Integrity360
your security in mind

Éclairez votre voie : le guide CyberFire Pour une stratégie MDR plus intelligente

Choisir le bon partenaire MDR n'a jamais été aussi essentiel — ni aussi complexe. Alors que le paysage des menaces évolue rapidement et que les attaquants gagnent en audace, de nombreuses organisations se disent frustrées par des prestataires qui :

- Génèrent trop de bruit et pas assez de visibilité
- Peinent à évoluer ou à s'adapter à la croissance des besoins
- Complexifient leurs tarifs avec des coûts cachés
- N'assurent pas une réponse et une remédiation à la hauteur des attentes

Beaucoup d'entreprises souscrivent à des services MDR en espérant un véritable partenariat – mais se retrouvent confrontées à la lassitude des plateformes, à une surcharge d'alertes et à une inflation des coûts. Cela vous rappelle quelque chose ?

C'est précisément là que **CyberFire MDR** fait la différence. Cette solution a été conçue comme la réponse à ces problèmes, en éliminant le bruit pour livrer des résultats concrets.

Les **frustrations** les plus fréquentes des acheteurs de services MDR :

- **Des plateformes difficiles à utiliser,** qui rendent la navigation et le reporting laborieux
- **Un suivi client insuffisant** et un manque de communication sur les tickets
- **Des processus de remédiation lents et incohérents,** laissant les équipes dans l'incertitude.

CyberFire MDR adresse précisément ces préoccupations :

- **Portail et reporting simplifiés :** une expérience fluide et intuitive
- **Experts dédiés à la réussite client :** responsabilité claire et communication continue
- **Procédures de triage et de remédiation guidées :** vous ne restez jamais sans réponse.

Frustrations courantes liées aux services MDR vs. CyberFire MDR

Défi	La solution
Les alertes sont souvent reçues sans véritable voie de résolution.	Chaque alerte inclut un triage mené par un analyste et des étapes de remédiation claires, faciles à suivre, même pour des ingénieurs non experts.
Certaines alertes semblent simplement transmises par les outils des éditeurs, sans validation.	Nous filtrons le bruit et les alertes non exploitables : vous ne recevez que des menaces vérifiées, à haute valeur opérationnelle.
Manque d'intégration avec des outils essentiels comme la gestion des accès à privilèges.	CyberFire s'intègre à un large éventail de technologies et évolue en fonction de votre environnement.
Le service ne semble pas vraiment intégré ni aligné avec les processus internes.	Vous bénéficiez d'un expert dédié à la réussite client et du soutien de 6 SOC répartis dans le monde, pour un alignement étroit et un véritable partenariat.
Réactivité et assistance insuffisantes de la part du prestataire MDR.	Votre expert dédié ne gère que 5 à 6 clients, garantissant un accompagnement rapide, compétent et constant.
Visibilité limitée sur les données de back-end, sauf moyennant des frais supplémentaires.	Accès transparent, reporting en libre-service et aucun coût caché.
Les journaux sont parfois incomplets, et les retours d'analyse manquent de profondeur.	Tous les journaux sont accessibles. Chaque dossier comprend une analyse des causes racines, un contexte complet et des recommandations claires.
Les tickets de support stagnent ou se ferment sans réelle résolution.	Nous garantissons la prise en charge complète du cycle de vie des incidents, chaque investigation va jusqu'à sa conclusion.
Interface peu fluide et inquiétudes quant à des coûts cachés ou variables.	Interface épurée et modèle tarifaire transparent : aucune hausse inattendue.
Le processus d'onboarding est passif, lourd en documentation et souvent incomplet.	Un onboarding piloté et encadré assure une mise en service rapide et complète.
Les fonctions de reporting et de tableau de bord sont décevantes.	Le module Enhanced Reporting propose des rapports personnalisés et une conservation des données à long terme pour la conformité.
Navigation peu intuitive, reporting ad hoc difficile à exécuter.	Un portail conçu pour la clarté : exécutez vos rapports, explorez vos données et gérez votre environnement en toute simplicité.
Trop d'alertes pendant la phase de déploiement ; les conseils de remédiation sont limités.	Nous offrons un triage guidé, une escalade pertinente et une remédiation experte, adaptée à votre environnement.

Les bénéfices attendus avec CyberFire MDR

- **Sérénité :** des alertes haute fiabilité pour ne traiter que ce qui compte vraiment
- **Maîtrise des coûts :** une tarification transparente, sans hausses dissimulées ni besoins matériels imprévus
- **Véritable résilience :** des heures de réponse à incident intégrées et une détection post-intrusion disponibles dès le premier jour
- **Mise en conformité facilitée :** un reporting enrichi, parfaitement adapté aux exigences d'audit et de conformité
- **Amélioration continue :** un service en évolution constante pour accompagner la croissance de votre organisation
- **Soutien de confiance :** une expertise locale, un partenariat proactif et un accompagnement centré sur le client

Ce qui nous distingue

Déploiement clé en main

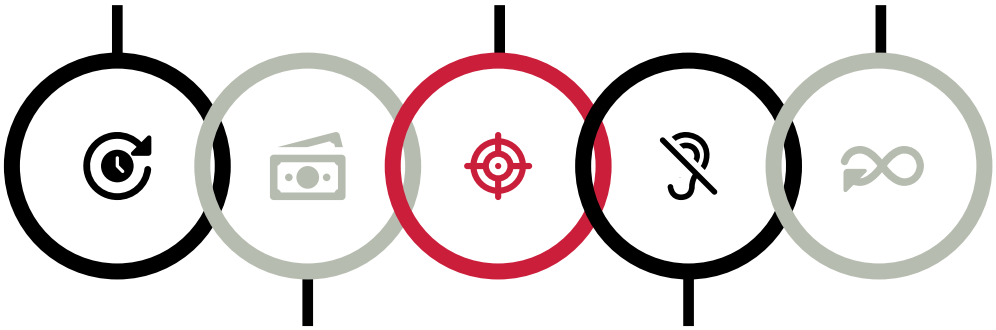
Intégration rapide dans tout environnement de sécurité en 4 semaines ou moins

Détection des menaces haute fidélité

Détection avancée grâce à une ingénierie de pointe et à des règles exclusives développées pour CyberFire MDR

Amélioration continue de la sécurité

Amélioration continue de la couverture de détection des menaces et du niveau global de sécurité



En finir avec les coûts SIEM élevés et imprévisibles

Tarification calculée selon le nombre de terminaux couverts par le service

Un minimum de bruit, une visibilité maximale

Alertes priorisées et de haute qualité, avec **prise en charge complète de la réponse aux incidents**

> "CyberFire ne nous considère pas comme un simple client. Leurs équipes cherchent réellement à comprendre nos défis et à y apporter des solutions. Cette adéquation culturelle a été l'un de nos plus grands succès. Avec notre ancien prestataire, nous étions toujours dans la réaction. Avec CyberFire, nous avons désormais une longueur d'avance."

Responsable Gouvernance, Risques et Conformité IT - Groupe de services financiers

Ce que vous attendez d'un service MDR et comment CyberFire y répond

Vos besoins	Pourquoi c'est essentiel	Notre approche
Visibilité réelle	Beaucoup de prestataires la promettent, peu la délivrent	Des informations exploitables en temps réel, sans bruit parasite, soutenues par une analyse et une qualification menées par nos experts
Réponse exploitable	Des alertes seules ne résolvent rien	Un accompagnement par nos analystes pour une remédiation guidée, avec des actions claires, même pour les équipes non expertes
Expérience simplifiée	Des portails complexes et des données dispersées font perdre un temps précieux et retardent la réponse	Une interface intuitive donnant accès aux incidents en cours, aux alertes historiques et aux rapports à la demande
Tarification claire et prévisible	Les coûts cachés et augmentations imprévues fragilisent la confiance et les budgets	Une tarification transparente, basée sur le nombre de terminaux, sans matériel imposé ni hausse annuelle intégrée
Approche intégrée	Les failles de détection apparaissent quand les outils MDR ne s'intègrent pas à votre environnement	CyberFire offre une intégration étendue et flexible avec vos plateformes : une solution évolutive et prête pour l'avenir
Support réactif	Un service MDR doit être un véritable partenariat, pas une simple plateforme	Un interlocuteur client dédié, un faible ratio clients/expert, et un accompagnement proactif et personnalisé
Déploiement rapide	Une mise en œuvre reposant uniquement sur la documentation entraîne retards et incompréhensions	Un déploiement encadré, piloté par projet et adapté à votre infrastructure
Moins de bruit, plus de signal	Trop de prestataires continuent de transmettre toutes les alertes, même les moins pertinentes	Nous supprimons les doublons, éliminons les faux positifs et n'escaladons que les menaces à forte valeur de signal
Accès en temps réel	Des données lentes ou restreintes freinent les investigations	Accès 24h/24 et 7j/7 aux journaux, historiques de cas, alertes et rapports à la demande, sans frais cachés
Amélioration continue intégrée	Un MDR ne doit pas être figé, il doit évoluer avec votre organisation	Des améliorations constantes des capacités de détection et de la posture de sécurité, avec suivi des menaces détectées et des indicateurs de sécurité (CSI)

En savoir plus www.integrity360.com

CyberFire MDR est adopté par des organisations issues de la finance, du commerce, de la santé et bien d'autres secteurs, y compris des déploiements dépassant 60 000 terminaux. Contrairement aux offres bruyantes ou surdimensionnées, notre service éprouvé s'adresse à ceux qui recherchent la précision, la confiance et la performance. Pour en savoir plus, contactez nos experts.