Livre Blanc

Quelle maturité, quelles attentes de la part des **organisations françaises** vis-à-vis des **outils CAASM* ?**

Résultat de l'étude réalisée conjointement par OverSOC et le CESIN

CESIN OVERSOC

*Cyber Asset Attack Surface Management

Sommaire

Édito

Aujourd'hui, toutes les activités d'une organisation - entreprise ou collectivité - sont interconnectées avec son système d'information, ce qui entraîne une augmentation exponentielle des données générées : les réseaux, les applications, les équipements physiques, les utilisateurs et les administrateurs avec de nombreux niveaux de privilèges. A cela s'ajoute la transformation digitale, laquelle complexifie les systèmes d'information, avec une augmentation de la vulnérabilité aux cyber-attaques. Protéger correctement son système d'information devient un vrai défi pour les organisations. Or, elles ont souvent une compréhension partielle et incomplète de leur système d'information, des différents actifs qui le composent et des interconnexions entre ceux-ci. Avec de tels enjeux, protéger son système d'information et ses données grâce à un inventaire exhaustif et à jour devient une priorité absolue.

Qualifiée par l'ANSSI comme un « outil indispensable à la maîtrise de son système d'information », la cartographie du SI prend place dans une démarche globale de gestion des risques cyber. Elle donne aux organisations une meilleure lisibilité sur les différents éléments qui constituent leur SI et leur permet donc d'en reprendre le contrôle. Si ce constat est largement partagé, la mise en œuvre concrète d'une cartographie du SI pêche encore dans de nombreuses organisations, réalisée manuellement à partir de données disparates issues d'outils fonctionnant en silo. Les outils de gestion de la surface d'attaque des actifs cyber à savoir CAASM (Cyber Asset Attack Surface Management) permettent justement d'agréger ces différentes données existantes, de manière beaucoup plus simple et lisible qu'à travers des « outils maison ».

Club d'échanges pour les experts de la sécurité et du numérique, le CESIN a travaillé conjointement avec OverSOC pour la réalisation d'une étude portant sur la maturité des organisations françaises au sujet du CAASM et leurs attentes en matière de soutien opérationnel dans ce domaine. Lieu dédié au partage de connaissances et d'expériences, le CESIN favorise l'émergence de solutions pragmatiques et performantes pour faire face aux risques auxquels sont confrontées les organisations.

Alain BOUILLÉ
Délégué général du CESIN

Contexte et objectifs de l'étude

Défini par Gartner comme préoccupation numéro 1 en cybersécurité, le contrôle de la surface d'attaque reste aujourd'hui l'un des sujets les plus en vue du paysage cyber. Gartner a d'ailleurs mis au point en 2021 un nouvel acronyme pour regrouper les solutions qui permettent d'agréger, de corréler, et de mettre à disposition l'ensemble des informations IT et cyber issues des outils déployés sur le parc informatique : il s'agit du Cyber Asset Attack Surface Management (CAASM).

Suite à un premier meetup fructueux pour les membres du CESIN le 11 janvier 2023 sur « Cybersecurity Asset Attack Surface Management : l'interopérabilité des solutions cyber françaises au service des responsables IT et cyber », Le CESIN et OverSOC ont décidé de lancer conjointement une étude en profondeur sur l'évaluation de la maturité des organisations au sujet du CAASM.

Cette étude a été menée à l'attention des RSSI et DSI français. Elle a reçu le soutien du Pôle d'Excellence Cyber (PEC) et de Systematic Paris-Région.

Ce travail trouve son origine dans plusieurs constats. Les systèmes d'information se complexifient. Les surfaces d'attaque, qu'elles soient exposées sur Internet ou non, deviennent de plus en plus compliquées à appréhender, à suivre dans le temps, à maîtriser, et donc à défendre. Si chaque solution est pertinente, les différents outils de sécurité sont silotés et parfois difficiles à faire travailler de concert. La cartographie du système d'information, identifiée par l'ANSSI comme un outil indispensable, permet justement d'obtenir une meilleure lisibilité de ces différentes données, une meilleure maîtrise de sa surface d'attaque et donc une meilleure défense, à chaud comme à froid.

« *Outil indispensable à la maitrise de son système d'information (SI) et obligatoire pour les Opérateurs d'importance vitale (OIV), la cartographie du SI permet de connaitre l'ensemble des éléments qui le constituent pour en obtenir une meilleure lisibilité, et donc un meilleur contrôle. Elle s'intègre dans une démarche globale de gestion des risques* » (ANSSI). »

Regagner la maîtrise de son système d'information est un objectif ambitieux, mais il n'en reste pas moins compliqué d'un point de vue opérationnel pour de nombreuses organisations. Les données dont elles disposent sont nombreuses, mais elles ont besoin d'être agrégées et corrélées. A cela s'ajoute un impératif d'automatisation, car les ressources humaines sont souvent insuffisantes pour traiter cette masse de données. La démarche de cartographie sans automatisation est aujourd'hui peine perdue. Il est inconcevable, à l'heure où la volatilité de l'information est à son paroxysme, de ne pas s'outiller pour mieux l'inventorier.

Les objectifs sont triples :

- anticiper : lancer des alertes sur des signaux clés pour anticiper de potentielles actions malveillantes sur l'infrastructure IT et améliorer les capacités d'analyse du contexte ;
- renforcer : réduire le délai de réponse, tirer parti des informations après un incident cyber, renforcer la posture de défense organisationnelle et technique face à ces menaces, ainsi que sensibiliser de manière précise et ciblée ;
- réagir : mettre en place un dispositif de réponse aux incidents pour une intervention immédiate et garantir une identification rapide des informations post-incident. Faire des retours d'expérience approfondis pour les rendre plus compréhensibles par les parties prenantes.

L'objectif global de cette étude est d'évaluer la maturité des organisations françaises sur le CAASM et les pistes de renforcement opérationnel attendues dans ce domaine.

Executive summary

Problématiques et enjeux des organisations françaises

- Dans un contexte où les menaces sont omniprésentes, les organisations françaises doivent prendre des mesures pour atténuer les risques de manière proactive, anticiper les cyber-risques, prévenir et limiter les dommages causés par les cyberattaques et les violations de données.

- Pour les organisations françaises, la maitrise du système d'information et la protection de la surface d'attaque (interne et externe) sur le plan opérationnel est complexe. La méconnaissance de l'ensemble de leur périmètre, le manque de ressources humaines, l'absence de tableaux de bord de pilotage et les contraintes budgétaires sont les raisons les plus citées.

- Le nombre d'attaques potentielles correspond au nombre de vulnérabilités existantes ; les organisations françaises doivent identifier leurs faiblesses et identifier leurs points d'entrée pour améliorer leur posture de sécurité et réduire la surface d'attaque.

- Protéger son système d'information et ses données grâce à un inventaire fiable et complet des actifs cyber, avec un contexte immédiat et une visibilité claire est une priorité majeure.

- L'étude met en évidence les divergences entre les besoins exprimés par les organisations françaises pour minimiser leur exposition aux risques cyber d'une part et leurs attentes vis-à-vis des solutions CAASM d'autre part.

Quelle perception par le Top Management des défis cyber ?

- La plupart des décideurs du Top Management (RSSI et DSI) estiment avoir une perception élevée de la compréhension des défis liés à la cybersécurité (57% des répondants de l'étude).

- En revanche, un pourcentage non négligeable de RSSI et DSI estime avoir un niveau moyen ou faible de compréhension (environ 30%).

- Si la CMDB est citée par près d'une entreprise sur deux, elle n'en reste pas moins très consommatrice en « temps homme » (beaucoup plus consommateur de « temps homme » que les outils CAASM). Dans une période de pénurie de professionnels qualifiés en cybersécurité, il s'agit d'une préoccupation majeure des RSSI et DSI des organisations françaises.

- Les organisations de plus petite taille ont encore un pourcentage non négligeable de niveau moyen ou faible de compréhension. Parmi les entreprises de moins de 1 000 employés, 48% estiment avoir une compréhension élevée du risque cyber. L'impact des cyberattaques sur ce type d'entreprise peut parfois conduire à la cessation pure et simple de leur activité (plus particulièrement les startups et les PME).

Les solutions envisagées pour gagner en maturité

- Sensibiliser les organisations françaises et les encourager à automatiser la collecte et l'exploitation des données de sécurité en utilisant une cartographie de leur SI devient essentiel. Cette approche permettrait d'améliorer la visibilité, la réactivité et l'efficacité des mesures de sécurité, réduisant ainsi le risque de menaces sur les données et les actifs sensibles.

- Outre les audits et les tests d'intrusion classiques, l'étude souligne l'importance et la pertinence des solutions CAASM pour identifier les actifs critiques et l'étendue des vulnérabilités, détecter les lacunes dans les contrôles de sécurité et ainsi réduire le risque d'attaques cyber.

- Les résultats de l'étude montrent que la plupart des entreprises n'ont pas encore pris conscience des avantages d'une solution CAASM pour automatiser la collecte, l'agrégation et l'exploitation des données de sécurité grâce à une cartographie de leur système d'information. Pourtant, celle-ci permettrait de gagner en efficacité et en précision, en évitant les tâches fastidieuses de traitement manuel et de croisement des données.

- Sensibiliser les organisations françaises et les encourager à automatiser la collecte et l'exploitation des données de sécurité en utilisant une cartographie de leur SI devient essentiel. Cette approche permettrait d'améliorer la visibilité, la réactivité et l'efficacité des mesures de sécurité, réduisant ainsi le risque de menaces sur les données et les actifs sensibles.

- Le manque de ressources humaines est aujourd'hui le critère le plus important pour constituer un inventaire complet et à jour. La mise en place d'une solution automatisée est la meilleure solution pour pallier ce problème.

Qu’est-ce que le Cyber Asset Attack Surface Management (CAASM) ?

Le "Cyber Asset Attack Surface Management" (CAASM) correspond à la gestion de la surface d'attaque des actifs numériques dans le domaine de la cybersécurité.

Selon Gartner, le Cyber Asset Attack Surface Management (CAASM) vise à permettre aux équipes de sécurité de surmonter les défis liés à la visibilité et à l'exposition des actifs. Il permet aux organisations de voir tous les actifs (internes et externes), principalement par le biais d'intégrations API avec des outils existants, d'interroger des données consolidées, d'identifier l'étendue des vulnérabilités et des lacunes dans les contrôles de sécurité, et de remédier aux problèmes.

Le CAASM élimine virtuellement les « angles morts » et permet aux équipes chargées des opérations de sécurité d'avoir une approche proactive pour anticiper les cyber-risques. En fait, grâce au CAASM, Gartner prévoit que le nombre d'organisations ayant une visibilité des actifs supérieure ou égale à 95% passera à 20% d'ici 2026, contre moins de 1% aujourd'hui.

Les principales étapes du CAASM comprennent :

- l’identification des actifs numériques : recenser et cartographier tous les actifs numériques d'une organisation, tels que les serveurs, les applications, les bases de données, les dispositifs IoT ;
- l’évaluation des vulnérabilités : identifier les vulnérabilités potentielles présentes dans chaque actif numérique, en effectuant des analyses de vulnérabilité et en utilisant des outils de sécurité ;
- l’analyse de la surface d'attaque : examiner tous les points d'entrée possibles à partir desquels un attaquant pourrait cibler un actif numérique. Cela peut inclure les ports ouverts, les protocoles exposés, les services en cours d'exécution ;
- la réduction de la surface d'attaque : mettre en œuvre des mesures pour réduire la surface d'attaque en fermant les ports non nécessaires, en désactivant les services inutilisés, en appliquant des correctifs de sécurité par exemple ;
- la surveillance continue : mettre en place une surveillance continue de la surface d'attaque pour détecter tout changement ou nouvelle vulnérabilité qui pourrait émerger ;
- la gestion des risques : évaluer et hiérarchiser les risques associés à chaque actif numérique en fonction de leur importance pour l'organisation, de la criticité des données.
- la gestion des accès et des identités (IAM) : s’assurer que les personnes et les entités ayant une identité numérique ont le bon niveau d’accès aux ressources de l’entreprise comme les réseaux et les bases de données (rôles utilisateur et privilèges d’accès).

En adoptant une solution CAASM, les organisations visent à renforcer leur posture de sécurité en minimisant les opportunités pour les attaquants de cibler et d'exploiter des failles de sécurité. Cela fait partie intégrante de la stratégie globale de gestion des risques en cybersécurité.

Méthodologie de l'étude et profil des répondants

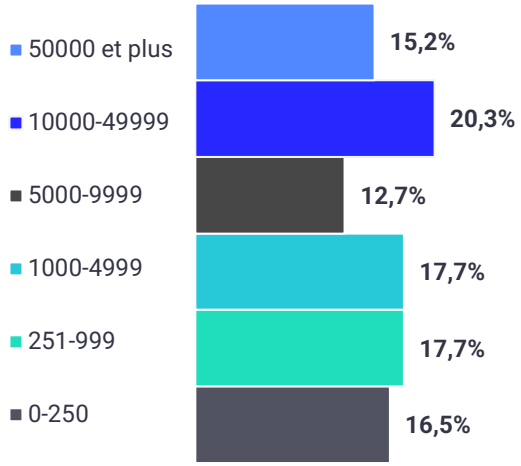
Méthodologie de l'étude

Un questionnaire en ligne de 25 questions a été élaboré et envoyé aux membres du CESIN. Les réponses ont été recueillies du 1er avril au 30 avril 2023.

79 des membres du CESIN ont répondu à l'étude.

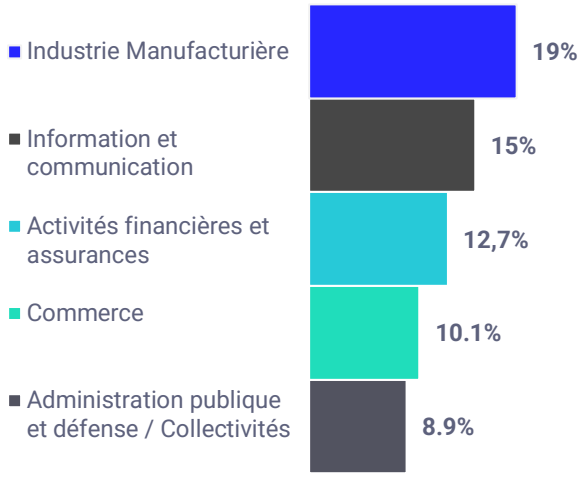
Profil des répondants

Nombre de salariés de l'organisation



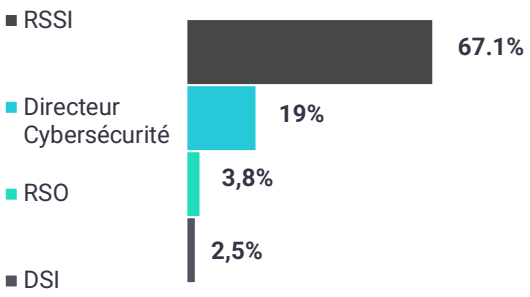
La tranche la plus représentée est celle des organisations ayant entre 10 000 et 49 999 salariés.

Secteur d'activité de l'organisation*



L'INSEE dispose d'une classification NAF (Nomenclature des Activités Françaises) qui représente une classification des activités économiques productives. Nous avons fait le choix de ce référentiel dans le cadre de cette étude.

L'industrie manufacturière est le secteur d'activité le plus représenté, suivi de « information et communication », « activités financières et assurances », « commerce » et « administration publique et défense / collectivités ».

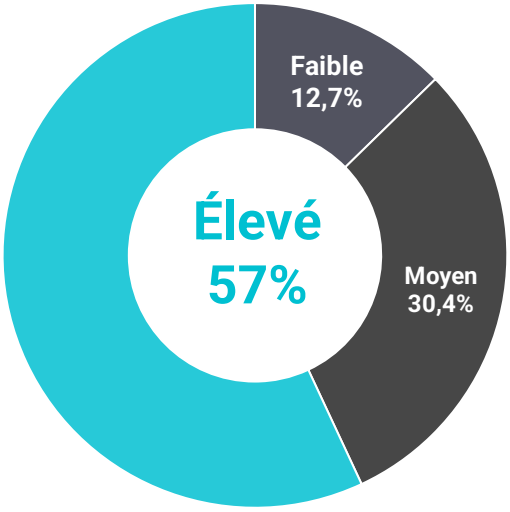


Fonctions

Les membres du CESIN sont principalement des RSSI ou équivalents d'où l'homogénéité des fonctions exercées.

Les répondants sont massivement des RSSI d'industries manufacturières. En revanche, la proportion du nombre de salariés au sein des organisations est plus homogène.

Comment estimez-vous le niveau de compréhension du risque cyber par votre top management ?

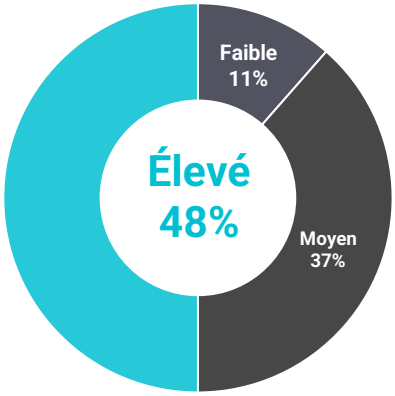


La majorité du top management, soit 57%, estime avoir un niveau élevé de compréhension du risque cyber. Environ 30,4% estiment avoir un niveau de compréhension moyen, tandis que 12,7% considèrent avoir un niveau faible de compréhension.

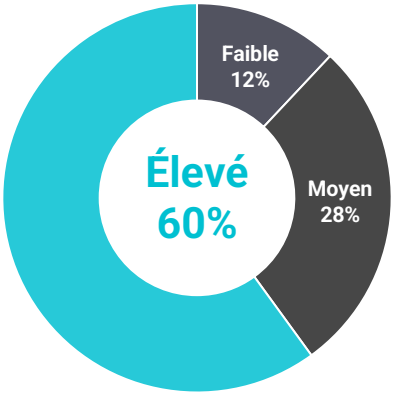
Ces résultats indiquent que la plupart des décisionnaires du top management ont une perception élevée de leur compréhension des enjeux liés à la cybersécurité. Cependant, il est également important de noter qu'un pourcentage non négligeable estime avoir un niveau moyen ou faible de compréhension. Cela souligne l'importance pour le top management de mettre en place une stratégie adaptée, de fixer des objectifs de sécurité et de s'engager dans une démarche de sensibilisation des risques. Le but étant d'améliorer la compréhension globale, de faciliter la priorisation et la prise de décision face aux situations de crise.

Niveau de compréhension du risque cyber en fonction de la taille d'organisation :

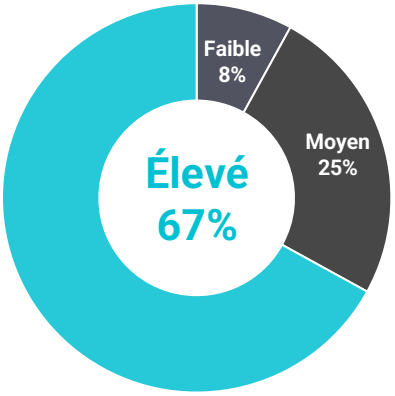
Entreprises avec moins de 1 000 employés



Entreprises entre 1 000 et 30 000 employés

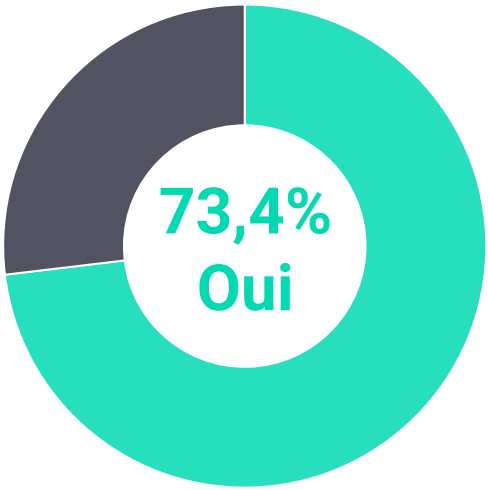


Entreprises avec 50 000 employés



Sur la base des 79 répondants à l'étude, on observe que plus la taille de l'organisation augmente, plus le niveau de compréhension du risque cyber est élevé. Parmi les entreprises de moins de 1 000 employés, 48% estiment avoir une compréhension élevée du risque cyber. Ce chiffre passe à 60% pour les entreprises de taille moyenne (entre 1 000 et 30 000 employés) et à 67% pour les grandes entreprises (plus de 50 000 employés). Cela souligne un niveau de maturité élevé dans les grandes entreprises sur les sujets cyber.
Ces résultats soulignent l'importance pour les entreprises de toutes tailles de continuer à renforcer leur compréhension du risque cyber et à investir dans des mesures de sécurité appropriées, en particulier pour les organisations de plus petite taille qui ont encore un pourcentage non négligeable avec un niveau moyen ou faible de compréhension. L'expérience montre que l'impact des cyberattaques sur ce type d'entreprise peut parfois conduire à la cessation pure et simple de leur activité (plus particulièrement les startups et les PME).

Afin de répondre à la menace cyber, disposez-vous d'un Security Operation Center (SOC) aujourd'hui ?



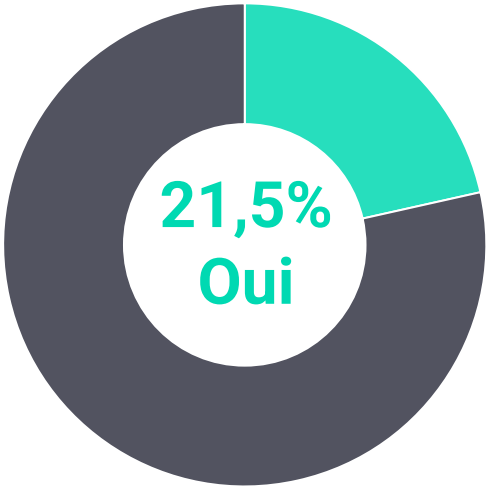
Un Security Operation Center (SOC) est un centre opérationnel de sécurité chargé de surveiller, analyser et répondre aux menaces de sécurité informatique. La majorité des organisations ont donc pris des mesures pour renforcer leur posture de sécurité en mettant en place un SOC, ce qui leur permet de détecter et de réagir plus rapidement aux événements de sécurité.

73,4 % des organisations disposent actuellement d'un Security Operation Center (SOC) pour faire face à la menace cyber, tandis

que que plus d'un quart des organisations ne disposent pas de SOC. Il est important pour ces organisations de considérer l'adoption d'un SOC ou d'autres mesures de sécurité appropriées afin de renforcer leur résilience face aux menaces cyber, compte tenu de l'évolution constante du paysage de la sécurité informatique.

💡 C'est dans ce contexte que les outils CAASM (CyberAsset Attack Surface Management) montrent tout leur intérêt. En donnant aux professionnels de la cybersécurité une liste exhaustive et contextualisée des différents actifs du système d'information, ils aident à mieux le protéger.

Avez-vous déjà mis en place l'une de ces solutions CAASM dans votre organisation ?



Les résultats montrent que la majorité des entreprises n'ont pas encore pris conscience de l'intérêt d'une solution CAASM pour leur organisation.

Il est important de noter que la mise en place d'une telle solution peut aider les organisations à gérer et à réduire les risques liés à la surface d'attaque de leurs actifs cyber. Cependant, la majorité des organisations semblent ne pas encore avoir pris cette mesure, ce qui peut indiquer un besoin d'amélioration en termes de sécurité et de gestion des risques cyber.

Cartographier son SI : un besoin évident et partagé

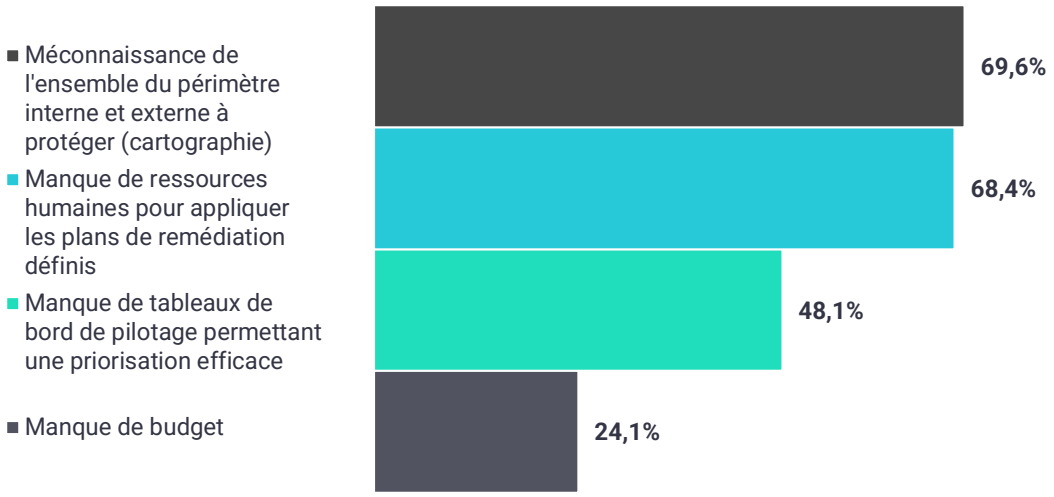
Si les pratiques en matière de cartographie restent très hétérogènes, la nécessité d'une telle démarche, notamment dans le cadre de la réponse à incident, est en revanche bien comprise. 84,8 % des professionnels interrogés pensent qu'une cartographie à jour de leur système d'information pourrait les aider à résoudre une attaque plus rapidement.

Cartographie du SI / CAASM : état des lieux des pratiques, besoins et difficultés

Maîtriser la totalité de son périmètre : une action nécessaire mais délicate

Protéger une surface d'attaque dans sa totalité (interne et externe) reste un projet difficile à mener. Lorsqu'on interroge les professionnels sur les facteurs qui affectent le plus leur organisation, la méconnaissance de l'ensemble de leur périmètre est la réponse la plus citée. Viennent ensuite le manque de ressources humaines, de tableaux de bord de pilotage permettant une priorisation efficace, et enfin de budget.

Il est difficile de protéger complètement une surface d'attaque. Quel(s) facteur(s) affecte(nt) le plus votre organisation ?



Selon les résultats obtenus, les facteurs qui affectent le plus votre organisation en ce qui concerne la protection de la surface d'attaque sont les suivants :

- **Méconnaissance de l'ensemble du périmètre interne et externe à protéger (cartographie) : 69,6 %.** Cela indique que la connaissance complète de toutes les zones à risque, tant à l'intérieur qu'à l'extérieur de l'organisation, est un défi majeur. Il est important d'avoir une vision claire et précise de l'ensemble du périmètre à protéger afin de mettre en place des mesures de sécurité appropriées.

💡 Il existe plusieurs solutions pour remédier à cette méconnaissance des zones à risque : cartographier le système d'information, réaliser des audits de sécurité, mettre en place une équipe interne dédiée à la veille et à la surveillance des menaces, installer et configurer des outils de surveillance et de détection des menaces, sensibiliser les salariés aux bonnes pratiques, élaborer un plan de gestion de crise, etc.

- **Manque de ressources humaines pour appliquer les plans de remédiation définis : 68,4 %.** Cela signifie que le manque de personnel qualifié et en nombre suffisant pour mettre en œuvre les plans de remédiation est un obstacle majeur. Une équipe compétente et correctement dimensionnée est nécessaire pour appliquer efficacement les mesures de sécurité et remédier aux vulnérabilités identifiées.

💡 Une approche pour faire face au manque de compétences en cybersécurité réside dans l'automatisation. Néanmoins, ce n'est pas chose aisée et cela nécessite une expertise particulière. Heureusement, il est possible de constituer une équipe d'experts pour une durée déterminée ou de faire appel à un service de sécurité managée, ce qui facilitera la mise en œuvre sans nécessiter un engagement permanent en termes de ressources humaines et de budget au sein de l'organisation.

- **Manque de tableaux de bord de pilotage permettant une priorisation efficace : 48,1 %.** Cela souligne l'importance des tableaux de bord de pilotage qui fournissent une vue d'ensemble des risques et permettent une priorisation efficace des mesures de sécurité. L'absence de ces outils peut entraver la capacité de l'organisation à hiérarchiser et à traiter les risques de manière optimale.

💡 Un tableau de bord de la sécurité des systèmes d'information (TDBSSI) offre la possibilité d'obtenir, à divers échelons décisionnels (à savoir pilotage et opérationnels) une vue d'ensemble condensée de la situation en matière de sécurité, aussi bien dans ses aspects techniques que fonctionnels (englobant la prise en compte des risques, l'efficacité de la politique de sécurité, le suivi des audits, des mesures prises, et les alertes émises…).

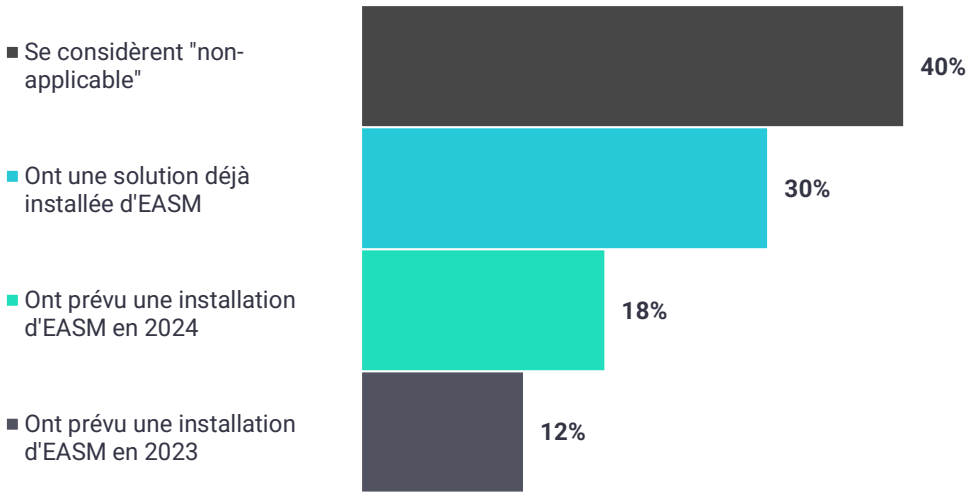
- **Manque de budget : 24,1 %.** Bien que ce pourcentage soit moins élevé que les autres facteurs, il est néanmoins significatif. Un manque de budget peut limiter les investissements dans les solutions de sécurité appropriées, les ressources humaines qualifiées et d'autres mesures de protection. Il est important de garantir un budget adéquat pour soutenir efficacement la protection de la surface d'attaque.

💡 Investir, oui mais par où commencer ? Nous vous recommandons d'adopter les cinq piliers de la cyber-hygiène : Identifier - Protéger - Détecter - Répondre - Récupérer. En d'autres termes, cela implique de bien comprendre ses actifs et les risques liés à ses activités, de mettre en place des solutions et des mesures de protection, de partir du postulat de départ qu'un risque peut arriver, de réfléchir à sa capacité à le détecter et à réagir en cas de besoin, d'avoir une politique de sauvegarde et des backups réguliers pour être en capacité de relancer l'activité après un incident.

Lorsqu'on pense à la surface d'attaque, on a tendance à y associer des solutions de type *External Surface Attack Management (EASM)*. Bien que les solutions d'EASM et de CAASM soient toutes deux importantes, elles répondent à des objectifs différents. Les solutions CAASM concernent tous les actifs, généralement collectés par l'intégration avec des sources de données tierces (VM, CMDB, etc.), tandis que les solutions EASM se concentrent sur les actifs externes collectés par DNS, Whois, les données de site web et les requêtes TLS, RBL.

Les organisations qui ne maîtrisent pas (encore) la totalité de leur périmètre sont malgré tout nombreuses à s'intéresser aux solutions d'EASM (External Attack Surface Management). **60 %** d'entre elles se sont dotées d'une solution d'EASM ou prévoient de le faire.

Sur les 55 entreprises qui ne maîtrisent pas leur périmètre :



Ces résultats montrent que malgré le fait de ne pas maîtriser entièrement leur périmètre, de nombreuses entreprises reconnaissent l'importance des solutions d'EASM pour la gestion de leur surface d'attaque externe. Un pourcentage significatif d'entre elles a déjà mis en place une solution d'EASM, tandis que d'autres prévoient de le faire dans un avenir proche.

La surface d'attaque représente la compilation des vulnérabilités d'un environnement, celles par lesquelles un pirate pourrait potentiellement pénétrer un système. Plus le nombre de vulnérabilités est élevé (donc plus la surface est étendue), plus les risques d'une attaque deviennent considérables.

Les intrusions peuvent se décliner en diverses formes, notamment :

- l'intrusion sur un serveur mal sécurisé ;
- l'accès distant à une base de données mal sécurisée ;
- l'exécution de code malveillant.

Le nombre d'attaques envisageables correspond au nombre de vulnérabilités présentes ; il est donc crucial de sécuriser autant de ces points faibles que possible. La première étape consiste à connaitre sa propre surface d'attaque, l'un des éléments clés pour garantir sa cybersécurité, et pour améliorer sa posture de sécurité en ligne.

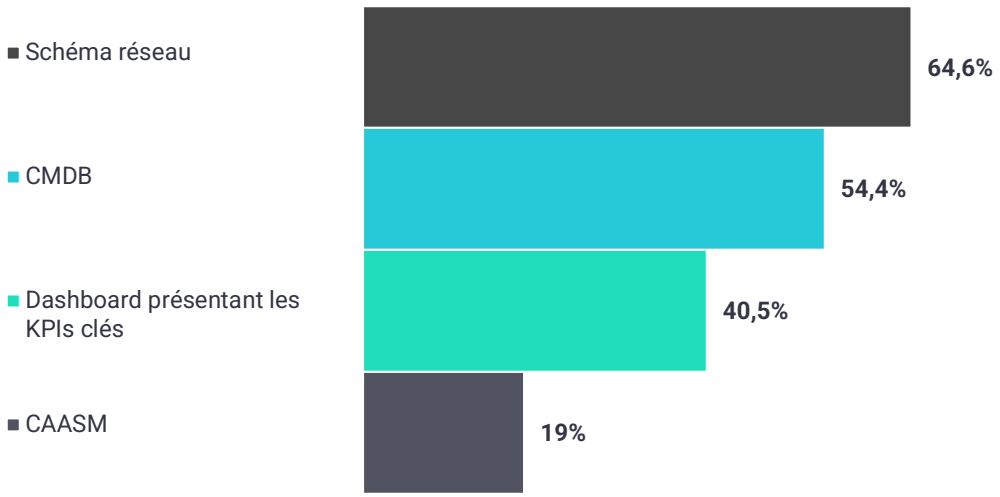
Les solutions d'EASM offrent aux entreprises des outils et des informations pour identifier, évaluer et prendre des mesures appropriées concernant les vulnérabilités potentielles.

Il est encourageant de constater que de plus en plus d'entreprises reconnaissent cette nécessité et s'engagent à mettre en place des solutions d'EASM pour renforcer leur posture de sécurité et protéger leur surface d'attaque.

Bien souvent, les organisations disposent déjà d'un ou plusieurs outils pour partager la connaissance de leur parc informatique. Parmi les outils utilisés par les répondants, les outils les plus fréquemment cités sont un schéma réseau, une CMDB (Configuration Management DataBase) et un tableau de bord présentant les KPIs clés.

La CMDB est un outil essentiel pour centraliser toutes les données des actifs informatiques et partager une vision commune du parc informatique au sein de l'organisation, ce qui permet une meilleure gestion des configurations et une amélioration de la sécurité. De ce fait, elle facilite l'identification des liens de dépendance existants entre les différents actifs.

Dans votre organisation, quel(s) est(sont) le(s) outil(s) que vous utilisez pour partager une vision commune de votre parc informatique à vos équipes ?

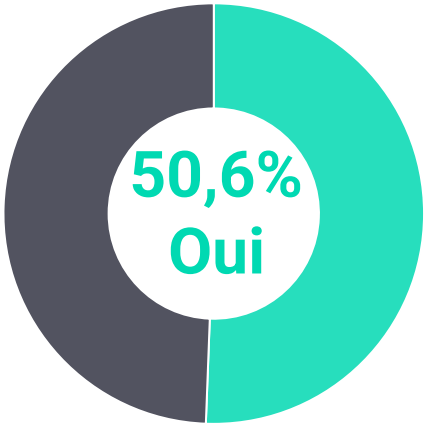


Ces chiffres indiquent que la majorité des organisations disposent déjà d'outils pour partager la connaissance de leur parc informatique avec leurs équipes. Les schémas réseau, les CMDB et les tableaux de bord de KPIs clés sont les outils les plus couramment cités. Aussi, il est intéressant de noter que près d'un répondant sur cinq utilise également le CAASM, ce qui témoigne de l'importance accordée à la gestion de la surface d'attaque et à la maîtrise des actifs en matière de cybersécurité.

Ces outils permettent de fournir une vision d'ensemble du parc informatique, de ses configurations, de son architecture réseau et des indicateurs clés de performance. Ils contribuent ainsi à faciliter la communication, la collaboration et la prise de décision au sein des équipes chargées de la cybersécurité. Le CAASM en particulier se distingue en offrant une solution spécifique axée sur la gestion de la surface d'attaque et la protection des actifs critiques contre les menaces cyber.

Si la CMDB est citée par près d'une entreprise sur deux, il n'en reste pas moins très consommateur en « temps homme » (beaucoup plus consommateur de « temps homme » que les outils CAASM). Dans une période de pénurie de professionnels qualifiés en cybersécurité, cet élément revêt une importance toute particulière.

Portez-vous actuellement un projet de CMDB ?



Ces chiffres indiquent que plus d'une entreprise sur deux reconnaît l'importance d'une CMDB et travaille activement sur la mise en place d'un tel projet.

Cependant, près de la moitié des entreprises interrogées n'ont pas encore entrepris de projet de CMDB. Cela peut s'expliquer par divers facteurs, tels que des contraintes de ressources humaines ou financières, des priorités différentes ou une méconnaissance de l'importance de la CMDB.

Il est essentiel de noter que la mise en place d'une CMDB demande du temps, des ressources et une planification rigoureuse. Les entreprises qui n'ont pas encore lancé de projet de CMDB peuvent envisager de le faire à l'avenir afin de bénéficier des avantages que celle-ci peut offrir en termes de gestion de leur parc informatique.

Cependant, lorsqu'on interroge les professionnels ayant mené un projet de CMDB sur leur satisfaction vis-à-vis de cette solution, les résultats sont mitigés :

- *« sa maintenance relève de la conviction car partiellement manuelle » ;*
- *« c'est partiel » ;*
- *« oui mais insuffisance des capacités automatiques de collecte de données techniques » ;*
- *« moyennement, problématiques de mise à jour » ;*
- *« démarré il y a plusieurs années avec des résultats insuffisants » ;*
- *« problème de CMDB à jour » ;*
- *« trop basé sur du déclaratif » ;*
- *« non. Compliqué à maintenir (manuel) ».*

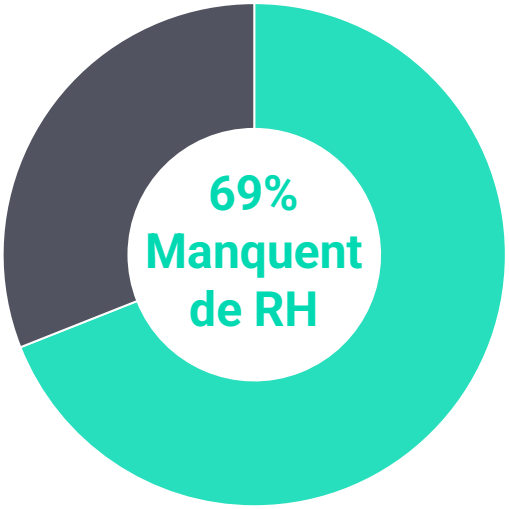
La CMDB est un outil traditionnellement issu de l'IT. À l'usage, cet outil se révèle insuffisant pour traiter des problématiques de sécurité et gagner en visibilité sur ses actifs numériques.

Cette absence d'automatisation des solutions CMDB est responsable de faibles taux d'adoption par les équipes. Lorsqu'on interroge les professionnels qui n'ont actuellement pas de projet CMDB en cours :

- *1/3 évoque la mise à jour manuelle comme explication à l'absence de projet CMDB ;*
- *38,5 % justifie cette absence de CMDB par le fait que les équipes IT et métiers ne l'utilisent pas ;*
- d'autre part, près de deux tiers (65 %) des entreprises qui n'ont pas de projet CMDB en cours manquent de RH (26 répondants). Elles ne sont que 35 % à ne pas manquer de RH (14 répondants).

L'élément humain apparaît aujourd'hui comme le critère le plus important pour constituer un inventaire complet et à jour. La mise en place d'une solution automatisée pourrait justement pallier ce problème.

Sur 43 entreprises ayant répondu « CMBD » à la question « Dans votre organisation, quel(s) est(sont) le(s) outil(s) que vous utilisez pour partager une vision commune de votre parc informatique à vos équipes ? » :



Ces résultats mettent en évidence l'impact de la CMDB sur la charge de travail des professionnels de la cybersécurité. Bien que la CMDB soit largement utilisée comme outil pour partager une vision commune du parc informatique, cela représente un défi supplémentaire pour les organisations surtout dans un contexte de pénurie de professionnels qualifiés en cybersécurité.

Le manque de ressources humaines peut entraîner des difficultés dans la gestion, la mise à jour et la maintenance de la CMDB. Cela peut également avoir un impact sur la capacité de l'équipe de cybersécurité à exploiter pleinement les informations contenues dans la CMDB pour prendre des décisions éclairées. En cause l'automatisation programmée par les RH et le fait d'avoir des outils automatisés et automatisables.

Il est donc essentiel pour les organisations de trouver des solutions pour optimiser l'utilisation de la CMDB, automatiser les processus et identifier les domaines où des améliorations peuvent être apportées afin de réduire la charge de travail liée à ce référentiel commun. Parallèlement, il est important de prendre des mesures pour attirer et former davantage de professionnels qualifiés en cybersécurité afin de combler la pénurie de talents dans ce secteur.

💡 Pour acquérir les compétences nécessaires pour définir, mettre en œuvre et exploiter une CMDB, voici des formations utiles :

- formations en gestion de configuration d'une CMDB : comprendre les principes fondamentaux, découvrir l'importance d'une CMDB et savoir comment la mettre en place ;
- certifications ITIL (Information Technology Infrastructure Library) : ITIL propose des certifications liées à la gestion des services informatiques, y compris la gestion d'une CMDB ;
- formations en gestion de projet : étant donné que la mise en œuvre d'une CMDB peut être un projet complexe, des compétences en gestion de projet sont utiles pour planifier, exécuter et suivre la mise en place de la CMDB ;
- formations proposées par des éditeurs de logiciels CMDB : si vous prévoyez d'utiliser des logiciels spécifiques pour votre CMDB, de nombreux éditeurs (comme GLPI-Project, Freshservice, ServiceNow) proposent des cours, des certifications et des formations pratiques en direct ou à la demande ;
- formations en ligne : il existe de nombreuses ressources en ligne, telles que des cours sur des plateformes d'apprentissage en ligne, des webinaires et des tutoriels ;

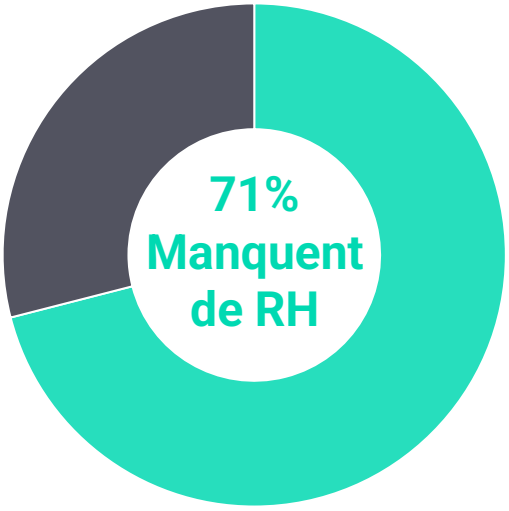
- formations continues : compte tenu de l'évolution constante de la technologie et des meilleures pratiques, la formation continue est importante pour rester à jour avec les nouvelles tendances et les avancées en matière de CMDB.

Sans RH, pas de tableaux de bord ?

Le manque de ressources humaines apparaît aujourd'hui comme le principal frein à la réalisation de tableaux de bord, puisqu'il est cité par plus des deux tiers des répondants (71 %), puisqu'il demande des compétences précises :

- connaissance en sécurité informatique : une solide compréhension des principes et concepts de base de la sécurité informatique est essentielle pour identifier les indicateurs clés de sécurité à surveiller ;
- maîtrise des outils de sécurité : une connaissance approfondie des outils de sécurité tels que les systèmes de détection d'intrusion (IDS), les pares-feux, les systèmes de gestion des informations et des événements de sécurité (SIEM) est cruciale pour collecter et analyser les données pertinentes ;
- compétences en analyse de données : la capacité à traiter, analyser et interpréter les données de sécurité est essentielle pour récolter des informations significatives à partir des indicateurs ;
- compétences en visualisation de données : savoir comment représenter visuellement les données sous forme de graphiques, diagrammes et autres éléments graphiques facilite la compréhension des tendances et des anomalies ;
- compréhension des risques et des menaces : une bonne compréhension des risques et des menaces spécifiques à votre environnement est nécessaire pour choisir les bons indicateurs à surveiller ;
- connaissance des normes et des cadres de référence : être familier avec les normes et cadres de référence de sécurité tels que ISO 27001, Framework NIST aide à définir des métriques appropriées ;
- compétences en communication : être en mesure de communiquer clairement et efficacement les informations de sécurité aux parties prenantes est essentiel pour que les tableaux de bord soient utiles et compréhensibles ;
- capacité à gérer les priorités : savoir identifier les indicateurs de sécurité les plus critiques et les plus pertinents en fonction des besoins de l'entreprise est important pour éviter une surcharge d'informations ;
- compétences en gestion de projet : la création et la maintenance de tableaux de bord peuvent être considérées comme des projets. Des compétences en gestion de projet aident à planifier, organiser et exécuter efficacement ces tâches ;
- curiosité et veille technologique : la sécurité informatique évolue constamment. Être curieux et au courant des dernières tendances et technologies de sécurité est nécessaire pour adapter les tableaux de bord aux nouvelles menaces.

Sur les 38 entreprises qui manquent de tableaux de bord :



La création, l'édition et le monitoring des tableaux de bord demandent du temps et des compétences spécifiques en matière d'analyse de données, de visualisation et de communication. Lorsque les ressources humaines sont insuffisantes, il devient difficile de recruter des profils capables de créer des tableaux de bord pertinents et exploitables.

Cette situation souligne l'importance de disposer d'un nombre suffisant de collaborateurs pour répondre aux besoins des organisations en matière de gestion des risques et à la mise en place d'outils de pilotage efficaces.

Il est essentiel pour les organisations de prendre des mesures pour attirer, former et retenir les profils cyber afin de renforcer la capacité à établir des tableaux de bord de pilotage adaptés à leurs besoins.

Le reporting est aujourd'hui principalement réalisé par des humains. Augmenter les ressources humaines permettrait-il de réaliser davantage de tableaux de bord ? Est-il possible de manquer de RH sans manquer de tableaux de bord ?

Le manque de ressources humaines est une réalité bien plus préoccupante que le manque de budget. Plus de deux tiers (69 %) des entreprises qui manquent de ressources humaines ne manquent pas de budget. Le manque de ressources humaines est tel qu'il ne saurait être comblé par une augmentation de budget.

Quelle importance accordez-vous aux indices de performance (KPIs) suivants dans votre stratégie de sécurité (note de 1 à 5) ?

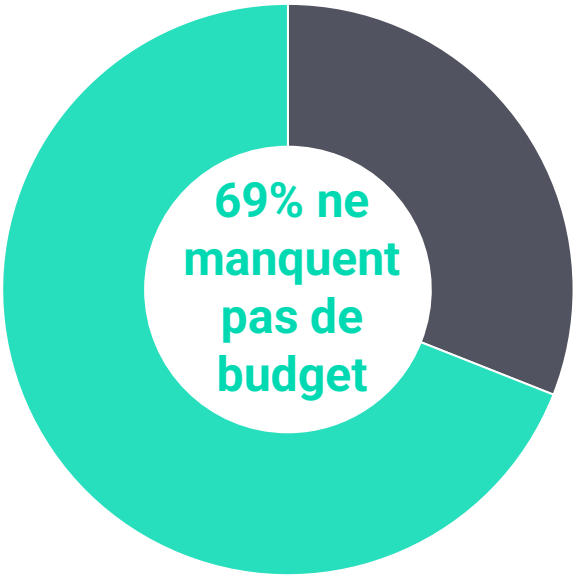
Nombre d'assets non couverts par votre EDR :
*79 % des répondants attribuent à cet indicateur de performance une note de **4 ou 5***

Nombre d'incidents :
*79 % des répondants attribuent à cet indicateur de performance une note de **4 ou 5***

Nombre de vulnérabilités résolues :
*79 % des répondants attribuent à cet indicateur de performance une note de **4 ou 5***

Temps moyen de résolution d'un incident :
*79 % des répondants attribuent à cet indicateur de performance une note de **4 ou 5***

Sur les 54 entreprises qui manquent de RH :



Ces résultats mettent en évidence une situation préoccupante où le manque de ressources humaines est plus problématique que le manque de budget. Même si certaines entreprises disposent d'un budget adéquat, elles ne parviennent pas à trouver les ressources humaines nécessaires pour combler leurs besoins.

Face à la pénurie de professionnels, le recrutement et la rétention de talents sont extrêmement difficiles. C'est pourquoi l'augmentation du budget ne résoudra pas automatiquement le problème du manque de ressources humaines.

Les organisations doivent adopter une approche holistique pour relever ce défi en investissant à la fois dans le recrutement et la formation de professionnels dans ce domaine.

La combinaison d'un budget adéquat et d'une équipe qualifiée en ressources humaines permettra aux organisations de renforcer leur posture et de faire face aux défis liés à ces métiers.

Le CAASM, une méthodologie émergente

Un besoin bien compris par les grandes entreprises

Les grandes entreprises semblent davantage conscientes de l'intérêt d'utiliser les outils CAASM pour partager une vision commune de leur parc informatique à leurs équipes ce qui souligne leur plus grande maturité en matière de gestion du risque cyber. Les entreprises qui utilisent déjà les outils CAASM ont une moyenne d'employés deux fois plus haute que les entreprises qui ne les utilisent pas.

Les entreprises qui utilisent déjà les outils CAASM se répartissent dans les secteurs suivants (par ordre d'importance décroissante) :

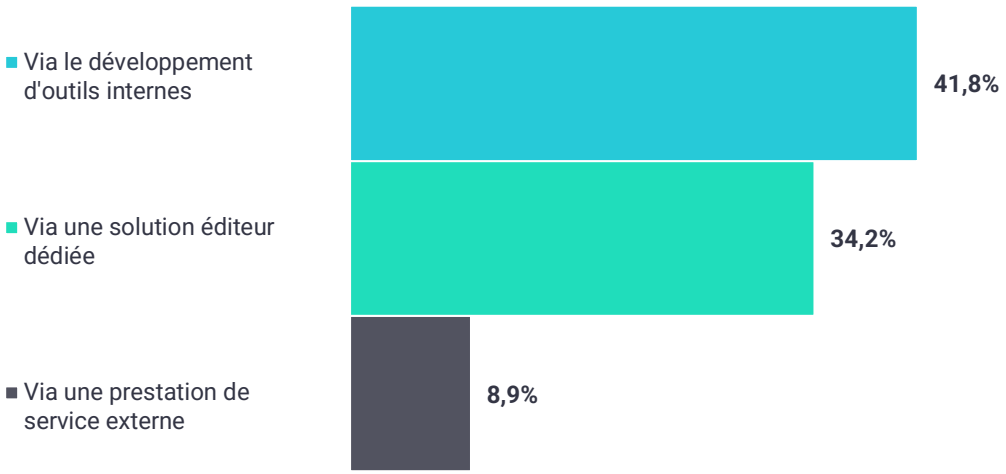
- industrie manufacturière ;
- secteur de la santé et médico-social ;
- administration publique et défense / Collectivités / Commerce ;
- information et communication.

Les outils « maison », un pis-aller ?

Conscientes de la nécessité de cartographier leur système d'information pour mieux le connaître et mieux le protéger, certaines entreprises essaient de le faire avec des outils « maison ».

Lorsqu'on interroge les entreprises sur la manière dont elles agrègent leurs données, le développement d'outils internes est la principale réponse citée.

Quelle est votre solution privilégiée pour consolider l'ensemble des données issues de vos solutions de sécurité ?



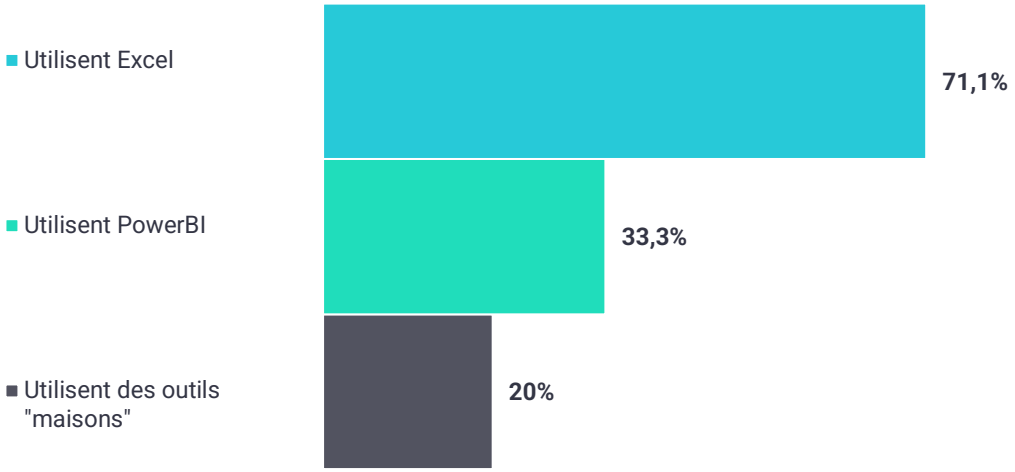
Ces résultats montrent que la majorité des organisations privilégient soit le développement d'outils internes, soit l'utilisation d'une solution éditeur dédiée pour consolider leurs données de sécurité. Cela témoigne de l'importance accordée à la consolidation des données pour une meilleure gestion de la sécurité informatique.

Le choix du développement d'outils internes peut permettre aux organisations de personnaliser la consolidation des données en fonction de leurs besoins métiers. Cependant, cela nécessite des ressources internes et du temps.

L'utilisation d'une solution éditeur dédiée offre une approche clé en main, permettant aux organisations de bénéficier de fonctionnalités avancées et d'adresser un maximum de cas d'usages et d'aller chercher de la valeur ajoutée. Cela peut être une option adéquate pour les organisations qui souhaitent une mise en œuvre plus rapide et une gestion simplifiée.

Enfin, une petite proportion des organisations optent pour une prestation de service externe pour la consolidation de leurs données. Cela peut être dû à un manque de ressources internes ou à une préférence pour externaliser cette tâche à des experts spécialisés.

Les entreprises ont des pratiques hétérogènes lorsqu'il s'agit de consolider leurs données via des outils internes. Parmi les entreprises qui agrègent leurs données en utilisant des outils internes :



Le manque de budget n'est pas en cause dans l'utilisation d'outils internes, puisque parmi les 33 entreprises qui développent des outils internes, 91 % ne manquent pas de budget.

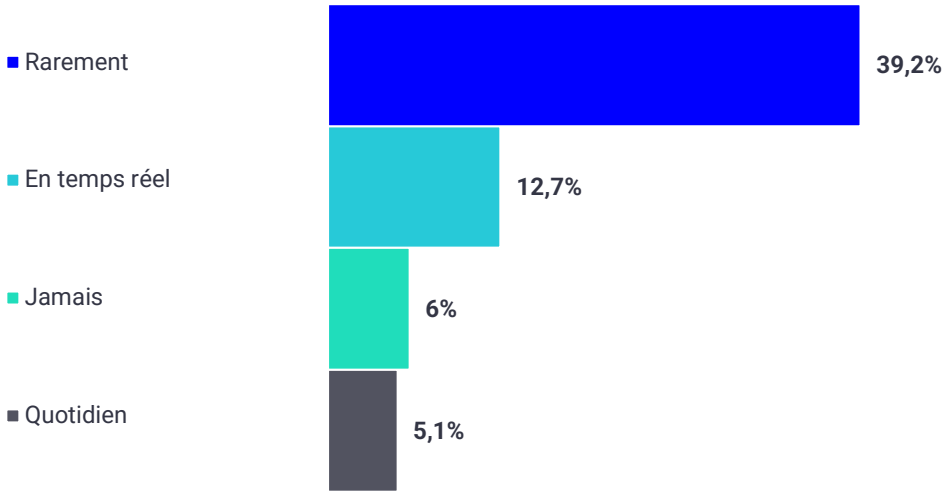
Ces réponses montrent que les entreprises qui utilisent des outils internes pour la consolidation de leurs données ont des préférences différentes dans la manière dont ils gèrent leur budget. Excel reste l'outil le plus largement utilisé, probablement en raison de sa familiarité et de sa disponibilité généralisée. PowerBI, Tableau, Oracle Business Intelligence et Kibana sont également populaires en tant que solutions de Business Intelligence prêtes à l'emploi.
Par ailleurs, les outils "maison" reflètent la volonté de certaines organisations de développer des solutions sur mesure pour répondre à leurs besoins liés à leur système d'information.

Revue de cartographie du SI : des attentes fortes en matière d'automatisation

L'étude fait ressortir une faible fréquence des revues de cartographie du SI.

La cartographie représente un outil essentiel pour la gestion efficace d'un système d'information. Elle offre la possibilité d'acquérir une compréhension exhaustive de tous les éléments qui le composent, en vue d'améliorer sa clarté et, par conséquent, un plus grand contrôle.

À quelle fréquence effectuez-vous une revue de votre cartographie du SI ?



Ces résultats montrent que la majorité des répondants n'effectuent pas de revues fréquentes de leur cartographie, avec 45,5 % d'entre eux qui le font rarement ou jamais. Cependant, une partie significative des répondants, soit 17,8 %, effectue des revues en temps réel ou quotidiennement, ce qui témoigne d'une routine proactive et régulière de la cartographie.

Pour les autres répondants, les revues de cartographie ont lieu de manière mensuelle, trimestrielle ou hebdomadaire.

L'automatisation constitue une attente forte. Lorsqu'on interroge les professionnels sur le facteur le plus fortement susceptible d'augmenter la fréquence de leur revue de cartographie, près d'un tiers répond « l'automatisation de la mise à jour » (19 sur 60).

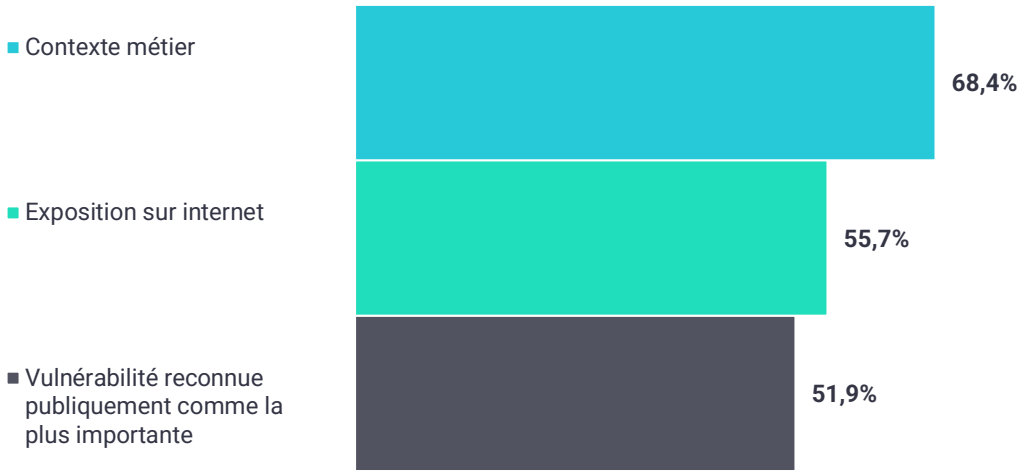
22 % des organisations utilisent le mot « automatisation » ou « dynamique ». Il s'agit d'ailleurs des organisations qui ont un fort taux de CMDB (70 %). Il existe donc aujourd'hui une demande forte d'automatisation de la part des organisations qui utilisent un outil de CMDB. La mise à jour de leur cartographie n'étant pas réalisée de manière automatique, les organisations qui ont recours à une CMDB ne revoient pas assez fréquemment leur cartographie.

Solutions et perspectives : les grands cas d'usage des outils CAASM

Les outils actuels (CMDB, EASM, scan de vulnérabilités) semblent insuffisants pour permettre aux organisations de protéger correctement leur surface d'attaque. Les organisations ont d'ailleurs une idée claire au sujet des précisions et des données supplémentaires dont elles aimeraient disposer pour mieux prioriser les assets porteurs de vulnérabilités qu'elles doivent patcher.

Quelles précisions / quelles données supplémentaires vous permettraient de mieux prioriser les assets porteurs de vulnérabilités à patcher ?

Les 3 facteurs devant ressortir sur la cartographie sont :



Ces 3 facteurs mettent en évidence l'importance de prendre en compte à la fois les aspects métier, les expositions sur Internet et les vulnérabilités reconnues publiquement lors de la création d'une cartographie d'un système d'information. En tenant compte de ces facteurs, les organisations peuvent mieux comprendre leur surface d'attaque et prioriser leurs efforts en matière de gestion des risques.

Les répondants accordent une grande importance à ces indicateurs de performance dans leur stratégie de sécurité. Ils cherchent à améliorer la couverture des actifs, à réduire le nombre d'incidents, à résoudre les vulnérabilités et à accélérer la résolution des incidents. En se concentrant sur ces aspects, les organisations peuvent renforcer leur posture de sécurité et atténuer les risques potentiels. Le point commun de ces différents indicateurs ? Ils peuvent tous être suivis à l'aide d'un logiciel CAASM.

Lorsque l'on regarde plus précisément, on se rend compte que les organisations équipées de CAASM suivent toutes le nombre d'assets non couverts par leur EDR sans surprise. Les organisations équipées répondent toutes qu'elles suivent cet indicateur.

Un EDR permet de détecter et bloquer les menaces connues et inconnues sur les terminaux en s'appuyant sur l'analyse comportementale, l'apprentissage automatique et la corrélation des événements. Il dispose de capacités de détection, d'investigation et de remédiation.

Si le niveau de maturité des répondants vis-à-vis des solutions CAASM est encore peu élevé, les professionnels interrogés ont en revanche des attentes sur les solutions leur permettant de réduire leur risque cyber.

Pour ce faire, les fonctionnalités suivantes proposées par les solutions CAASM vous permettraient-elles de réduire votre risque cyber (note de 1 à 5)

*Tableaux de bord facilitant la définition des priorités dans le cadre d'un plan de remédiation : 49 % des répondants attribuent à cette fonctionnalité une note de **4 ou 5***

Définition de zones vitales ou critiques pour votre organisation à surveiller :
*49 % des répondants attribuent à cette fonctionnalité une note de **4 ou 5***

Mise en avant des assets non couverts par votre EDR :
*49 % des répondants attribuent à cette fonctionnalité une note de **4 ou 5***

Détection automatisée de nouveaux assets :
*49 % des répondants attribuent à cette fonctionnalité une note de **4 ou 5***

Ces résultats révèlent que ces fonctionnalités proposées par les solutions CAASM sont perçues comme utiles pour réduire le risque cyber. Les tableaux de bord, la définition de zones vitales, la mise en avant des assets non couverts et la détection automatisée de nouveaux assets sont autant d'éléments qui contribuent à améliorer la visibilité, la priorisation et la gestion des risques au sein des organisations.

Avec l'évolution rapide du paysage cyber, les RSSI et DSI des organisations ont aujourd'hui à leur disposition d'autres sources de données autres que la CMDB, l'EASM et le scan de vulnérabilités. L'étude met donc en lumière différents points de vue entre, d'une part, les besoins exprimés par les organisations pour réduire leur risque cyber, et d'autre part, les fonctionnalités proposées par les outils CAASM. Elle conforte l'utilité et la pertinence du CAASM pour identifier les faiblesses et réduire le risque de cyber-attaques par une meilleure gestion des actifs et l'éventuelle prise de mesures correctives de sécurité ciblées.

Conclusion

En plus d'audits ou de tests d'intrusion pour évaluer la sécurité d'un système d'information (SI) et les processus de gestion des alertes, les résultats de l'étude soulignent les avantages d'une solution CAASM pour automatiser la collecte, l'agrégation et l'exploitation des données de sécurité, à l'aide d'une cartographie du système d'information. Cette étude révèle la forte appétence des non-utilisateurs des outils CAASM pour certaines fonctionnalités. L'automatisation de la cybersécurité opérationnelle arrive en tête des attentes des sondés. Dans la plupart des organisations, les données sont bien disponibles, mais restent inexploitées. L'habitude d'agréger manuellement de grandes quantités de données est encore bien présente contrairement à des solutions de type SIEM / SOC.

En effet, l'automatisation permet de gagner en efficacité et en précision, en évitant les tâches fastidieuses de traitement manuel et de croisement des données. Les organisations pourraient ainsi mieux exploiter leurs ressources et se concentrer sur l'analyse des résultats, accélérer les prises de décisions et prioriser les actions.

Il est donc essentiel de sensibiliser les organisations à l'importance de l'automatisation et de les encourager à adopter des solutions CAASM pour tirer pleinement parti des données de leur système d'information et les utiliser à bon escient.

En définitive, cela permettrait d'améliorer la visibilité, la réactivité et l'efficacité des mesures de sécurité pour prévenir et réduire le risque cyber menaçant les données les plus critiques. Ces menaces sont une réalité à laquelle toutes les organisations font face et pour lesquelles elles doivent prendre des mesures d'atténuation des risques.