsi que pour la sécurité, les audits et la conformité.

Pour voir concrètement ce que cette visibilité sur les actifs change dans des environnements IT et OT dispersés, réservez une démonstration produit gratuite.

RÉSERVER UNE DÉMO

9.1 Méthodologie

Ce livre blanc s'appuie sur plusieurs types de sources et d'expériences :

- Études et analyses de marché publiques
- Exigences réglementaires et normatives
- Projets menés auprès de clients
- Ateliers, déploiements et retours d'utilisateurs
- Observations de terrain dans des secteurs aux structures d'actifs dispersées

Il s'appuie notamment sur les enseignements et exigences issus de :

- La norme ISO/IEC 27001:2022 / Annexe A
- La directive NIS2
- Publications de Verizon, IBM et d'autres acteurs de la recherche en cybersécurité
- Projets menés dans l'IT, l'OT et le facility management

Les niveaux de maturité présentés, les exemples de KPI et les recommandations pratiques sont à considérer comme une cible pragmatique et non comme un modèle de conformité rigide. Ce livre blanc propose une **initiation pratique à la mise en place d'un registre des actifs adapté à la sécurité de l'information**, en mettant l'accent sur la réduction des risques, la faisabilité opérationnelle et une transparence conforme aux exigences d'audit.

9.2 Sources

[1] https://www.verizon.com/business/resources/infographics/2025-dbir-infographic.pdf
[2] https://www.ibm.com/reports/data-breach
[3] https://eur-lex.europa.eu/eli/dir/2022/2555/oj
[4] https://www.trendmicro.com/explore/aichangingcyberrisk