



LIVRE BLANC

Maîtriser la cybersécurité grâce à un centre d'opérations de sécurité efficace

Découvrez quel modèle de SOC est le mieux adapté aux besoins de votre organisation.

Résumé

Le paysage de la cybersécurité est en constante évolution, avec des menaces toujours plus sophistiquées et omniprésentes. Dans ce contexte, les centres d'opérations de sécurité (SOC) sont essentiels, car ils permettent aux organisations de détecter, d'analyser et de répondre rapidement aux cyber incidents. Encore faut-il savoir choisir le modèle de SOC le mieux adapté à chaque organisation — interne, hybride ou externalisé — et s'assurer ensuite d'utiliser les bons indicateurs pour mesurer ses performances afin de garantir une sécurité continue tout en restant en phase avec les objectifs commerciaux.

Le rôle d'un SOC dans le paysage de la cybersécurité d'aujourd'hui

L'avènement du numérique s'est accompagné d'une recrudescence des cybermenaces, et les cybercriminels et les acteurs soutenus par des États sont désormais en mesure de mener des attaques sophistiquées. Les tendances actuelles indiquent une réduction inquiétante du temps séparant l'intrusion initiale du déploiement du ransomware, qui est aujourd'hui **de seulement 2 jours en moyenne**². Qui plus est, la pénurie de personnel compétent dans le secteur de la cybersécurité ne faiblit pas, ce qui complique davantage la mise en place et la gestion d'un SOC interne.

Un SOC est une fonction organisationnelle dédiée à la gestion des processus d'identification, d'investigation et de remédiation des incidents de sécurité. Au nombre de ses missions spécifiques figurent la gestion des actifs, des changements, des vulnérabilités, des événements de sécurité, des incidents, ainsi que l'intégration des renseignements sur les menaces et diverses activités de DevOps telles que l'automatisation et l'assurance qualité. Bien que les SOC ne contrôlent pas tous les aspects de la sécurité d'une organisation, ils jouent un rôle crucial dans la coordination de leur réponse aux problèmes de cybersécurité. La mission et les objectifs spécifiques d'un SOC peuvent varier considérablement, selon la tolérance au risque de l'organisation, le secteur d'activité, le niveau de maturité et les outils et processus qu'elle utilise.

63 % des organisations

Sont victimes d'un ransomware en raison d'un manque de personnel ou de compétences¹.

Pénurie de talents

La pénurie de personnel qualifié continue de peser lourdement sur le secteur de la cybersécurité.

Types de modèles de SOC

Les organisations peuvent choisir parmi plusieurs modèles de SOC, chacun disposant de caractéristiques et d'avantages propres :



Les SOC internes se retrouvent généralement dans des organisations bien financées qui sont en mesure de soutenir des opérations continues avec une équipe dédiée. Ces SOC sont parfois amenés à externaliser certaines fonctions spécialisées, telles que les tests d'intrusion, la chasse aux menaces par des experts ou les renseignements sur les menaces. Les grandes organisations ou celles qui sont dispersées géographiquement peuvent utiliser un modèle à plusieurs niveaux dans lequel plusieurs SOC fonctionnent sous une structure de commandement unifiée.



Les SOC hybrides sont de plus en plus populaires. Ils combinent des ressources internes et des services externes pour créer une fonction de sécurité sur mesure dans le cadre d'un modèle de partenariat. Le fournisseur de services de cybersécurité est généralement responsable de la surveillance 24/7, du triage des alertes, des investigations sur les incidents, de la chasse aux menaces et de la fourniture d'un soutien de la part d'experts. Cette solution permet à l'équipe interne de maximiser ses ressources grâce à des activités telles que l'architecture et la conception de la sécurité, la gestion des politiques et de la conformité, l'atténuation des risques, la formation à la sensibilisation à la sécurité et l'exécution d'actions de réponse lorsque l'organisation préfère confier les tâches de remédiation à son équipe interne. La flexibilité qui en découle et la possibilité de pallier la pénurie de compétences et les contraintes budgétaires rendent cette solution particulièrement intéressante.



Un SOC entièrement externalisé est un service tiers qui fournit des capacités complètes de surveillance et de réponse aux menaces. Les organisations qui ont besoin de mettre rapidement en place un SOC de base sans disposer de l'expertise interne nécessaire peuvent opter pour ce modèle, en accordant leur confiance à un fournisseur de services MDR (Managed Detection and Response) reconnu. L'organisation peut permettre au fournisseur externe de s'intégrer à ses technologies informatiques et de sécurité existantes afin qu'il puisse bénéficier d'une visibilité étendue sur l'ensemble de l'environnement et coordonner ainsi les activités de réponse aux incidents.

Le saviez-vous ?

88 % des attaques de ransomware sont déployées en dehors des horaires de bureau classiques².

Quel modèle vous convient le mieux ?

Déterminer le modèle de SOC le plus adapté à votre organisation dépend de plusieurs facteurs, y compris votre profil de risque global. Aussi est-il impératif d'évaluer le niveau de risque acceptable de votre organisation par rapport au budget que vous êtes prêt à consacrer à la cybersécurité. Plusieurs considérations clés entrent en jeu, notamment :

1

Les contraintes de ressources internes (disponibilité d'expertise ou de personnes/capacité)

2

L'équilibre entre ce qui doit être détenu en interne et ce qui doit être externalisé

3

La maturité actuelle de vos opérations de sécurité

4

Les difficultés liées au recrutement, à la formation et à la rétention du personnel clé possédant des compétences spécialisées

5

La nécessité d'un engagement continu envers les technologies émergentes et de rester en avance sur l'évolution constante du paysage des menaces et des techniques des adversaires actifs.

6

Les dépendances interdépartementales vis-à-vis des services informatiques, juridiques, de gestion des risques, de conformité et d'autres départements commerciaux.

Quel que soit le modèle que vous choisissez, il est important de réaliser une analyse de rentabilité, afin de justifier le modèle et les ressources indispensables à la viabilité du SOC. Des évaluations régulières des capacités de votre SOC sont également cruciales pour garantir qu'il est conforme à la conception et aux objectifs opérationnels prévus.

La plupart des organisations sont confrontées à une pénurie de personnel qualifié en matière de cybersécurité, et nombre d'entre elles ne disposent tout simplement pas du budget nécessaire pour mettre en place et maintenir un SOC interne fonctionnant 24 h/24 et 7 j/7. Les RSSI expérimentés savent également combien il est précieux de conserver un contrôle stratégique sur leurs opérations de cybersécurité et, par extension, sur la pérennité de leur organisation, en maintenant la supervision et le contrôle.

Avantages d'un modèle de SOC hybride

- ✓ Le modèle de SOC hybride combine efficacement les avantages des approches internes et externalisées. Il permet aux organisations de tirer parti de l'expertise et de l'efficacité d'un fournisseur tiers tout en maintenant un niveau de personnalisation et de contrôle sur leurs opérations de sécurité.
- ✓ L'un des principaux avantages d'un SOC hybride est l'accès à des experts en sécurité chevronnés et à des renseignements sur les menaces validés. Ces professionnels font partie d'un vivier de talents plus large, continuellement exposé à un large éventail de menaces, ce qui leur permet de rester à la pointe des derniers développements dans le domaine de la cybersécurité. Difficile pour une équipe interne autonome de rivaliser avec une telle expérience, et une telle portée, compte tenu de l'évolution rapide du paysage des menaces.
- ✓ De plus, s'associer à un fournisseur tiers garantit une couverture continue — 24/7, 365 jours par an — y compris les nuits, les week-ends et les jours fériés, moments au cours desquels les équipes internes sont parfois amenées à se déconnecter.
- ✓ Un SOC hybride peut réduire considérablement la fatigue liée aux alertes en aidant les organisations à affiner leurs systèmes de détection, ce qui permet ainsi de réduire le temps moyen de réponse (MTTR) aux incidents. Les organisations peuvent également faire l'économie des frais substantiels inhérents à la recherche dédiée sur les menaces, dans la mesure où leurs partenaires externes s'en chargeront à leur place, et ajouteront en permanence de nouvelles capacités de détection à mesure que celles-ci seront développées.
- ✓ Un autre avantage réside dans la capacité de concentrer les ressources internes sur les questions fondamentales en matière d'informatique, de technologie et de conformité, et de confier au partenaire SOC la gestion des incidents de cybersécurité. Cette répartition des tâches permet une allocation plus efficace des ressources et des expertises. Elle peut également permettre à d'autres départements de se concentrer sur leurs responsabilités supplémentaires liées à la sécurité.
- ✓ La formation en cybersécurité, qui s'avère parfois coûteuse et chronophage, est optimisée dans un modèle hybride. Le fournisseur externe s'assure que son personnel est à jour sur tous les aspects de la cybersécurité : des analyses forensiques et logiciels malveillants à la réponse aux incidents en passant par la sécurité du cloud. Ainsi, les membres de l'équipe interne n'ont plus la lourde tâche de se tenir au fait de tous les aspects de la cybersécurité et peuvent se concentrer sur les domaines les plus pertinents pour leur entreprise.
- ✓ Le modèle de SOC hybride offre également la flexibilité nécessaire pour prioriser les opérations en fonction de la tolérance au risque de l'organisation et pour adapter les méthodologies de réponse en conséquence. Il est ainsi possible de mettre en place des mesures de sécurité plus efficaces et mieux ciblées. De plus, les économies de coûts associées à un SOC hybride en font une option attrayante non seulement pour les petites et moyennes entreprises, mais aussi pour les grandes organisations qui souhaitent externaliser certaines fonctions de sécurité.

Mesurer l'efficacité du SOC

Quel que soit le modèle qu'il vous faut, pour évaluer l'efficacité d'un SOC, il est essentiel d'employer un ensemble de métriques qui sont en phase avec le paysage de la sécurité et l'efficacité des ressources du SOC retenu. Les indicateurs suggérés ci-dessous, ainsi que d'autres, peuvent être résumés dans un tableau de bord pour afficher des décomptes en temps réel, ainsi que des statistiques hebdomadaires, mensuelles et trimestrielles qui permettent de suivre les tendances au fil du temps, en mettant l'accent sur la réactivité du SOC et la qualité des investigations.

Pour ce qui est du paysage de la sécurité, ces indicateurs doivent fournir des informations sur l'étendue et le volume des menaces potentielles, les points faibles de l'organisation et l'exposition globale au risque. Il peut s'agir, par exemple, du volume d'emails suspects ou malveillants reçus, du nombre de tentatives d'analyse et d'exploitation de faille de sécurité visant des systèmes externes, ou encore du nombre d'incidents de sécurité par origine.

En ce qui concerne l'efficacité du SOC, les indicateurs doivent permettre de suivre les performances par rapport aux objectifs déclarés en matière de politique de sécurité et de posture, lesquels sont liés à des résultats commerciaux tels que la réduction des risques et la conformité réglementaire. Il peut s'agir de la réactivité et de la qualité des investigations, temps consacré par le personnel de sécurité à diverses activités, du nombre d'incidents par catégorie de conformité et de la quantité de travail d'ingénierie liée à la réduction de la surface d'attaque. Les indicateurs clés incluent également le temps de triage des investigations, le nombre d'investigations ayant donné lieu à des actions correctives, le nombre d'actions correctives issues de chasses proactives aux menaces, et le nombre de vulnérabilités corrigées, classées par gravité.

En surveillant régulièrement ces données, les organisations peuvent s'assurer que leur SOC fonctionne non seulement de façon optimale, mais améliore également la posture de sécurité globale et favorise la réalisation des objectifs commerciaux.

Les indicateurs devraient :

- Fournir un aperçu de l'étendue et du volume des menaces potentielles
- Trouver les points de vulnérabilité d'une organisation
- Montrer l'exposition globale au risque
- Suivre la performance par rapport aux objectifs de politique et de posture déclarés

Indicateurs clés :

- Temps de triage des investigations
- Nombre d'investigations ayant donné lieu à des actions correctives
- Nombre d'actions correctives basées sur des chasses aux menaces proactives
- Nombre de vulnérabilités corrigées, classées par gravité



Trouver une solution de SOC avancée

Chaque entreprise est unique, et présente des niveaux de maturité en matière de sécurité qui lui sont propres. Pour faire face à un paysage des menaces en constante évolution, l'accès à un SOC compétent est indispensable pour toute organisation qui prend au sérieux la question de la cybersécurité. Que les organisations choisissent de développer des capacités internes, de travailler avec un fournisseur externe ou d'adopter une approche hybride, nouer le bon partenariat peut garantir à la fois une défense efficace et un alignement avec les objectifs commerciaux.

De nombreuses entreprises se tournent vers des modèles de SOC hybrides ou entièrement managés pour faire face à la pénurie de personnel qualifié, aux contraintes budgétaires et à la complexité croissante des cybermenaces. Ces modèles offrent flexibilité, expertise et une couverture 24/7, permettant aux équipes internes de se concentrer sur des initiatives stratégiques, tandis que des partenaires de confiance assurent des opérations de sécurité évolutives.

[Sophos MDR](#) est l'illustration parfaite de la force de cette approche. Avec des formules à plusieurs niveaux conçues pour répondre aux besoins des organisations à chacune des étapes de leur parcours de cybersécurité, Sophos délivre des capacités avancées de détection, d'investigation et de réponse aux menaces adaptées aux besoins de chaque entreprise. Que ce soit pour soutenir une équipe SOC interne ou agir en tant que partenaire entièrement externalisé, Sophos MDR améliore la visibilité et la réponse aux menaces, aidant les organisations à renforcer leurs défenses et à protéger ce qui compte le plus.

¹ [Rapport Sophos « L'état des ransomwares 2025 »](#)

² [Rapport Sophos Active Adversary 2025](#)



Apprenez-en plus sur nos
services MDR (Managed
Detection and Response) sur
www.sophos.fr/mdr

Sophos France

Tél. : 01 34 34 80 00

Email : info@sophos.fr