OVERVIEW by OVERSOC Pour le CESIN

Cybersecurity
Asset Attack Surface Management – CAASM

Rapport 2024

Les besoins et les attentes des organisations françaises vis-à-vis des outils de Cybersecurity Asset Attack Surface Management

Une étude menée auprès des membres du CESIN

L'ÉDITO

Alain Bouillé
Directeur Général du CESIN

Après le succès du premier livre blanc en 2023, le CESIN et OverSOC ont souhaité approfondir leur collaboration pour une nouvelle étude sur le Cybersecurity Asset Attack Surface Management (CAASM). Ce second livre blanc s'inscrit dans la continuité de nos efforts pour accompagner les professionnels de la cybersécurité face aux défis de l'évolution numérique.

Le CAASM, en tant que pilier émergent de la gestion des risques, suscite aujourd'hui un intérêt croissant dans notre écosystème.

Les récentes avancées du secteur en témoignent : en 2024, la valorisation d'Axonius, spécialiste de la gestion des actifs cyber, a atteint 2,6 milliards de dollars, tandis que Rapid7 a acquis Noetic Cyber, un acteur clé de cette discipline, pour offrir une visibilité accrue de la surface d'attaque à ses clients.

Ces mouvements montrent combien la gestion de la surface d'attaque est devenue un enjeu central, où l'identification et la protection des actifs numériques sont des priorités critiques.

Gartner identifie d'ailleurs le CAASM comme un domaine stratégique, indispensable pour une posture de sécurité renforcée et résiliente. Ce livre blanc vise à donner aux entreprises une feuille de route pratique et structurée pour appréhender cet enjeu.

À l'heure de la complexification des systèmes d'information, les solutions de CAASM permettent non seulement une meilleure visibilité sur les actifs numériques, mais également une gestion proactive des menaces. Au-delà de la technique, cette approche permet d'allouer les ressources de manière optimale et de favoriser la collaboration entre les différentes parties prenantes du SI.

Nous espérons que ce livre blanc contribuera à sensibiliser et à accompagner les organisations vers une gestion proactive de leurs surfaces d'attaque, tout en renforçant leur résilience face aux menaces numériques croissantes.

TABLE DES MATIÈRES

1 Introduction 5

2 Le CAASM : l'inventaire consolidé au service de la cyber 6

3 Data Collection : Au coeur du CAASM, la donnée consolidée existante 10

4 Data Unification : Enrichir la donnée et segmenter l'information pour rendre la vision pertinente 12

5 Data Exploitation : Pourquoi et comment utiliser un outil de CAASM au quotidien ? 14

6 Conclusion 17

7 Annexe 18

RÉSUMÉ

Cette étude a été menée sur 4 semaines entre septembre et octobre 2024 en interrogeant les membres du CESIN sur leur maturité vis-à-vis du sujet CAASM pour dresser l'état des lieux 2024 et le comparer avec celui de 2023. 78 personnes ont répondu.

Résultats clés de l'étude

Le manque de ressources humaines (77,5%), la méconnaissance de l'ensemble de la surface d'attaque (66,7%) et le manque de budget (50,7%) sont cités comme les trois freins principaux à la gestion de la surface d'attaque.

73,9% des répondants ne disposent pas d'outils leur permettant de réconcilier l'ensemble des sources IT et cyber présentes dans leurs SI.

Le manque de centralisation des informations, la connaissance partielle du SI et l'absence d'inventaire consolidé en général sont citées comme des raisons pour lesquelles le niveau de criticité n'est pas connu.

95.2% des répondants pensent que la mise en place d'un référentiel commun à l'ensemble des équipes IT et cyber est nécessaire, afin de fluidifier les interactions entre les équipes.

Les principales fonctionnalités du CAASM

Consolider des données techniques et métier
Pour permettre aux équipes opérationnelles de prioriser leurs actions de remédiation en fonction du contexte de leur organisation

Fédérer l'ensemble des sources de données d'un SI
Pour en exploiter pleinement toutes les données

Favoriser la coordination des équipes IT et cyber
Grâce à un référentiel commun, l'outil de CAASM

Donner le bon niveau d'information à la bonne personne
Pour prioriser les actions, favoriser la collaboration, suivre les différents projets dans le temps, et éviter les zones de non-responsabilité

Réduire le temps perdu à chercher la donnée entre plusieurs consoles
Pour l'exploiter pleinement et se focaliser sur la remédiation.

Faire ressortir la donnée utile
Mettre en avant des KPIs pertinents pour votre organisation, et créer des dashboards personnalisés en fonction des indicateurs que vous cherchez à suivre

Garantir une compatibilité agnostique
En n'étant pas impacté par l'ajout ou le changement de nouvelles sources de données

Mettre à jour l'ensemble des outils déployés sur le parc

INTRODUCTION

Le paysage cyber en 2024

Le paysage de la cybersécurité est en pleine mutation, porté par des transformations technologiques rapides et des menaces toujours plus sophistiquées.

Voici **les 5 tendances majeures qui ont redéfini ce contexte en 2024**.

1 Les outils IT et cyber se multiplient dans les entreprises

La prolifération des outils IT et cyber ajoute une couche supplémentaire de complexité dans la gestion des systèmes d'information (SI).

Bien que ces solutions soient essentielles, elles silotent l'information et compliquent l'agrégation des données, ce qui nuit à la capacité des équipes à obtenir une vue unifiée de leur surface d'attaque.

En moyenne **+15 solutions* en place** dans les entreprises (*CESIN, 2024)

Une pénurie mondiale de talents en cybersécurité 2

La rareté des compétences opérationnelles cyber se fait particulièrement sentir dans tous les secteurs, publics comme privés, où les équipes sont souvent surchargées, devant jongler entre des tâches techniques, la gestion des incidents, et le respect des réglementations.

4 millions* de postes non pourvus **dans le monde** (*World Economic Forum, 2024), dont **15 000* en France** (*Wavestone, 2023)

3 Un cadre réglementaire de plus en plus strict

La pression ne cesse de s'intensifier avec l'entrée en vigueur de nouvelles directives comme NIS 2, DORA ou les exigences renforcées de l'ISO 27 001, qui imposent une gouvernance stricte et une traçabilité accrue des assets. Résilience est le maître-mot pour 2025.

La surface d'attaque s'agrandit et se complexifie 4

Avec la multiplication du nombre et des types d'assets, l'interconnexion croissante des systèmes, les nouvelles habitude de travail à distance et le contexte géopolitique international tendu… La surface d'attaque s'agrandit, se complexifie, et le risque de cyberattaque augmente.

5 Les équipes opérationnelles sont surchargées

Le temps perdu à des tâches manuelles reste un problème structurel majeur : les équipes opérationnelles passent un temps considérable à croiser manuellement des données issues de multiples outils.

Ce manque de fluidité freine leur capacité à agir rapidement et efficacement face aux menaces, et les oblige à avoir une posture réactive plus que préventive.

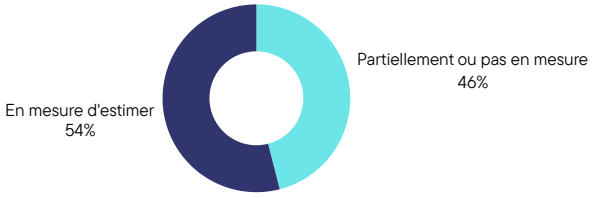
LE CAASM : DÉFINITION

Dans un contexte global qui évolue (très) rapidement, la gestion des assets s'impose comme un pilier fondamental

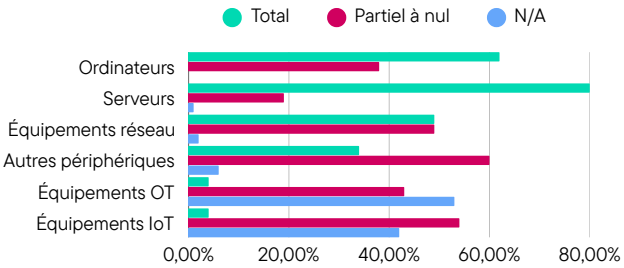
Sans une visibilité complète et en temps-réel sur l'ensemble de leurs assets, il devient impossible pour les équipes opérationnelles d'identifier les points faibles, de prioriser les risques et de réagir efficacement aux attaques. Comme dit l'adage : on ne peut pas protéger ce qu'on ne connaît pas.

Questions aux membres

Seriez-vous en mesure d'estimer le nombre ou le pourcentage de chaque type d'asset informatique dans votre SI ?



Selon vous, pour chacun de ces types d'assets informatiques, à quel niveau pensez-vous en avoir la visibilité / le contrôle ?



Selon vous, quel(s) facteur(s) affecte(nt) le plus votre organisation dans la gestion de ses assets et de sa surface d'attaque ?

	2023	2024
Manque de ressources humaines pour appliquer les plans de remédiation définis	**68,4%**	**72,46%**
Méconnaissance de l'ensemble du périmètre interne et externe à protéger	**69,6%**	**66,67%**
Manque de budget	**24,1%**	**50,72%**
Manque de tableaux de bord de pilotage permettant une priorisation efficace	**48,1%**	**37,68%**

Ces réponses parlent d'elles-mêmes : 2/3 des organisations ont du mal à appréhender le périmètre qu'elles doivent protéger tout en n'ayant pas, pour 1/3 d'entre elles, des tableaux de bord leur permettant un pilotage efficace. La visibilité sur les ordinateurs et serveurs n'est pas parfaite, mais on réalise également ici qu'il est particulièrement difficile d'avoir une bonne visibilité sur les environnements IoT et OT. Ce sont ces points, particulièrement, auxquels répond le CAASM.

Introduite dans le Hype Cycle pour la première fois en 2021, Gartner explique l'apport d'outil de gestion de la surface d'attaque (CAASM, Cybersecurity Asset Attack Surface Management) comme aidant les équipes de sécurité à surmonter les défis liés à la visibilité et à l'exposition des actifs.

Elle permet aux organisations de collecter les données existantes sur leurs assets internes et externes, à partir des différents outils déjà en place (CMDB, scan de vulnérabilités, AD, MDM, scanner réseau, etc.). Ces données sont ensuite consolidées dans un référentiel unique, un inventaire qui est régulièrement mis à jour via des API ou par l'importation de fichiers plats, et est enrichi par les enjeux métiers des différents assets.

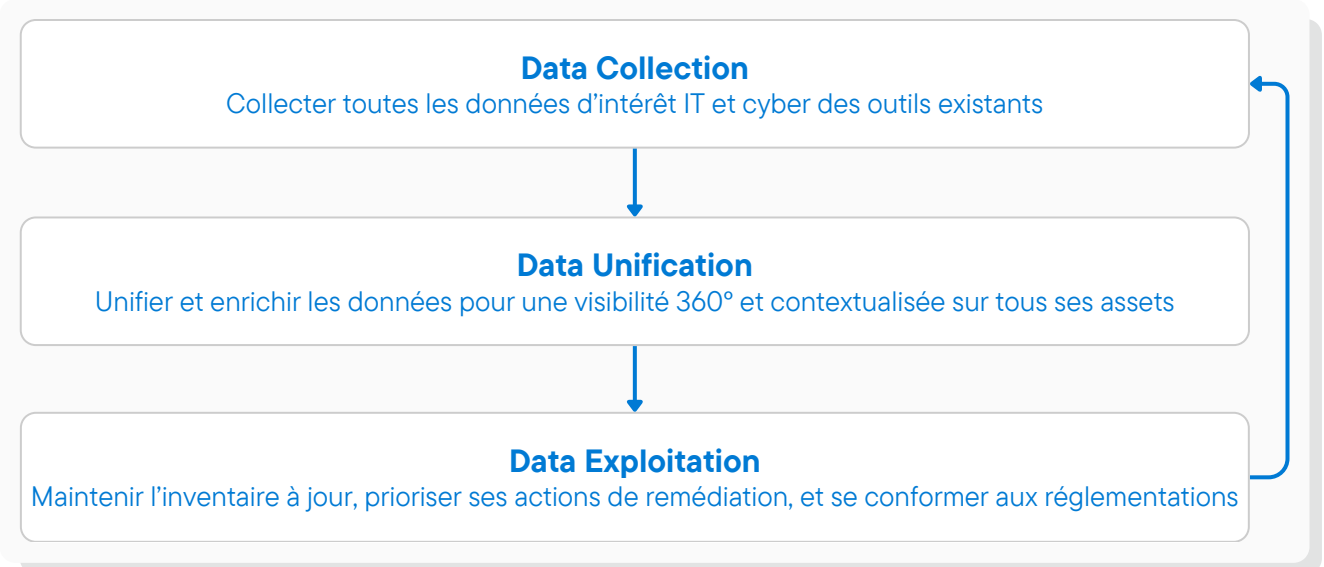
Si l'acronyme vous était inconnu, l'idée d'un « inventaire cyber » doit vous paraître plus familier, Pour en savoir plus, nous vous invitons à consulter le premier livre blanc sur le sujet paru en 2023.

Le CAASM : l'inventaire consolidé au service de la cyber

Cependant, si le terme « inventaire » est utilisé à la fois par les équipes IT et les équipes cyber, il ne désigne pas exactement la même chose, et ne répond pas aux mêmes besoins.

L'objectif de ce livre blanc est d'aider le lecteur à comprendre les problématiques liées à l'absence d'outil de Cybersecurity Asset Attack Surface Management, et de l'informer sur les cas d'usage auquel ils répondent. Dans la continuité de la première étude réalisée en 2023, l'évolution de la perception et de l'utilisation de ce type d'outils par les organisations françaises sera également mis en avant, à travers les réponses des membres du CESIN qui ont été interrogés, ainsi que des extraits d'interviews.

Enfin, pour faciliter la compréhension de tous les aspects du CAASM, ce livre blanc est structuré autour de trois axes, qui représentent les étapes de la fluidification du « Pipeline de données » IT et cyber.



Mais avant cela, revenons d'abord sur la notion d'inventaire, qui est au coeur du CAASM.

Qu’est-ce qu’un inventaire ?

En IT, l'inventaire est une liste exhaustive de l'ensemble des ressources informatiques d’une organisation. Cela inclut les assets physiques (serveurs, postes de travail, etc.), les logiciels (applications, systèmes d’exploitation, etc.), les assets virtuels (machines virtuelles, environnements cloud, etc.) ou encore le contexte métier (configurations, propriétaires, etc.).

Qu’attendent les équipes IT de l’inventaire ?

Les équipes IT utilisent l’inventaire pour recenser, identifier et maintenir à jour le SI, à travers une vue globale de l’ensemble des assets de leur organisation.

Généralement, l’IT utilise l’inventaire pour connaître les informations sur tous les assets actifs et inactifs, organiser les interventions de maintenance, ou encore anticiper les besoins d’amortissement des coûts. Ainsi, l’inventaire doit régulièrement être mis à jour, et les données techniques doivent être croisées avec d’autres données comme les informations métiers.

Qu’attendent les équipes cyber de l’inventaire ?

Si le travail des équipes IT est de gérer l’inventaire, celui des équipes cyber est de sécuriser tous les assets qui le composent. Ainsi, elles ont besoin d’une vision dynamique, presque instantanée sur leur SI, en se basant sur un inventaire à jour et en temps-réel : un besoin auquel les CMDB ne répondent pas toujours.

« Un inventaire, pour moi, c’est quelque chose qui doit vivre. S’il ne bouge pas pendant 1 mois, il ne sert plus à rien. Il doit vivre automatiquement. »

RSO – Retailer

Pour maîtriser et protéger la surface d’attaque, les équipes cyber ont besoin d’un inventaire consolidé et unifié en temps-réel, qui reflète l’état actuel du SI. Cet inventaire doit offrir une vision à 360° :

- Sur tous les types d’assets (physiques et virtuels)
- Dans tous types d’environnements (hybrides, cloud, *on-premises*)
- Et provenant de tous les outils existants pour sécuriser la surface d’attaque (EDR/XDR, scans de vulnérabilités, scans réseaux, etc.)

Un outil de CAASM (Cybersecurity Asset Attack Surface Management) permet aux équipes cyber de disposer d’un tel inventaire, afin d’interroger à partir d’une console unique toutes les informations remontées par tous leurs outils existants. Ainsi, ils peuvent facilement prioriser et suivre leurs actions de remédiation.

« La valeur du CAASM, c’est sa capacité à fédérer différentes sources d’infos pour en générer une seule, unique, fiable et à jour, pour comprendre dans quel outil creuser, corriger et agir. »

Stéphane Joguet, Global CISO – Retailer

Plus que de mettre à disposition une console unique, le CAASM va permettre d’agréger, de corréler et d’unifier automatiquement toutes les données remontées par les outils auxquels il est connecté. Ainsi, parce qu'elles sont fraîches et à jour, les informations remontées par un outil de CAASM peuvent également servir à alimenter une CMDB, un VOC, ou encore un SIEM en retour.

DATA COLLECTION

Le manque de visibilité du SI et la manutention chronophage des données : deux défis majeurs auquel répond le CAASM

L'accumulation d'outils submerge de données les équipes opérationnelles et rend difficile la priorisation des actions de remédiation. Ce travail, essentiel pour prioriser leurs actions, est mené par certaines équipes manuellement.

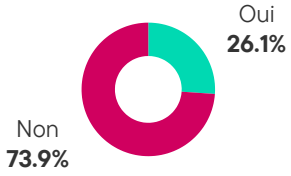
Cependant, ces équipes peinent à rendre le résultat exploitable, car elles rencontrent beaucoup de freins à la consolidation des données : fréquence de mise à jour, pertinence des données, lien(s) entre un même actif au travers des sources, dynamisme des requêtes, diversité des sources, etc.

En parallèle, comme le montrent le graphique ci-contre, une majorité d'entreprises ne dispose pas d'outils conciliant l'ensemble des données qui seraient nécessaires pour les équipes cyber et IT.

Ainsi, la difficulté principale pour les opérationnels réside dans l'absence d'une source unique de vérité, à jour et exploitable, leur permettant de prioriser leurs actions de remédiation, par exemple.

Question aux membres

Disposez-vous d'un outil vous permettant de réconcilier l'ensemble des sources IT et cyber présentes dans votre SI ?



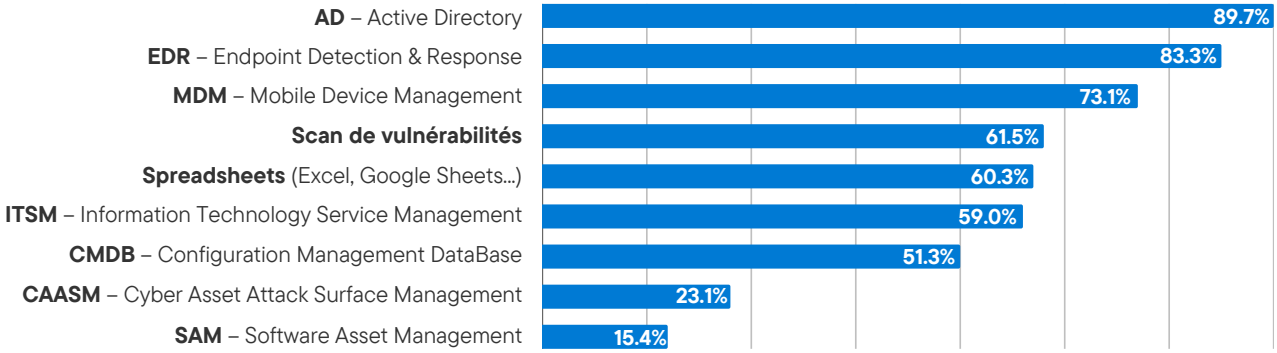
Au coeur du CAASM, la donnée consolidée existante

« L'important est de consolider l'existant. Une fois cette vision complète, on peut l'utiliser pour étendre le périmètre d'installation de chacun des agents / outils. Puis, en faire son point de référence pour avoir une vision sur l'obsolescence, les vulnérabilités, etc. »

Pierre Bedel, RSSI – Groupe Hospitalier Privé

Question aux membres

Dans votre organisation, quels sont les outils que vous utilisez pour gérer et consolider l'ensemble des assets informatiques présents sur votre environnement ?

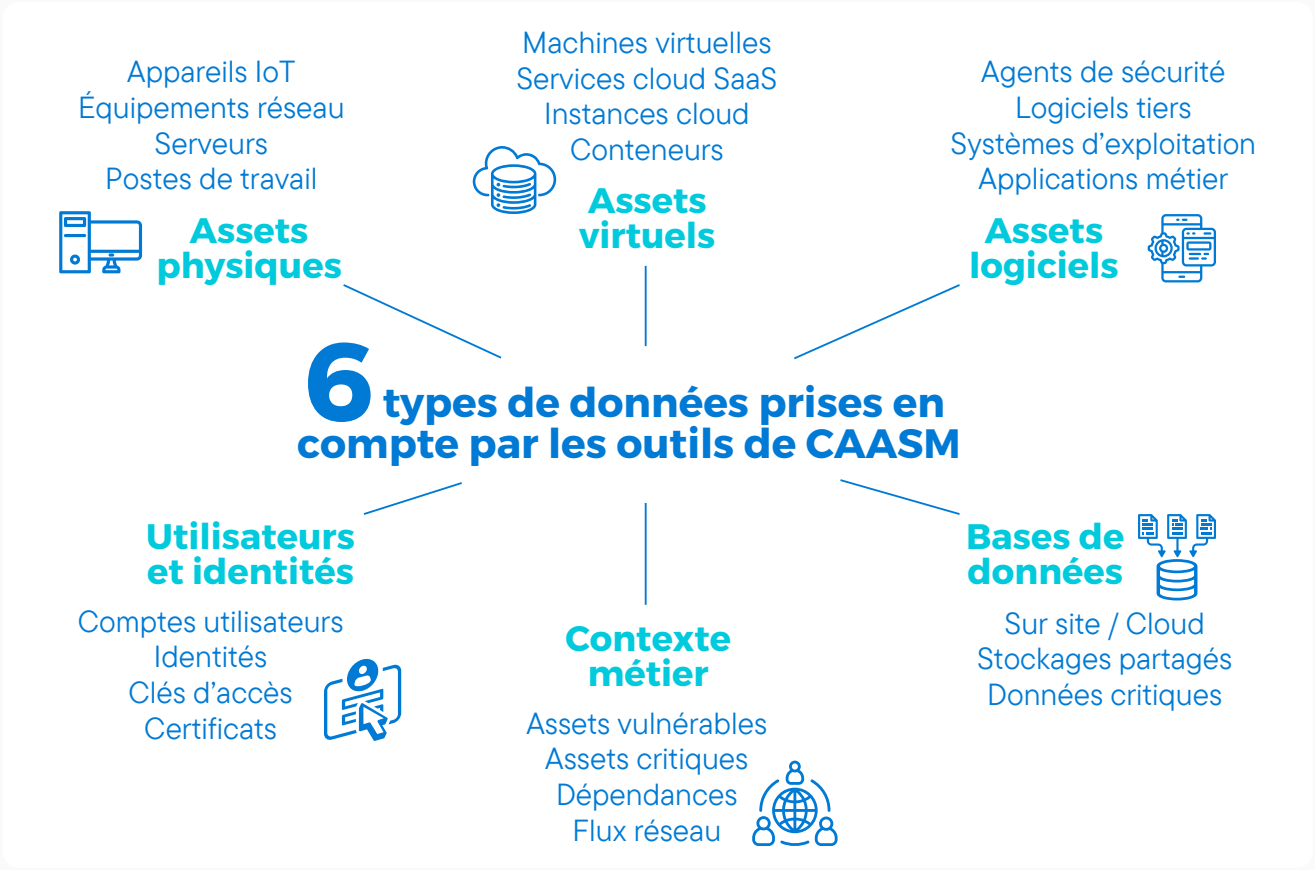


Comme le montrent ces réponses, un des problèmes principaux réside dans le fait que les équipes ont à leur disposition plusieurs points de référence pour consolider les informations. C'est en partie cela qui amène les complexités opérationnelles de traitement des informations.

La valeur du CAASM réside dans sa capacité à fédérer l'ensemble des sources de données d'un SI pour en exploiter pleinement toutes les données. Le référencement de ces sources se fait auprès des équipes opérationnelles qui en ont la connaissance.

« Démultiplier les consoles, c'est augmenter la charge mentale. Ne pas avoir les bons outils est un handicap sur la visibilité de son SI, et son travail de tous les jours. »

David Cauvin, RSSI – Collectivité Urbaine



Les différents types de données prises en compte par les outils de Cyber Asset Attack Surface Management – OverSOC

La prise en charge de ce large éventail de données par le CAASM présente de nombreux avantages :

- **Collecter** les informations directement depuis les outils existants, sur tous types d'assets
- **Exploiter** toutes les données remontées depuis une plateforme unique
- **Améliorer** la visibilité sur vos outils déployés

« On n'a pas les mêmes outils partout dans le groupe. Et avec l'acquisition de nouvelles entités, on a encore de nouveaux périmètres avec leurs propres solutions. Une solution de CAASM permet de centraliser tout ça. C'est un outil qui donne une unique information, et surtout, la bonne information. »

Pierre Bedel, RSSI – Groupe Hospitalier Privé

De plus, les outils CAASM sont compatibles avec tous les outils du marché qui remontent cette donnée : cela permet aux entreprises de changer le reste de leur stack cyber sans perdre les bénéfices de la consolidation des données.

Les outils de CAASM sont agnostiques : ils intègrent automatiquement les données apportées par l'ajout ou le changement de nouvelles sources de données.

DATA UNIFICATION

Croiser, unifier et enrichir les données : plus qu'un inventaire, le CAASM structure la donnée au service de toutes les parties prenantes

« Le CAASM permet, en un claquement de doigt, d'avoir une vue très large sur tous les assets en instantané. »

RSO – Retailer

L'unification des données provenant de l'ensemble des sources de données IT et cyber est au coeur des outils de CAASM. Cette capacité à unifier l'information en temps-réel grâce à son moteur d'unicité permet de supprimer automatiquement les doublons sur l'ensemble des données, et d'identifier les clés de jointure pertinentes entre les données, qu'elles soient techniques ou non : identifiants uniques, adresses IP, etc.

Enrichir la donnée : connaître les bonnes clés de jointure pour rendre la vision pertinente

Avoir les bonnes clés de jointure permet de consolider la donnée pour aider sur les différents cas d'usage du CAASM. Par exemple, pour bien prioriser son patch management, il est important que la donnée soit à la fois exhaustive, unifiée, enrichie et exploitable. Ainsi, il est difficile pour les opérationnels d'établir un plan de remédiation efficace en se basant uniquement sur les données opérationnelles (version d'OS, criticité de la vulnérabilité, état de l'agent EDR…).

Les données métiers sont indispensables pour comprendre le contexte de chaque asset, et prioriser de façon sur-mesure par rapport à votre organisation.

Dans le cas où la criticité d'un asset est connue (57% des répondants), l'information est le plus souvent compilée dans des Spreadsheets (Excel, Google Sheets…) (45%). Elles ne sont donc pas/peu exploitables ou exploitées par les équipes opérationnelles, malgré leur pertinence.

Grâce au CAASM, la consolidation des données techniques et de ces données métier est rendue possible.

La consolidation de l'inventaire permet aux opérationnels d'évaluer les niveaux de criticité de chaque assets en fonction de leur nature, de leur degré d'exposition, ou encore de leurs dépendances / relations avec d'autres assets.

Questions aux membres

Sur l'ensemble de vos assets informatiques, connaissez-vous leurs niveaux de criticité ?

Je ne souhaite pas répondre **12.7%**

Si non, pour quelle(s) raison(s) pensez-vous ne pas connaître leurs niveaux de criticité ?

« Connaissance partielle » « CMDB incomplète » « Shadow IT »
« Business Owner pas identifié » « Pas de centralisation »
« Pas de processus » ***« Pas d'inventaire »*** « Périmètre IoT »
« Équipement dépendant d'autres services »

« Le sujet CAASM dépasse le scope de ce que fait un RSSI, c'est un sujet qui touche la sécurité, mais aussi l'infra. Pour réussir à cartographier son SI, il faut nécessairement aller à la rencontre des métiers. »

Ghislain Banville, RSSI Opérationnel – Naval Group

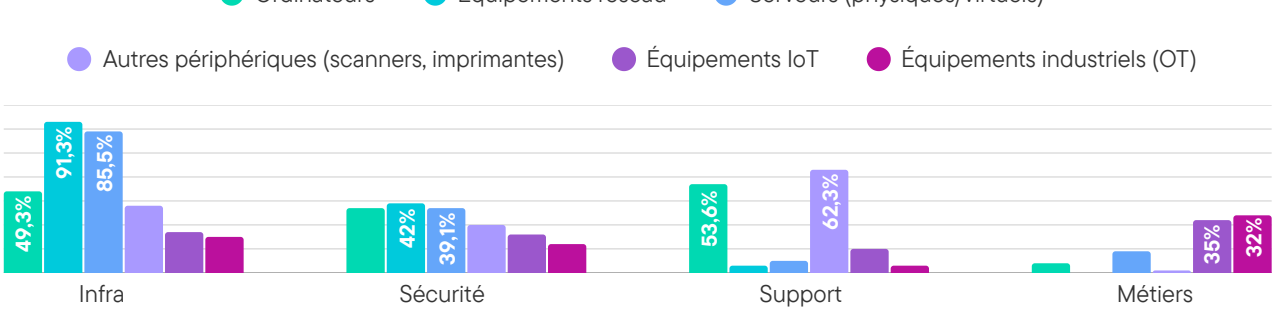
La valeur du CAASM est dans sa capacité à fédérer des informations techniques et métiers pour permettre aux équipes opérationnelles de prioriser leurs actions de remédiation en fonction du contexte de leur organisation.

« Faire le distinguo entre un asset critique et non critique, c'est la responsabilité des métiers avec le support de l'équipe sécu si nécessaire. Inventorier cette donnée et la mettre à disposition des équipes sécu et infra, c'est de la responsabilité de la DSI et ce doit être une fonctionnalité clé du CAASM. »

Ghislain Banville, RSSI Opérationnel – Naval Group

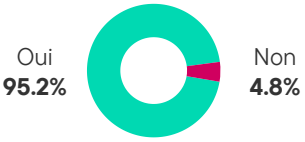
Segmenter l'information : pourquoi le faire, et comment faut-il le faire ?

Question aux membres **Selon vous, qui devrait avoir la responsabilité de l'application des bonnes pratiques de sécurité (applications de correctifs, limitation des droits…) en fonction des assets présents dans votre organisation ?**



Comme le montre ce graphique, la responsabilité de la sécurité des différents assets est un sujet plus complexe qu'il n'y paraît. Pourtant, son impact est conséquent. Le contexte métier est au coeur du CAASM : grâce à la segmentation des informations, il vous permet de mettre en avant le contexte ou le périmètre dans lequel se situe un asset pour aider à responsabiliser les équipes dans la gestion de leurs tâches.

Question aux membres **Selon vous, la mise en place d'un référentiel commun à l'ensemble des équipes IT et cyber est-elle nécessaire pour piloter la sécurité de votre organisation ?**



Pourquoi ?

« On doit parler le même langage, avec les mêmes données. »
« Il faut être synchros : les équipes cyber détectent, l'IT corrige. »
« Sans référentiel commun, pas de connaissance de la criticité des assets et de leurs propriétaires. »

95.2% des répondants pensent que la mise en place d'un référentiel commun à l'ensemble des équipes IT et cyber est nécessaire, afin de fluidifier les interactions entre les équipes. Cependant, 73.9% des répondants disent ne pas disposer d'un outil leur permettant de réconcilier l'ensemble des sources de données IT et cyber présentes dans leur organisation (*cf. page 10, Data Collection*).

Ces deux statistiques nous montrent l'actualité du sujet, mais surtout le besoin et la volonté des équipes à disposer d'un référentiel commun.

« Le CAASM devient la source de vérité, parce que c'est l'outil que tout le monde utilise pour le dashboarding. »

Pierre Bedel, RSSI – Groupe Hospitalier Privé

Grâce à l'automatisation de l'unification de l'ensemble des sources de données IT et cyber, le CAASM est la source de vérité unique permettant de coordonner l'ensemble des équipes (Infra, Support, SecOps, Gouvernance, Métiers…). Sans donner directement accès aux consoles dédiées, les outils de CAASM permettent aux équipes d'avoir une vision 360° sur leurs périmètres dédiés, favorisant la réussite de leurs projets.

La valeur du CAASM réside dans sa capacité à donner le bon niveau d'information à la bonne personne. Ainsi, elle peut prioriser ses actions, suivre les différents projets dans le temps, et éviter les zones de non-responsabilité.

DATA EXPLOITATION

Le référentiel unique produit par le CAASM permet à toutes les parties prenantes d'y trouver leur compte : IT / Infra, SecOps et Gouvernance

« Le CAASM est uniquement juge par la vision, mais on utilise les autres outils en place pour faire les actions. »

RSO – Retailer

Grâce à la centralisation des données, le CAASM offre une vue à 360° sur l'ensemble des assets, permettant ainsi de consulter dans un référentiel unique toutes les informations concernant un même asset. Les opérationnels peuvent alors se concentrer sur la remédiation et mener des actions directement depuis/sur les outils.

Question aux membres **Selon vous, quels sont les 3 indicateurs cyber les plus importants à avoir dans votre organisation ?**

« Indicateurs de risques / performance / conformité »
« Taux de correction des vulnérabilités »
« Taux d'avancement du plan de remédiation »
« Maîtrise du périmètre / de la surface d'attaque »
« Taux de couverture antivirus / EDR / XDR »
« Cycle de vie des assets »
« KPI de rentabilité / Budget »
« Pourcentage de CVE critique non patchée après 6 mois »

La question était ouverte. Ces réponses sont les principales obtenues. Le CAASM permet, grâce à la centralisation des données et à son historisation native, d'exploiter n'importe quel KPI nécessaire aux équipes, d'identifier les écarts entre les sources de données, et de mettre à jour les outils en place.

Pourquoi utiliser un outil de CAASM au quotidien ?

Question aux membres **Quelles sont les principales difficultés que vous rencontrez dans la création de vos tableaux de bord et la définition de vos indicateurs ?**

Absence de croisement d'informations entre les différents connecteurs	**58%**
Pas suffisamment de connecteurs intégrés à mes tableaux de bord	**56%**
Manque de contexte associé aux assets (Business Owner, criticité de l'asset…)	**51%**
Manque de fiabilité des données remontées	**47%**
Pas assez de templates disponibles et pré-configurés pour créer mes tableaux	**43%**
Je ne sais pas quel indicateur suivre	**22%**

Certaines organisations tendent à mettre en place un outil interne de centralisation des données. Cependant, il y a plusieurs difficultés, et les coûts associés sont conséquents. Comme constaté, le sujet de l'inventaire impacte quotidiennement de nombreux sujets : il est nécessaire que les tableaux de bord et les informations soient adaptés pour chacune des équipes.

« Le CAASM nécessite un accompagnement pour adapter les dashboard à ses besoins, tout en ayant la liberté de le faire soi-même. »

Pierre Bedel, RSSI – Groupe Hospitalier Privé

Le CAASM permet de faire ressortir la donnée utile, de mettre en avant des KPIs pertinents pour votre organisation, et vous permet de créer des dashboards personnalisés en fonction des indicateurs que vous cherchez à suivre.

Concrètement, à quoi sert le CAASM ?

Équipes Infra : Automatiser la mise à jour de la CMDB

« L'inventaire global n'est pas toujours à jour, et notre CMDB est loin d'être complète. La grande question, c'est : 'Comment ça se maintient ? Comment on tient ça à jour ?'. »

Stéphane Desmets, Head of Global Cyber Defense – Dekra

La force du CAASM réside dans sa capacité à se connecter à l'ensemble des sources d'une organisation. En ce sens, il permet d'avoir une vue exhaustive sur l'ensemble du parc. En opposant les assets remontés par vos outils et non-présents dans votre CMDB, vous pouvez mesurer en quelques clics l'écart d'inventaire, et mettre à jour ce dernier. Aussi, comme le montrent les réponses aux questions ci-dessous, il est également attendu d'un outil CAASM d'avoir by-design des connexions natives à d'autres outils (le nombre de connecteurs disponibles, jugée à 34% comme une feature très importante) et des indicateurs qui permettent d'en mesurer les écarts.

Question aux membres

Selon vous, quelle importance donneriez-vous aux critères suivants pour choisir une solution de BI cyber / gestion d'assets informatiques / CAASM ?
(Note de 0 (inutile) à 3 (très important)

L'ordre d'importance pour les critères retenu pour la question est le suivant :

1. Le nombre de connecteurs disponibles
2. La possibilité de contextualiser les assets depuis l'interface
3. La création de rapports automatisés
4. La possibilité d'écrire et de mettre à jour mes inventaires (CMDB)
5. La diversité des tableaux de bord pré-configurés

Équipes Gouvernance : Raccorder les données opérationnelles à la gouvernance et combler l'écart existant

« Toutes les normes te demandent de maîtriser ton SI. Donc il est nécessaire d'avoir une visibilité sur tout ce qui doit être protégé. »

Stéphane Joguet, Global CISO – Retailer

Avec l'entrée en vigueur des différentes normes, la mise en conformité des organisation devient une priorité. Mais comment faire ? Par où commencer ?

Beaucoup d'outils permettent de piloter la gouvernance de votre SI pour vous permettre l'alignement progressif de votre SI par rapport aux exigences réglementaires, mais sur quelles informations cela repose ?

En effet, l'enjeu est de taille pour les responsables gouvernance quand il s'agit de relier les normes à leur SI. L'inventaire est, là encore, clé. Les outils CAASM permettent de faire le lien entre la réalité opérationnelle et les exigences des normes.

Le CAASM permet de mettre à jour l'ensemble des outils déployés sur le parc.

Équipes SecOps : Maîtriser sa surface d'attaque et exploiter toutes ses ressources au maximum

« Je n'ai jamais rien modifié dans le CAASM. Le but est de visualiser l'info, de récupérer les assets concernés, puis de pousser une action aux équipes IT. »

Pierre Bedel, RSSI – Groupe Hospitalier Privé

La centralisation automatique des données d'inventaire est clé pour les équipes SecOps, pour leur permettre de prioriser leurs actions en temps-réel.

Pour bien prioriser, les équipes doivent consulter les données d'EDR/XDR, de vulnérabilités, d'inventaire et de contexte métier : le challenge est de taille, mais dans la réalité, le résultat est peu exploitable. Le silotage de l'information ne leur permet pas de trouver les bonnes informations pour leur priorisation.

Question aux membres **Quelles précisions / données supplémentaires vous permettraient de mieux prioriser les assets porteurs de vulnérabilités à patcher ?**

Contexte métier **64.3%**	Exposition sur Internet **58.6%**	Analyse de risques **54.3%**
Responsable de l'asset **41.4%**	Score CVE / EPSS **42.9%**	

Au-delà de la priorisation quotidienne de leurs actions, il est difficile pour les responsables opérationnels de justifier de l'efficacité de leurs équipes. La capacité à prendre du recul et à expliquer simplement les mouvements de la surface d'attaque est clé. L'historisation quotidienne des données facilite grandement le suivi et la communication sur les actions menées.

« Ce qui est intéressant dans le CAASM, c'est d'avoir l'historique des assets qui ont "disparu". "Mon parc, il y a 3 semaines, c'était ça. Et aujourd'hui, c'est ça." Pouvoir partir en arrière, revenir, expliquer pourquoi… Pour justifier de la conformité permanente, et qui perdure. »

Stéphane Joguet, Global CISO – Retailer

Équipes Support : Prioriser le Patch Management

« Connaître et renseigner la criticité et le responsable métier d'un asset, ça nous permet de mieux prioriser le patch management, sans devoir investiguer, comprendre et rechercher les infos, ce qui peut ralentir notre plan d'action, et notamment s'il y a une urgence à traiter. »

Ghislain Banville, RSSI Opérationnel – Naval Group

La priorisation du patch management est un sujet clé pour la sécurisation du SI. Mais comment s'assurer qu'on a bien toutes les informations nécessaires ?

Par exemple, le support de Windows 10 prend fin le 14 octobre 2025. Quels sont les assets concernés ? Qui a la charge de la mise à niveau ? Dans quel ordre prioriser ? Selon quels critères ? Comment suivre l'avancée du projet ?

La vision 360° sur un asset que donnent les outils de CAASM permet aux équipes de prioriser, suivre dans le temps et maîtriser leur politique de patch management.

La centralisation en temps-réel de l'ensemble des données du SI change le quotidien des équipes opérationnelles en leur permettant de ne plus perdre de temps à chercher la donnée entre plusieurs consoles, mais de l'exploiter pour se focaliser sur leur coeur de métier : la remédiation.

Concrètement, comment déployer un CAASM ?

Comment se passe le déploiement d'un outil CAASM ?

Un déploiement en quelques jours

Le déploiement d'un outil de CAASM se fait en quelques jours seulement et sans avoir besoin de déployer d'agent. L'outil se nourrit des données existantes dans les outils déjà déployés par deux moyens : via des requêtes API ou à travers l'import de fichiers plats issus d'extraits des données des outils en place. Une fois les connexions établies ou les fichiers reçus, les équipes OverView monte la plateforme en quelques heures.

Des bénéfices immédiats en termes de visibilité

Grâce aux tableaux de bord pré-packagés déjà présents dans l'outil, il est possible de voir instantanément où se situent les écarts d'inventaire et de mettre en action les équipes concernées en exportant la liste des actifs concernés, tout aussi bien que les indicateurs essentiels aux équipes infrastructure, de sécurité opérationnelle ou de gestion de la conformité.

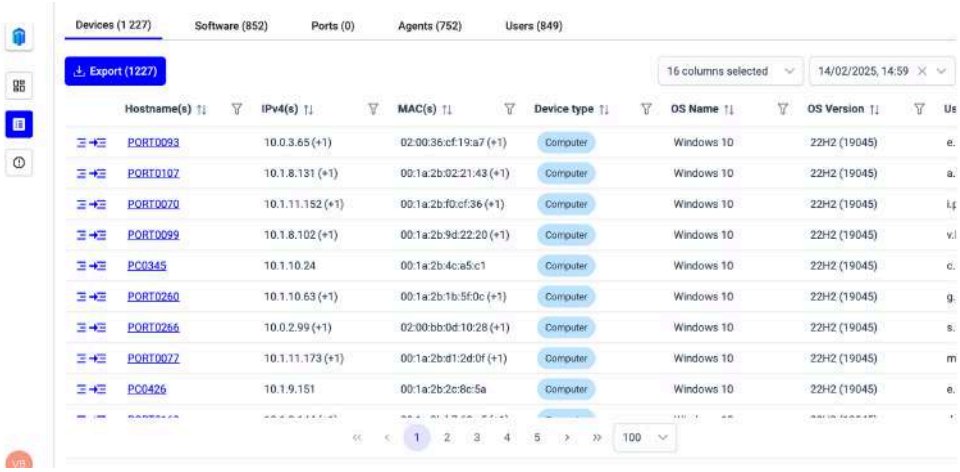
50% de temps gagné par les équipes de sécurité opérationnelle

Plus besoin de naviguer de console en console lorsqu'elle cherche des informations sur le système d'information, et plus de question sur la pertinence de la donnée : les organisations qui utilisent un logiciel de CAASM disent passer jusqu'à moitié moins de temps à chercher, vérifier et consolider de la donnée issue de leurs outils, et donc ont davantage de temps à accorder à des tâches à plus forte valeur ajoutée. Et lorsqu'une question de la direction de l'entreprise ou des assureurs se pose, la réponse est déjà présente dans les tableaux de bord, ou prend quelques clics à trouver.

À quoi cela ressemble-t-il en pratique ?

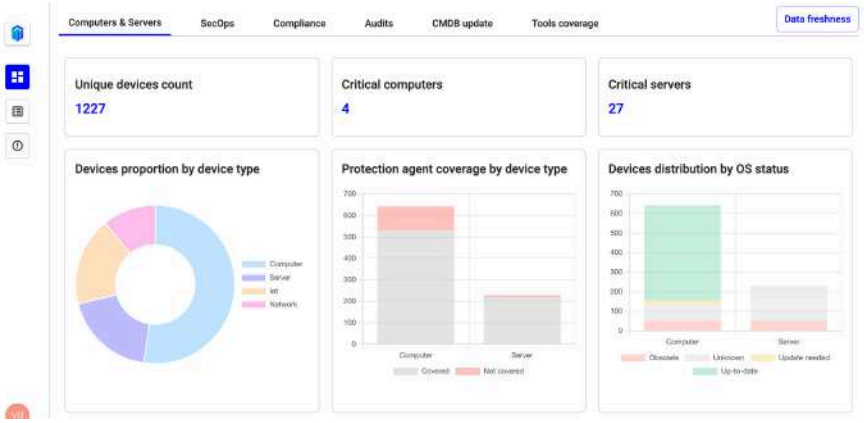
Voici sur les captures d'écran ci-dessous la forme que prend un outil de CAASM.

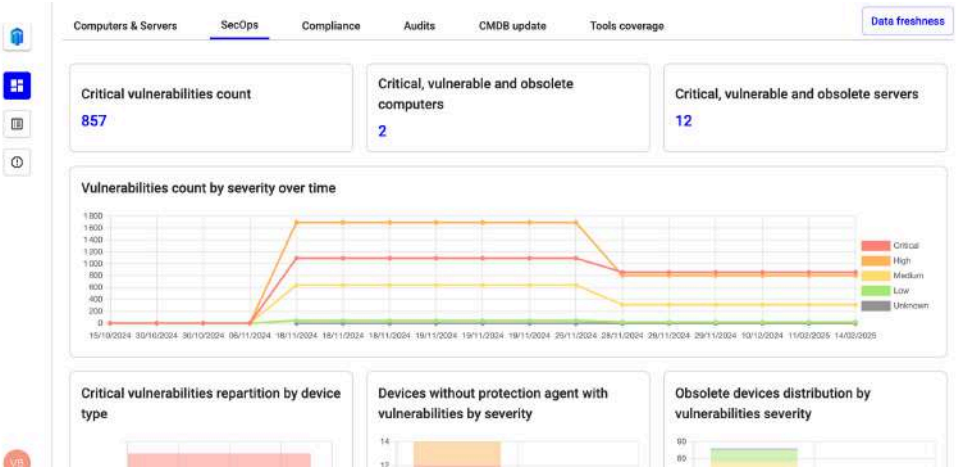
On y retrouve :



- Les listes de l'ensemble des actifs centralisées au même endroit (devices, software, ports, agents, users) et liées entre elles ;

- Différents tableaux de bord pré-packagés (computers & servers, SecOps, Compliance, Audits, CMDB update, Tools coverage), et les différents KPI les constituant ;





- Les données historisées, ce qui permet de rejouer un instant antérieur ou comparer des états du système d'information dans le temps.

CONCLUSION

Le Cybersecurity Asset Attack Surface Management, une brique essentielle de la gestion des assets IT et cyber.

Dans la première édition de ce livre blanc (2023), les outils de CAASM étaient perçus comme une approche encore émergente. La consolidation des données se faisait majoritairement avec des solutions internes (41,8%), dont Excel (71%), ou PowerBi (33%).

Cependant, en 2024, les organisations font toujours face à des problématiques majeures de visibilité sur leur système d'information, et le besoin de consolidation de l'inventaire IT et cyber est un enjeu plus que jamais d'actualité.

73,9% des répondants ne disposent pas d'outils leur permettant de réconcilier l'ensemble des sources IT et cyber présentes dans leurs SI.

95.2% des répondants pensent que la mise en place d'un référentiel commun à l'ensemble des équipes IT et cyber est nécessaire, afin de fluidifier les interactions entre les équipes.

Ainsi, après une apparition dans le 9ème Baromètre de la Cybersécurité du CESIN, cette deuxième édition du Rapport CAASM 2024 montre que les solutions de CAASM gagnent de plus en plus en maturité auprès des organisations.

Grâce à la consolidation de l'inventaire, le CAASM permet de répondre aux besoins de visibilité des équipes de sécurité opérationnelle, tout en jouant un rôle clé dans la collaboration entre IT et cyber. Il devient ainsi un véritable outil de convergence, capable d'aligner les priorités des équipes et de fluidifier les processus internes.

Toutefois, malgré cette montée en puissance, le marché du CAASM souverain reste limité, OverView by OverSOC est la seule solution française. Les entreprises françaises et européennes, soucieuses de maîtriser leur infrastructure et leurs données sensibles, devront donc rester attentives aux évolutions de l'offre pour trouver des solutions adaptées à leurs exigences de sécurité et de conformité.

Dans un paysage où la complexité IT et les menaces cyber ne cessent d'évoluer, le CAASM représente un levier d'action. En offrant une visibilité consolidée et exploitable, il permet aux organisations de reprendre le contrôle de leur surface d'attaque et de bâtir une stratégie cyber plus robuste et plus résiliente.

Question aux membres **Quelle est la perception des outils de CAASM par les opérationnels ?**

Pour vous, le CAASM fait-il l'objet d'un projet en 2025 ?

Oui
41,8%

Pour vous, quelle serait votre prochaine étape vis-à-vis d'une solution de CAASM ?

Je suis intéressé·e par une démo
53.5%

Je suis en phase de benchmark
16.2%

J'aimerais tester
30.3%

CONCLUSION

Le Cybersecurity Asset Attack Surface Management, une brique essentielle de la gestion des assets IT et cyber.

Face à une menace cyber toujours plus sophistiquée et un environnement IT en constante évolution, les logiciels de gestion de la surface d'attaque des actifs (CAASM) s'imposent comme un levier stratégique pour renforcer la résilience des entreprises.

Pourtant, notre étude révèle que 73,9 % des répondants ne disposent pas d'outils leur permettant de réconcilier l'ensemble des sources IT et cyber présentes dans leurs SI. Ce constat souligne une fragmentation des données et des processus qui freine la capacité des organisations à obtenir une visibilité complète et unifiée sur leur exposition aux risques.

L'enjeu est donc de taille : pour répondre aux nouvelles exigences de cybersécurité, les entreprises doivent impérativement repenser leur approche de la gestion des actifs en brisant les silos entre les équipes IT et cyber.

À cet égard, 95,2 % des répondants estiment nécessaire la mise en place d'un référentiel commun permettant d'améliorer la collaboration et d'accélérer la prise de décision. Une telle démarche est aujourd'hui incontournable pour renforcer la réactivité face aux menaces et optimiser les efforts de remédiation.

Le marché du CAASM est en pleine expansion, porté par une double nécessité : une meilleure gouvernance des actifs et une automatisation accrue pour alléger la charge opérationnelle des équipes de sécurité. Ces outils ne sont pas une tendance passagère ; ils répondent à un besoin fort et durable des entreprises, qui peinent encore à obtenir une vision unifiée de leur surface d'attaque.

L'acquisition récente de Noetic Cyber par Tenable confirme cet engouement et témoigne de la structuration progressive du marché. Mais au-delà des outils, l'efficacité repose aussi sur la fluidité des échanges entre les équipes IT et cyber.

Pour 64 % des répondants, comme dans le premier livre blanc, le contexte métier reste le facteur le plus important pour faciliter le dialogue et les opérations de remédiation. Cette continuité souligne l'enjeu central de la contextualisation des actifs et des vulnérabilités pour mieux prioriser les actions et optimiser les efforts de remédiation. Avec une adoption qui s'accélère et une offre technologique en constante évolution, le CAASM s'impose comme un pilier durable de la cybersécurité et continuera à transformer les pratiques des entreprises face aux menaces de demain.

ANNEXE

Profil des répondants et de leurs systèmes d'information

78 membres du CESIN ont répondu au questionnaire, entre mi-septembre et mi-octobre 2024.

Nombre de collaborateurs dans l'organisation

TPE / PME : **14,3%**

ETI : **38,1%**

Grandes entreprises : **47,6%**

Secteur d'activité de l'organisation

Services : **31,7%**
Industrie / BTP : **15,9%**
Services publics : **23,8%**
Commerce : **28,6%**

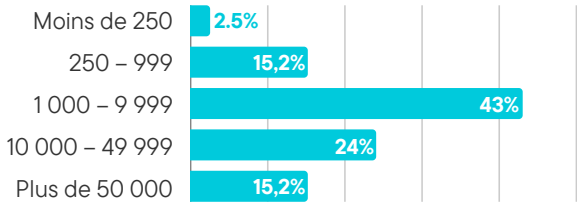
Profil des répondants

Sur 78 répondants :

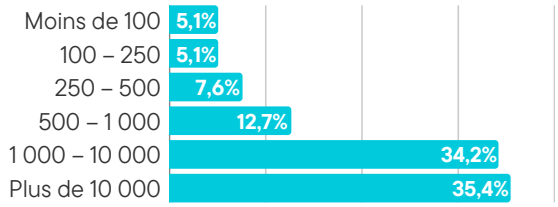
Responsable de la Sécurité des Systèmes d'Information (RSSI) : **71,4%**
Directeur Cybersécurité : **23,8%**
Directeur du Système d'Information (DSI) : **1,6%**
Autres (Administrateur Système, Consultant Cyber, ...) : **4,8%**

En moyenne, savez-vous... :

Combien d'assets composent votre SI ?



Combien d'utilisateurs compte votre SI ?



Quels sont les types d'assets informatiques qui composent votre système d'information ?

100% Ordinateurs

97,5% Serveurs (physiques/virtuels)

98,7% Équipements réseau

91% Autres périphériques

51,9% Équipements industriels (OT)

55,7% Équipements IoT

34,2% Autres

OverSOC et le CESIN remercient chaleureusement l'ensemble des témoins, des répondants et des participants qui ont permis de mener à bien cette étude.

À propos du CESIN

Le Club des Experts de la Sécurité de l'Information et du Numérique - CESIN - est une association Loi 1901 favorisant l'échange de connaissances, le partage d'expérience et la coopération entre professionnels de la sécurité de l'information et du numériques. Ses membres actifs sont des experts occupant des postes de management de la sécurité de l'information et du numérique (RSSI, DSSI, DSI, CISO), au sein d'entreprises privées ou publiques à l'exclusion des entreprises commerciales dont l'activité principale est la fourniture d'équipements ou de conseil en sécurité de l'information et du numérique. Les spécialistes du Droit associé à la sécurité de l'information et du numérique sont également membres actifs.Les membres associés sont des représentants des services de l'Etat (justice, police, services du premier ministre) dont l'activité s'effectue en étroite collaboration avec les experts de la sécurité de l'information et du numérique, membres du CESIN.

Pour plus d'information : https://cesin.fr/

CESIN - Club des Experts de la Sécurité de l'Information et du Numérique
115 rue Saint-Dominique - 75007 PARIS

E-mail : contact@cesin.fr

À propos d'OverSOC

La Data Intelligence au service de vos équipes informatiques et cybersécurité.
OverSOC est un éditeur de logiciel basé dans le Campus Cyber des Hauts-de-France et de Lille Métropole fondé en 2020.
OverSOC se positionne comme référence française et européenne sur le sujet du *Cybersecurity Asset Attack Surface Management* (CAASM), ou — gestion de la surface d'attaque des actifs numériques — une typologie d'outils émergente de consolidation d'inventaire à partir de l'ensemble des sources de données informatiques et cybersécurité déjà en place dans les organisations.
OverSOC est membre d'Hexatrust, du Pôle d'Excellence Cyber et de Systematic, et alumni de la Cyber Défense Factory du Ministère des Armées et du programme Cyber@Station F de Thales.
La publication en octobre 2023 de la première édition du « Rapport CAASM 2023 », suivie d'une seconde un an plus tard « Rapport CAASM 2024 », atteste de la position d'OverSOC en tant que référence du CAASM (Cyber Asset Attack Surface Management) sur le marché Français et Européen.

Pour plus d'information : https://oversoc.com/

OverSOC SAS
177 Allée Clémentine Deman - 59000 Lille

E-mail : contact@oversoc.com