

Le guide de l'acheteur pour les services de MDR cogérés

Comment tirer le meilleur parti de vos investissements EDR et SIEM, développer la résilience et renforcer votre posture de sécurité.



Ce qui est inclus

Ce guide explique comment évaluer un fournisseur de services MDR gérés à travers deux optiques distinctes : les besoins stratégiques d'un RSSI et les réalités opérationnelles d'une équipe de sécurité interne. Vous trouverez également les bases des services MDR proactifs et collaboratifs, ainsi que les possibilités de personnaliser votre engagement MDR en fonction de l'évolution de vos besoins.

En outre, il fournit une auto-évaluation pour vous aider à comprendre vos propres besoins, détaille les services que vous devriez attendre d'un partenaire qui se concentre sur vos objectifs de cyber-résilience. Enfin, il explique comment les services MDR cogérés peuvent augmenter le retour sur investissement de vos plateformes EDR et SIEM existantes, en servant d'extension à votre équipe de sécurité interne.

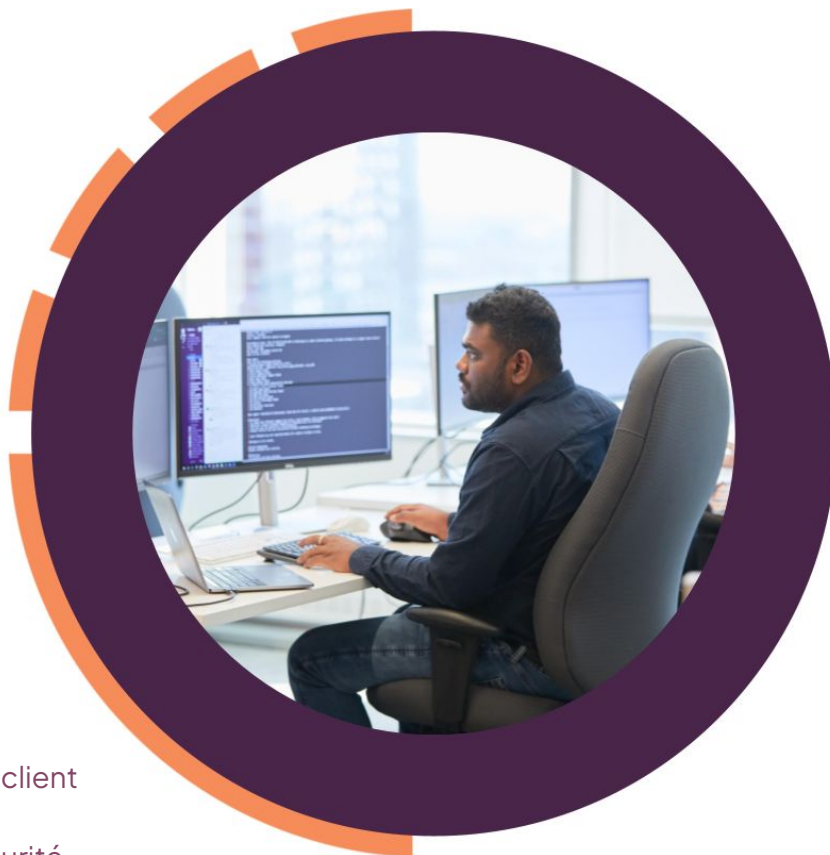


Table des matières

L'importance d'une approche centrée sur le client

L'intérêt d'être propriétaire de sa pile de sécurité

PARTIE 1: Pour le responsable de la sécurité de l'information (CISO)

PARTIE 2: Pour le directeur de l'équipe de sécurité interne

PARTIE 3: Auto-évaluation : Connaître ses besoins avant d'acheter

PARTIE 4: De la prévention à la cyber-résilience : Services et produits attendus

PARTIE 5: Maximiser votre retour sur investissement : L'effet multiplicateur de l'intégration

MDR en copropriété : la réponse aux services MDR adaptés au contexte de votre entreprise

L'importance d'une approche centrée sur le client

La gestion de la détection et de la réponse (MDR) est un service crucial pour les organisations qui cherchent à renforcer leur posture de sécurité. Cependant, de nombreux fournisseurs proposent un modèle unique qui traite la sécurité comme un produit transactionnel. Face à des menaces de plus en plus sophistiquées et à une technologie qui évolue rapidement, une approche traditionnelle ne suffit plus. Le MDR est un investissement justifié qui fournit une défense continue, de niveau expert, nécessaire à la continuité de l'activité, à l'innovation et à la croissance stratégique.

Notre approche "boutique" répond à ces besoins. Nous pensons qu'une sécurité efficace est un partenariat fondé sur une approche de services de sécurité par conception et axée sur le client. Cela inclut les entreprises dont les besoins ne correspondent pas aux offres à l'emporte-pièce des fournisseurs de plateformes MDR. Il s'agit d'entreprises confrontées à une croissance rapide, au changement et à l'échelle, ce qui signifie qu'un contrat traditionnel de trois ans sera dépassé dès la deuxième année.



L'intérêt d'être propriétaire de sa pile de sécurité

Dans un programme de sécurité moderne, la question de savoir qui possède la technologie est aussi importante que ce que fait la technologie.

De nombreux fournisseurs de MDR vous obligent à utiliser leur plateforme propriétaire, ce qui crée une "boîte noire" dans laquelle vous avez une visibilité limitée sur vos propres données et devez vous adapter à leurs processus. Cette approche peut entraîner des problèmes importants tels que le verrouillage du fournisseur et l'absence de contrôle stratégique à long terme.

Cela fonctionne bien pour les petites entreprises, celles qui n'ont pas investi dans des outils de sécurité internes, ou celles qui s'attendent à ce que 95 % de leurs alertes proviennent de l'EDR. Une meilleure approche pour les grandes entreprises dotées d'une infrastructure complexe et d'équipes de sécurité internes limitées consiste à s'associer à un service MDR qui fonctionne avec les outils de sécurité que vous possédez déjà, comme votre EDR et votre SIEM.

En étant propriétaire de votre pile de sécurité, vous vous assurez de ce qui suit :

- **Vous gardez le contrôle de vos données.** Les données télémétriques de votre environnement restent en votre possession, ce qui vous donne la possibilité de les utiliser à des fins d'investigation interne, de conformité et d'autres besoins spécifiques à votre entreprise.
- **Vous évitez l'enfermement dans un fournisseur.** Vous ne liez pas votre programme de sécurité à la technologie d'un seul fournisseur. Si les besoins de votre entreprise changent, si vos systèmes évoluent ou si vous choisissez un nouveau partenaire, vous pouvez le faire sans avoir à mettre en place un projet de remplacement coûteux et perturbateur.
- **Vous préservez et développez les personnalisations existantes.** Les entreprises investissent beaucoup de temps et de ressources dans l'adaptation de leurs plateformes de sécurité avec des règles de détection, des tableaux de bord et des playbooks personnalisés. Un partenaire qui travaille dans le cadre de votre pile existante préserve et affine en permanence cette précieuse propriété intellectuelle, évitant ainsi les coûts et le temps considérables nécessaires pour reconstruire ces personnalisations sur une nouvelle plate-forme propriétaire, si un changement s'avérait nécessaire.
- **Votre équipe conserve des connaissances précieuses.** Votre équipe interne continue à travailler et à développer son expertise sur les plateformes que vous avez choisies, ce qui garantit qu'elle n'est pas seulement un consommateur d'un service mais qu'elle participe activement à votre posture de sécurité. Les conseils et les recommandations des experts en sécurité des MSSP élargissent leurs connaissances tout en renforçant votre dispositif de sécurité.



Ce guide s'adresse aux responsables de la sécurité qui comprennent que le MDR n'est pas simplement l'achat d'un service, mais qu'il s'agit d'une capacité essentielle à construire, à renforcer et à maintenir sur le long terme.

Partie 1: Pour le responsable de la sécurité de l'information (CISO)

Le rôle du RSSI est de gérer les risques, d'assurer la continuité des activités et d'aligner la sécurité sur les objectifs de l'organisation. Lors de l'évaluation d'un service de MDR cogéré, l'accent est mis sur la valeur stratégique, et pas seulement sur les caractéristiques techniques.

1. Partenariat stratégique et alignement

Au-delà d'un fournisseur :

Comprendre le processus que le fournisseur mettra en œuvre pour démontrer qu'il est un véritable partenaire qui comprend le contexte et les objectifs de votre entreprise, votre tolérance au risque et le paysage de la conformité. Recherchez un fournisseur prêt à investir dans une relation à long terme.

Questions à poser :

- Comment mesurez-vous le succès d'un partenariat de sécurité à long terme au-delà des simples indicateurs ?
- Pouvez-vous donner la référence d'un client avec lequel vous travaillez depuis plus de trois ans et qui peut parler du modèle de partenariat ?



Approche de la cogestion des services :

Renseignez-vous sur la manière dont le fournisseur conçoit ses services pour qu'ils constituent un élément fondamental de votre stratégie de cybersécurité, et non un service purement réactif. Recherchez une approche qui met l'accent sur l'amélioration continue en vue de renforcer la résilience cybernétique.

Questions à poser :

- Comment contribuez-vous activement à notre posture de sécurité au-delà de la simple détection réactive des menaces ?
- Quel est votre processus d'intégration à nos investissements existants en matière de sécurité ? À quoi ressemble votre processus d'intégration ?
- Comment la couverture 24/7/365 est-elle assurée ? Les analystes travaillent-ils 24 heures sur 24 ou dans le cadre d'équipes de jour normales, en fonction du lieu où ils se trouvent ?
- Avec personnalisation : Compte tenu de notre environnement, quelles recommandations feriez-vous pour des ajouts personnalisés qui améliorent notre posture de sécurité ?

2. Réduction des risques et retour sur investissement

Alignement sur la tolérance au risque :

Vous voulez que votre MSSP démontre que ses services correspondent à l'appétit de votre organisation pour le risque de sécurité. Demandez des indicateurs qui vont au-delà du simple nombre d'alertes, tels que la diminution du MTTD et du MTTR, et l'alignement sur des cadres tels que le NIST ou le MITRE ATT&CK.

Questions à poser :

- Pouvez-vous fournir un exemple de rapport qui associe vos services à des contrôles spécifiques dans des cadres tels que NIST ou MITRE ATT&CK ?
- Votre rapport indiquera-t-il les alertes traitées et les alertes restantes avec l'identification des niveaux de risque ? Quel niveau d'orientation fournirez-vous pour améliorer nos résultats en matière de détection et de réponse ?
- Quels niveaux de contrôle pouvons-nous maintenir en relation avec les services MDR ?
- Avec personnalisation : Quelles mesures clés allez-vous suivre pour démontrer une réduction tangible du risque de notre organisation ?
- Avec personnalisation : Que faudrait-il pour ajouter des applications personnalisées et/ou des applications en nuage et des automatisations à nos services MDR ?



Rentabilité et coût total de possession (TCO) :

Évaluez le modèle de tarification du fournisseur. Il doit offrir une structure de coûts prévisible et évolutive. Comparez cela aux dépenses importantes et à la difficulté de construire et de conserver un centre d'opérations de sécurité (SOC) en interne, 24 heures sur 24 et 7 jours sur 7.

Questions à poser :

- Que comprend votre service de base et que considérez-vous comme un ajout ou un coût supplémentaire ?
- Comment votre modèle de tarification s'adapte-t-il à la croissance de l'entreprise, par exemple en cas de fusion ou d'acquisition ou d'ajout de nouveaux sites ?

3. Évolutivité et flexibilité

Adaptation à la croissance :

Soyez assuré que le service MDR cogéré s'adaptera de manière transparente à la croissance de votre entreprise, qu'il s'agisse de fusions et d'acquisitions, de l'adoption de l'informatique dématérialisée ou de l'expansion sur de nouveaux marchés.

Questions à poser :

- Comment prenez-vous en charge les opérations de sécurité lors d'une fusion ou d'une acquisition ?
- Quel est le délai moyen d'intégration d'un nouvel environnement en nuage ou d'une nouvelle unité commerciale ?
- Quelle est la procédure de modification d'un contrat pendant sa durée ?

Agnostique en matière de plateforme :

Vérifiez que le fournisseur possède l'expertise nécessaire pour s'intégrer à votre pile technologique existante (par exemple, EDR, SIEM, infrastructure en nuage). Un écosystème flexible et ouvert est essentiel pour maximiser vos investissements dans les outils de sécurité existants et éviter le verrouillage des fournisseurs.

Questions à poser :

- Quelle est votre approche de l'intégration dans un environnement multi-cloud ou hybride ?
- Pouvez-vous fournir une liste de vos plateformes EDR et SIEM supportées, et quel est le processus d'intégration avec un outil qui ne figure pas sur cette liste ?



Partie 2: Pour le directeur de l'équipe de sécurité interne

Le directeur de la sécurité gère les opérations quotidiennes et l'exécution tactique du programme de sécurité. Il se concentre sur l'amélioration du flux de travail, de l'intégration et de la collaboration qui permet de réduire les risques et d'améliorer la réactivité afin d'assurer la continuité des activités conformément à la stratégie de cybersécurité du CISO.

1. Sources de journaux personnalisées et simplicité opérationnelle

Validation des sources de logs et réponse active :

Toutes les sources de logs n'ont pas la même valeur. Un fournisseur de services MDR personnalisés et orienté client ne se contentera pas d'ingérer les journaux, mais collaborera avec votre équipe pour valider et hiérarchiser les sources les plus critiques pour la détection et la réponse, y compris les sources de journaux personnalisées. Il construira activement des règles de corrélation et des requêtes de chasse aux menaces sur ces sources validées, en s'assurant que vos journaux sont une source d'intelligence exploitable, et non un simple stockage de données.

Questions à poser :

- Quelles sont les sources de logs que vous étudiez activement et sur lesquelles vous construisez des règles de détection ?
- Quel est votre processus de validation de la fidélité de nos sources de logs et quel pourcentage de nos logs utilisez-vous activement pour la détection ?

Intégration transparente :

Vous devez savoir comment le service MDR cogéré s'intégrera aux outils que votre équipe utilise quotidiennement. L'objectif est d'améliorer, et non de remplacer, vos capacités existantes.

Questions à poser :

- Comment garantisiez-vous l'intégrité et la transparence des données lors de l'ingestion de notre télémétrie ?
- Pouvons-nous accéder aux données brutes que vos analystes utilisent pour leurs investigations ?

Visibilité unifiée :

Vous voulez une vue unique et consolidée de toutes les alertes et de tous les incidents, quelle qu'en soit la source. Recherchez un fournisseur capable de corréler les données provenant des terminaux, du réseau, du cloud et des plates-formes d'identité.

Questions à poser :

- À quoi ressemble votre tableau de bord unifié et quel type de visibilité en temps réel offre-t-il ?
- Comment gérez-vous le triage et la hiérarchisation des alertes pour éviter la lassitude ?
- Avec la personnalisation : Que faudrait-il faire pour inclure les journaux de pare-feu, les proxies et intégrer notre système de billetterie dans le service MDR ?

2. Expertise et collaboration humaine

Accès à des analystes désignés :

La relation et la familiarité avec votre environnement sont essentielles. Assurez-vous que votre équipe aura un accès direct à un analyste de sécurité spécialisé qui comprend votre environnement. Évitez les fournisseurs qui vous dirigent vers un groupe d'assistance générique et anonyme.

Questions à poser :

- Aurons-nous des équipes partiellement dédiées pour garantir la familiarité avec notre environnement et notre contexte commercial ? À quoi cela ressemble-t-il ?
- Quelles sont les procédures d'escalade en cas d'incident critique et quels sont les délais de réponse garantis ?
- Comment gérer l'humain dans la boucle (HITL) avec l'automatisation et l'IA ?

Enquête collaborative et confinement :

Découvrez à quoi pourrait ressembler la collaboration entre l'équipe du fournisseur et la vôtre lors d'un événement de sécurité en direct. Un partenaire centré sur le client fournit des canaux de communication clairs, des playbooks détaillés et travaille aux côtés de votre équipe pour l'endiguement et la remédiation.

Questions à poser :

- Pouvez-vous nous présenter un scénario récent de réponse à un incident dans lequel vous avez travaillé avec l'équipe interne d'un client ?
- Comment fournissez-vous le support et la documentation pour les actions de remédiation et de récupération ?



3. Transparence et renseignements exploitables

Des rapports transparents :

Ne vous contentez pas d'un simple PDF mensuel. Renseignez-vous sur votre capacité à accéder à des tableaux de bord en temps réel et à des rapports détaillés qui fournissent des informations exploitables sur votre paysage des menaces.

Questions à poser :

- Quelle est la fréquence de vos rapports et sont-ils adaptables à nos besoins ?
- Fournissez-vous une analyse des causes profondes après la résolution d'un incident ?
- Fournissez-vous une assistance et des rapports de conformité pour nous aider à passer les audits et à répondre aux exigences de l'assurance cybernétique ? Ou s'agit-il d'un ajout personnalisé ?

Une chasse aux menaces fondée sur des hypothèses :

La chasse aux menaces ne doit pas être un service "boîte noire". Vérifiez si le MSSP propose un modèle de collaboration dans lequel les chasseurs de menaces travaillent avec votre équipe pour définir de manière proactive les prémisses et les hypothèses de la chasse aux menaces. Un fournisseur spécialisé partage ses connaissances et ses méthodologies pour aider votre équipe à se développer.

Questions à poser :

- Comment partagez-vous vos conseils et vos recommandations sur les "événements d'intérêt" avec notre équipe ?
- Comment notre équipe interne peut-elle participer ou contribuer à vos activités de chasse aux menaces ?



Partie 3: Auto-évaluation : Connaître ses besoins avant d'acheter

Avant de choisir le bon partenaire, vous devez vraiment comprendre votre propre environnement de sécurité. Cette auto-évaluation est l'étape la plus critique pour s'assurer que le service de MDR cogéré que vous choisissez est le bon, et elle vous évite d'acheter une solution qui ne résoudrait pas vos problèmes réels.

Pour le RSSI : une auto-évaluation stratégique

Votre priorité est d'aligner la sécurité sur l'activité de l'entreprise. Avant de vous engager avec un MSSP, répondez à ces questions avec votre équipe de direction :

Quels sont nos principaux actifs critiques ?

- Seront-ils activement surveillés ?
- Avons-nous des sources de logs personnalisées que nous devons inclure dans le service MDR ?
- Quels sont les vecteurs de menace qui ciblent notre secteur d'activité ?

En répondant à ces questions, vous pourrez filtrer les fournisseurs en fonction de leur capacité à traiter vos risques les plus importants, plutôt que de vous contenter d'offrir un service générique.

Quelles sont nos principales obligations en matière de conformité et de réglementation ?

- Quels sont les cadres réglementaires (par exemple, HIPAA, PCI DSS, GDPR) auxquels nous sommes tenus d'adhérer ?
- Quel est notre niveau de maturité actuel pour chacun d'entre eux ?

Votre fournisseur de services MDR doit être en mesure de prendre en charge et de fournir des rapports pour ces exigences spécifiques afin d'éviter de futurs maux de tête liés à la conformité.

Quelle valeur notre opération de sécurité apporte-t-elle à l'entreprise ?

- Quels sont les objectifs commerciaux que nous réalisons aujourd'hui ?
- Quels objectifs commerciaux devons-nous atteindre dans les trois prochaines années ?
- Comment prouver cette valeur à l'équipe de direction et au conseil d'administration ?

Un MSSP doté d'un programme d'assurance client travaille avec vous pour comprendre vos attentes et vous montrer comment le service MDR apporte cette valeur, avec un rapport rédigé pour les parties prenantes de l'entreprise.

Quel est notre véritable coût total de possession (TCO) ?

- Au-delà des salaires, que dépensons-nous en licences technologiques, en formation, en recrutement et en charges opérationnelles liées à la gestion d'une fonction de sécurité 24 heures sur 24 et 7 jours sur 7 ?

Cette évaluation vous aide à monter un dossier solide sur les services gérés de MDR, en démontrant qu'ils permettent de libérer des capitaux et des ressources pour d'autres initiatives stratégiques.

Pour le directeur de l'équipe de sécurité interne : Une auto-évaluation tactique

Vous vous concentrez sur les opérations quotidiennes. Une évaluation franche des capacités et de la charge de travail de votre équipe est essentielle pour trouver un fournisseur qui sera un véritable multiplicateur de force, et non un simple outil de plus.

Quelles sont les compétences et les lacunes de notre équipe ?

- Disposons-nous d'une expertise en matière d'investigation des incidents, de sécurité dans le nuage ou de chasse aux menaces ?
- Qui assure la couverture après les heures de travail ?

Cela permet d'identifier les services spécifiques dont vous avez besoin pour renforcer votre équipe et vous évite de payer pour des capacités que vous possédez déjà en interne.

À quoi ressemble notre charge de travail opérationnelle quotidienne ?

- Quelles sont les sources de logs que nous devons surveiller activement pour protéger nos actifs critiques et la continuité de nos activités ?
- Combien d'alertes recevons-nous en moyenne par jour ?
- Quel est le temps moyen nécessaire au triage d'une alerte et à l'investigation d'un incident confirmé ?

En identifiant les sources de logs, vous pouvez valider spécifiquement ce que le service MDR travaillera activement et quelles données seront stockées à froid. La quantification des alertes et des délais permet de définir des objectifs clairs pour le service MDR et de mesurer son succès.

Notre pile de technologies de sécurité actuelle est-elle pleinement utilisée ?

- Tirons-nous le meilleur parti de notre EDR ou de notre SIEM ?
- La conservation des données est-elle suffisante pour une chasse aux menaces à long terme ?

Cette évaluation vous aide à trouver un partenaire qui maximisera vos investissements existants et comblera les lacunes sans vous obliger à mettre en œuvre un projet de remplacement coûteux.



Partie 4: De la prévention à la cyber-résilience : Services et produits attendus

Un service MDR cogéré et véritablement axé sur le client ne se contente pas d'arrêter les attaques. Il vous aide à mettre en place un programme de sécurité résilient, capable de résister aux menaces et de s'en remettre, garantissant ainsi la continuité des activités. Vous trouverez ci-dessous trois services et prestations de base que vous devriez attendre d'un prestataire de services de MDR cogérés qui s'aligne sur cette philosophie. En outre, vous trouverez deux compléments personnalisés à envisager en fonction de vos priorités.

1. Réponse aux incidents collaborative et exploitable

Ce à quoi on peut s'attendre : En cas d'incident, la réponse du fournisseur doit être un effort de collaboration visant à assurer la continuité de l'activité. Il doit non seulement aider votre équipe à contenir la menace, mais aussi travailler avec vous pour rétablir rapidement les opérations normales.

- **Résultats attendus :** Un plan de réponse à l'incident clair (ou "playbook") qui détaille les responsabilités, les canaux de communication et les mesures d'endiguement. Un rapport post-incident comprenant une analyse détaillée des causes profondes et des recommandations exploitables pour éviter que de tels incidents ne se reproduisent.

Pourquoi c'est important : L'accent est mis sur la résilience. Un bon fournisseur comprend qu'un incident de sécurité est aussi une interruption de l'activité. Il agit pour minimiser les temps d'arrêt et permettre à votre entreprise de reprendre ses activités le plus rapidement possible.

2. Approche agnostique de l'agent et intégration transparente

Ce à quoi vous pouvez vous attendre : Un service MDR cogéré moderne ne devrait pas vous obliger à déployer un nouvel agent. Au contraire, il doit pouvoir s'intégrer à votre agent de sécurité des points finaux (EDR) existant pour collecter les données nécessaires. Ce modèle "agnostique" vous permet de tirer parti de vos investissements actuels et d'éviter les perturbations opérationnelles et les coûts associés au déploiement d'un nouvel outil dans l'ensemble de votre environnement. Il garantit que le service MDR est un multiplicateur de force pour vos outils existants, et non un remplacement.

- **Produits livrables :** Un plan d'intégration clairement défini qui décrit comment le MSSP ingérera les données de votre agent existant, ainsi qu'une liste des plates-formes prises en charge.

Pourquoi c'est important : Cette approche est cruciale pour la rentabilité et la continuité opérationnelle. Vous évitez le coût important des nouvelles licences d'agent et le processus fastidieux d'un nouveau déploiement. En outre, vos équipes internes peuvent continuer à utiliser les outils et les flux de travail qui leur sont déjà familiers, ce qui réduit les frictions et permet un partenariat plus fluide et plus efficace.

3. Amélioration continue et orientation stratégique

Ce à quoi vous pouvez vous attendre : Un véritable partenaire ne se contente pas de fournir un service ; il vous aide à faire évoluer votre programme de sécurité. Le fournisseur doit proposer des réunions régulières et des conseils stratégiques basés sur les informations qu'il recueille sur votre environnement et sur le paysage des menaces au sens large.

- **Produits livrables :** Des analyses périodiques qui résument les principaux résultats, fournissent une feuille de route pour l'amélioration de la sécurité et vous aident à démontrer le retour sur investissement à votre direction générale.

Pourquoi c'est important : Cela garantit que votre programme de sécurité est une entité vivante et évolutive. Il transforme le service MDR d'un simple utilitaire en un atout stratégique qui vous aide à prendre des décisions éclairées et à mettre en place une posture de sécurité solide et à l'épreuve du temps.

Des compléments personnalisés à prendre en compte

Chaque entreprise a des besoins uniques en matière de sécurité. En fonction des compétences de votre équipe interne et des domaines sur lesquels elle doit se concentrer, les deux services complémentaires personnalisés suivants peuvent être considérés comme une approche rentable. Examinez votre feuille de route en matière de cybersécurité, votre environnement de menaces et votre surface d'attaque pour déterminer la valeur ajoutée potentielle de votre programme de sécurité.

1. Renseignements sur les menaces et chasse aux menaces en fonction du contexte

Ce à quoi vous pouvez vous attendre : Au lieu de s'appuyer sur des flux génériques, le fournisseur personnalisera les renseignements sur les menaces en fonction de votre secteur d'activité, du contexte de votre entreprise et de vos actifs critiques. Ses chasseurs de menaces utiliseront ces informations pour rechercher de manière proactive les menaces les plus susceptibles de cibler votre organisation.

- **Produits livrables :** Un briefing sur les renseignements sur les menaces qui décrit les menaces spécifiques ciblant votre secteur, et des rapports périodiques sur la chasse aux menaces qui détaillent les méthodologies et les résultats des chasses proactives.

Pourquoi c'est important : Cette approche ciblée garantit que le MSSP se concentre sur les menaces qui comptent pour votre entreprise, en réduisant le bruit et en donnant la priorité à la protection de vos actifs les plus précieux.



2. Gestion des vulnérabilités

Ce à quoi il faut s'attendre : Le fournisseur peut proposer des services qui améliorent activement votre posture de sécurité au fil du temps. Cela va au-delà de la simple détection et comprend l'identification et l'aide à la correction des faiblesses avant que les attaquants ne les exploitent.

- **Produits livrables :** Des rapports réguliers sur les vulnérabilités et la configuration qui mettent en évidence les mauvaises configurations ou les lacunes, ainsi que des recommandations de remédiation classées par ordre de priorité.

Pourquoi c'est important : La gestion des vulnérabilités est une approche de service de "sécurité par conception". Elle vous aide à réduire de manière proactive votre surface d'attaque et à construire des fondations plus solides, ce qui rend votre organisation plus résistante aux attaques futures.

Partie 5: Maximiser votre retour sur investissement : L'effet multiplicateur de l'intégration

De nombreuses organisations ont déjà réalisé des investissements importants dans des plateformes de sécurité telles que Endpoint Detection and Response (EDR) et Security Information and Event Management (SIEM). Un service MDR de qualité ne vous oblige pas à abandonner ces outils, mais vous aide à en tirer le meilleur parti, en vous permettant d'en exploiter tout le potentiel.



Pour le RSSI : L'analyse de rentabilité stratégique de l'intégration des plates-formes

Vos systèmes EDR et SIEM existants représentent des investissements importants. Un fournisseur de services MDR cogérés qui s'intègre à ces plateformes permet de rentabiliser ces investissements de manière plus efficace et plus intelligente.

Ce à quoi il faut s'attendre : Le MSSP doit utiliser son expertise spécialisée pour filtrer les milliers d'alertes de faible priorité ou faussement positives générées par vos plateformes. Il ne doit transmettre à votre équipe que les menaces les plus critiques et les plus fiables. Ainsi, vos outils ne seront plus une source de bruit écrasante, mais un moteur de détection très efficace.

Pourquoi c'est important : Cette approche justifie le retour sur investissement à long terme de vos licences EDR et SIEM. En vous déchargeant du triage constant et de l'investigation initiale, vous pouvez prouver au conseil d'administration que vous utilisez vos outils de sécurité existants au maximum de leur potentiel. Cela vous permet de réorienter vos ressources internes vers des projets stratégiques de plus haut niveau, tels que la gestion des vulnérabilités, les révisions d'architecture et le soutien aux initiatives de transformation numérique, en veillant à ce que les dépenses de sécurité s'alignent directement sur les objectifs de l'entreprise.

Pour le directeur de l'équipe de sécurité interne : Renforcer les capacités et les connaissances

Le bien le plus précieux de votre équipe est son temps. Un partenariat MDR collaboratif libère ce temps et fournit une voie directe vers la montée en compétences de votre équipe.

Ce à quoi il faut s'attendre : Les analystes du prestataire de services de MDR ne doivent pas opérer dans une "boîte noire". Ils doivent au contraire fonctionner comme une extension de votre équipe, en assurant un transfert direct des connaissances. Ils doivent partager leurs méthodologies, expliquer leur logique pendant les enquêtes et fournir un contexte lorsqu'ils contiennent les menaces et y remédient.

Pourquoi c'est important : Ce modèle de collaboration permet de combler le manque de compétences en cybersécurité au sein de votre organisation. Votre équipe acquiert de l'expérience sur le terrain avec des techniques avancées de chasse aux menaces et des manuels de réponse aux incidents, ce qui la rend plus apte à gérer les futures menaces de manière indépendante. Le service MDR n'est plus une béquille mais un programme de formation, qui renforce la résilience cybernétique à long terme de l'intérieur et permet à votre équipe de se concentrer sur les projets critiques.

En outre, si vous optez pour une couverture 24/7/365, vous serez soulagé de la charge de travail que représente une opération 24 heures sur 24, ce qui réduira le risque d'épuisement de votre équipe de sécurité. Il est essentiel de conserver les talents en matière de cybersécurité pour accroître la maturité et la résilience de la sécurité. La flexibilité d'affecter les professionnels de la sécurité à des tâches significatives contribue à la rétention, à la productivité et à la satisfaction au travail.



MDR en copropriété : la réponse aux services MDR adaptés au contexte de votre entreprise

Si vous êtes une entreprise qui attend de votre EDR qu'il déclenche 95 % de vos alertes de sécurité, un service de MDR géré de type "boutique" est superflu. Un fournisseur de MDR à taille unique est un meilleur choix.

En revanche, si vous disposez de réseaux complexes, d'environnements hybrides, de milliers de terminaux et/ou de sites multiples, vous avez besoin d'un équilibre entre flexibilité et contrôle, que vous obtiendrez grâce à une approche "boutique" du MDR cogéré, axée sur le client.

Le MDR ne consiste pas seulement à envoyer des analystes de sécurité L1 et L2 sur des fichiers journaux. C'est un élément stratégique de votre programme de sécurité. La cybersécurité est un catalyseur de l'activité et un programme d'assurance de la continuité de l'activité. Il ne s'agit plus d'essayer d'empêcher une violation, mais d'adopter une approche orchestrée qui réduit le risque d'exposition et le niveau de dommages aux opérations commerciales, à la réputation de la marque et à l'affinité avec les clients.

Pour atteindre ce résultat, vous avez besoin de services MDR cogérés, conçus et exécutés en fonction du contexte de votre entreprise et de votre secteur d'activité, et conçus spécifiquement pour protéger vos actifs et processus d'entreprise les plus critiques.

En utilisant les conseils ci-dessus pour évaluer un fournisseur de services MDR cogérés, vous avez toutes les chances d'obtenir les résultats dont vous avez besoin pour parvenir à la cyber-résilience.

À propos de SecureOps :

SecureOps est un fournisseur de services de sécurité managés (MSSP) de type « boutique » proposant une expertise en matière de SOC personnalisé, de MDR en copropriété, de sécurité des infrastructures et de gestion des vulnérabilités. Nous nous adaptons aux besoins de nos clients grâce à notre approche de sécurité dès la conception. Notre modèle de continuité d'activité 24 h/24 et 7 j/7 garantit aux entreprises et aux particuliers du monde entier le contrôle permanent de leurs données protégées grâce à la technologie qu'ils ont choisie.

Pour en savoir plus,
rendez-vous sur www.secureops.com

