formind

6 critères essentiels pour faire le choix d'un prestataire de SOC managé

Édito

Réconcilier technologie et accompagnement humain : les clés de la réussite d'un SOC

Les attaques informatiques ne cessent de se complexifier et les réseaux de pirates se multiplient et s'organisent. 45% des répondants à une récente enquête du CESIN[1] déclarent avoir détecté une cyberattaque réussie.

Le phénomène de "cloudification" des infrastructures IT, la démocratisation du télétravail, la multiplication des appareils connectés et le *shadow IT* constituent autant de portes d'entrée pour les attaquants modernes. Face à l'ampleur du phénomène, la question n'est plus de savoir si vous allez vous faire attaquer, mais à quel moment cela se produira et si vous serez suffisamment armé pour y faire face.

Partant du postulat que toute interaction au sein du système d'information (SI) est susceptible de se traduire par une compromission, l'approche *Zero Trust* représente un changement de paradigme inévitable pour faire face à cette nouvelle réalité. La mise en place d'un SOC (*Security Operation Center*) s'inscrit dans cette logique consistant à ne jamais faire confiance à qui ou quoi ce soit. Axé sur la supervision des actifs et la détection des attaques avant qu'elles ne mettent en péril l'activité, le **SOC Formind** s'articule autour d'équipes expertes qui orchestrent les opérations de cybersécurité, en s'appuyant notamment sur des outils de *Security Information and Event Management* (SIEM) performants tels que **Microsoft Sentinel**, afin de détecter très rapidement les attaques tout en écartant les faux positifs.

Si la pertinence d'un SOC ne fait aucun doute, la mise en œuvre de ces services peut être entravée par des considérations économiques, des raisons organisationnelles ou la rareté des compétences d'analystes. Un SOC managé tel que celui de **Formind**, basé sur le SIEM **Microsoft Sentinel**, constitue une solution adaptée pour surveiller votre SI, poser les premières briques de votre stratégie de défense et évoluer si vous le souhaitez vers un SOC interne.

Pour initier une telle démarche, le prisme technique doit aller de pair avec un accompagnement humain. Votre partenaire doit s'appuyer sur les meilleures technologies du marché, mais également être en mesure de faire progresser vos équipes. Comment s'assurer de la pertinence des méthodes et outils mis à disposition par votre prestataire de SOC managé ? **Formind** a répertorié dans cet ebook 6 critères afin d'éclairer vos choix.

1. 8ème édition du baromètre annuel du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique)

01 Exploiter la combinaison XDR + SIEM pour une détection précoce des menaces

Selon le 8ème baromètre du CESIN, les entreprises utilisent en moyenne 14,9 solutions, l'EDR (*Endpoint Detection & Response*) arrivant en tête, suivi de près par l'authentification multi-facteurs et le scanner de vulnérabilité. Votre prestataire doit déployer les bons outils tout en limitant le nombre de technologies afin d'en maîtriser tout leur potentiel.

Pour **Charles Melin, Directeur SOC & CERT et associé chez Formind**, "aujourd'hui, la première brique d'un SOC est l'EDR". Cependant, pour aller au-delà de la protection des identités et des endpoints gérés par l'EDR (terminaux des utilisateurs, serveurs, etc.), l'approche "Extended Detection and Response" (XDR), alliée à un SIEM tel que **Microsoft Sentinel**, représente une avancée significative.

La stratégie de **Formind** vise à unifier les alertes de l'EDR avec celles émanant d'autres dispositifs de sécurité (NDR, SIEM, etc.) au sein du XDR. "Notre démarche consiste à déployer le XDR en aval de l'EDR dès le début du projet, afin d'anticiper l'extension des périmètres de sécurité" précise le directeur SOC & CERT.

Quant au NDR (*Network Detection and Response*), "il offre une nouvelle perspective sur les menaces de sécurité, permettant d'identifier des chemins jusque là invisibles, notamment ceux associés au *shadow IT*" indique **Charles Melin**. Des fonctionnalités telles que l'analyse du trafic réseau et l'inspection en temps réel des communications réseau permettent aux solutions NDR de détecter et d'étudier les menaces, les comportements anormaux et les activités à risque sur l'intégralité du réseau.

L'orchestrateur, pièce maîtresse du SOC : Les bénéfices du SIEM Microsoft Sentinel

Parmi les différentes technologies exploitées dans le cadre d'un SOC, l'orchestrateur **Microsoft Sentinel** joue un rôle décisif : il pilote les outils de sécurité et donne une cohérence à l'ensemble de la démarche.

4 raisons de s'appuyer sur Microsoft Sentinel dans le cadre d'un SOC

1. Collecter des données à l'échelle du cloud — sur tous les utilisateurs, appareils, applications et infrastructures, à la fois sur site et dans plusieurs clouds.
2. Détecter les menaces précédemment découvertes et minimiser les faux positifs à l'aide d'analyses et de renseignements inégalés sur les menaces de Microsoft.
3. Enquêter sur les menaces avec l'IA et traquer les activités suspectes à grande échelle, en exploitant des décennies de travail sur la cybersécurité chez Microsoft.
4. Répondre rapidement aux incidents grâce à l'orchestration intégrée et à l'automatisation des tâches courantes.

Accessible en mode SaaS, Microsoft Sentinel demande peu de configuration et de maintenance. Très abordable en l'absence de logs unitaires, il dispose d'une puissance comparable aux grands outils SOAR[2] du domaine. ❞

Charles Melin,
Directeur SOC & CERT
et associé Formind

Conçue en environnement Microsoft, cette solution SIEM intelligente s'intègre en une heure et prend place naturellement dans les environnements clients existants (Azure, Office 365, etc.), ce qui simplifie la surveillance et la gestion des environnements clients utilisant déjà ces services.

En tant que SIEM cloud natif, **Microsoft Sentinel** est 48% moins cher et 67% plus rapide à déployer que les anciens SIEM sur site[3].

2. Security Orchestration, Automation, and Response (SOAR)

3. Selon une étude Forrester : "*The total economic impact of Microsoft Azure Sentinel*"

02 Un accompagnement pour monter en compétences sur les sujets cyber

Un examen attentif des services proposés par les partenaires SOC fait souvent ressortir un manque de visibilité sur la gestion des alertes et des incidents ainsi qu'un manque d'évolutivité et de prise en compte des changements de l'organisation client. "Les experts SOC doivent vous accompagner dans vos problématiques de surveillance et de détection des menaces grâce à des points de suivi réguliers et opérationnels" souligne Charles Melin.

Pour cela, **Formind** a fait le choix de mettre en place des comités de pilotage et d'amélioration opérationnelle afin de faire progresser les équipes sur la posture de sécurité à adopter.

> *De nombreuses organisations débutent dans la cybersécurité avec des équipes généralistes, en mettant l'accent sur les outils de protection plutôt que de détection. Travailler avec un prestataire de SOC managé permet de faire monter les équipes en compétence. Ensemble, le prestataire et l'entreprise vont peu à peu co-construire une cellule opérationnelle en charge de la détection. Des process vont se mettre en place au sein de l'organisation, des pratiques vont émerger et le niveau de maturité augmentera progressivement.*

Charles Melin,
Directeur SOC & CERT
et associé Formind

En débutant par un SOC externalisé, vous pouvez ainsi évoluer vers un mode de gestion hybride. Puis, selon les capacités budgétaires et la capacité à mobiliser vos équipes (notamment lors des astreintes en 24/7) vous aurez le choix d'évoluer vers une gestion internalisée de votre SOC. Quoi qu'il en soit, votre partenaire doit être un accompagnateur.

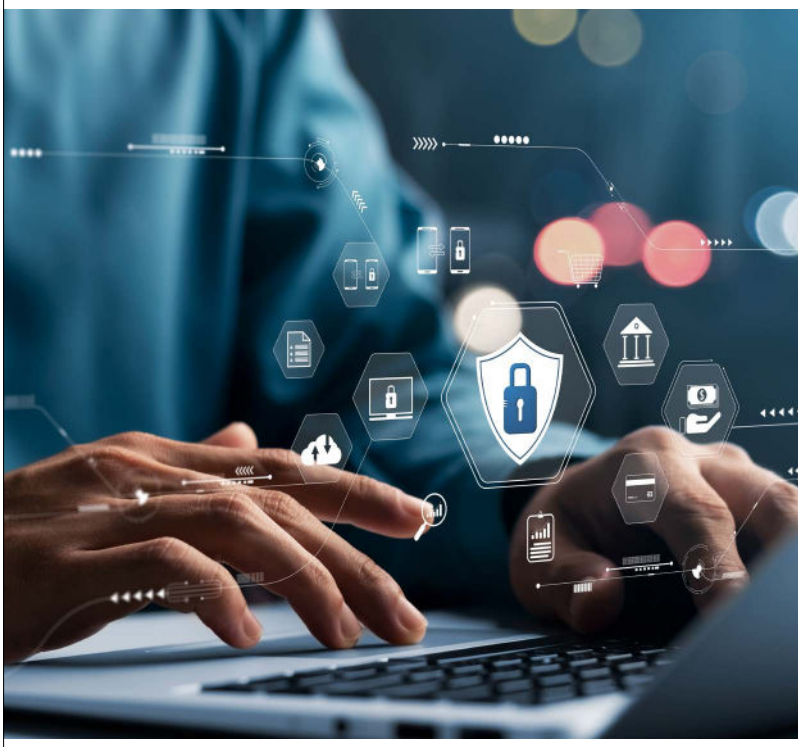
03 Une faculté d'adaptation constante à l'évolution des menaces

Deux tiers des vulnérabilités les plus critiques sont scannées et exploitées par les attaquants moins de 48h après la publication[4].

Plus de 1500 vulnérabilités étant découvertes chaque mois, le concept d'amélioration continue doit être au cœur de la démarche d'un SOC. Les règles de détection doivent être continuellement adaptées à votre contexte pour prendre en compte votre parc informatique et les vulnérabilités associées à l'état de la menace. La démarche implique :

- Le déploiement rapide d'un set de règles standard et personnalisées lors de la construction de l'environnement technologique, et ce quel que soit le SIEM utilisé.
- L'intégration constante des améliorations afin d'être en permanence à jour sur les menaces
- L'automatisation de certaines actions de réaction (comme l'isolation d'un poste, par exemple) pour limiter la propagation et permettre aux analystes du SOC de se focaliser sur les alertes les plus complexes et les plus impactantes pour votre business.

Par ailleurs, afin de garantir la robustesse opérationnelle et technique du SOC, il est essentiel d'intégrer la pratique de tests récurrents. Ces tests, qu'ils soient opérationnels ou techniques, permettent d'évaluer en continu la performance du SOC face à divers scénarios d'attaques simulées. Cette approche proactive assure que les capacités de détection, de réaction et d'adaptation du SOC demeurent efficaces dans un environnement en constante évolution. En incluant la notion de tests réguliers dans la stratégie du SOC, **Formind** s'engage à maintenir un niveau optimal de préparation et de résilience face aux menaces.



4. source: CERT-FR (Centre gouvernemental de veille, d'alerte et de réponses aux attaques informatiques)

04

Un partenaire accompagnateur, pas une boîte noire !

Prêtez une attention particulière à la transparence du modèle de coûts appliqué par votre futur prestataire. Vous devez être en mesure d'identifier facilement les coûts associés à la phase de *Build*, de *Run* et à l'ensemble des services d'accompagnement. "Chez **Formind**, chaque étape est clairement identifiable" indique le directeur SOC & CERT Formind. Les services s'articulent en trois phases, associées à des coûts transparents : le coût des licences en fonction de la volumétrie ou du nombre d'équipements placés sous supervision, les coûts associés aux comités de pilotage (déterminés en fonction du nombre de jours), ainsi qu'aux phases de *Build* et de *Run*, avec une facturation à l'incident. "Si le périmètre à protéger évolue, notre modèle permet de facilement l'anticiper".

Dans le même objectif de transparence, Formind a fait le choix de donner à ses clients l'accès à la console de supervision, où qu'elle soit hébergée. Ces derniers peuvent ainsi contrôler l'activité, faire progresser les équipes si nécessaire, et conserver la maîtrise et la visibilité sur l'ensemble des opérations.

05 Une capacité à accélérer les projets

La rapidité à obtenir les premières remontées d'alertes est également un critère à prendre en compte. Les bons choix technologiques associés à des développements éprouvés permettent d'accélérer les projets tout en s'adaptant à n'importe quel environnement.

Formind applique une méthodologie standardisée, basée sur des ateliers visant à identifier les scénarios d'attaques, choisir le périmètre de déploiement, sélectionner les bons outils. Une infrastructure de collecte simplifiée, reposant sur les alertes générés par les outils de sécurité permet de simplifier l'intégration. Contrairement à un SOC standard, pour lequel 6 mois sont souvent nécessaires pour obtenir les premières remontées d'alertes, le **SOC Formind** est opérationnel en moins de deux mois.

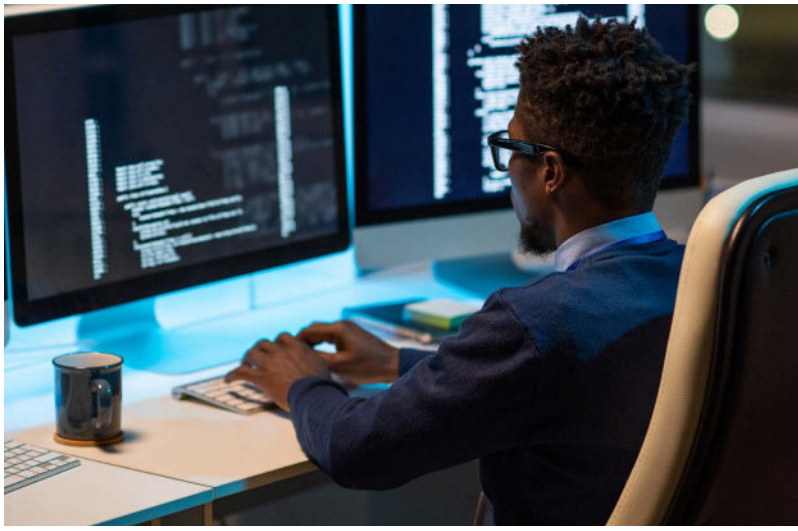
> *Le SOC Formind se déploie rapidement et se positionne comme un orchestrateur d'alertes de diverses sources permettant à nos experts de se concentrer sur les investigations à forte valeur ajoutée. Les règles de détection sont adaptées et testées continuellement.*

Charles Melin,
Directeur SOC & CERT
et associé Formind

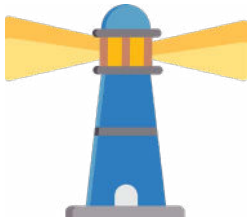
06 Une démarche transverse incluant la réponse en cas d'attaque

Une stratégie basée sur un SOC, même bien orchestrée, ne peut garantir une protection à 100%. La démarche doit être globale, incluant une stratégie de surveillance, une capacité à anticiper mais également à réagir rapidement si l'attaque se produit.

L'approche **Formind** intègre ces trois dimensions pour une protection complète.



LE SERVICE SOC FORMIND



SOC
(Security Operation Center)

Alimenté par un renseignement continu du CERT sur la menace, il détecte les incidents, les qualifie en investiguant et levant les doutes.

Microsoft Sentinel

CERT - VOC
(Cellule de renseignement sur la menace)

En connexion avec les cellules de renseignement CERT du monde entier, il rassemble et synthétise les dernières vulnérabilités et attaques.

CERT - FIR
(Réponse à incident)

Cette équipe d'experts intervient directement pour limiter l'impact business d'une attaque avérée.

formind

Security for Business Performance

EN SAVOIR PLUS SUR LE SOC FORMIND

EN SAVOIR PLUS SUR MICROSOFT SENTINEL

Pour en savoir plus :

contact@formind.fr

soc-cert.formind.fr