Integrity360
your **security** in mind

ÉTUDE DE CAS : Comment CyberFire MDR a renforcé la résilience cyber d'un cabinet de conseil de premier plan

Le client

Un cabinet de conseil de premier plan, spécialisé dans la cybersécurité pour de grands comptes, cherchait à renforcer rapidement ses capacités de détection et de réponse — sans supporter les coûts, les délais et la complexité d'un SOC interne.

Après avoir évalué plusieurs déploiements SIEM traditionnels et services de détection managée, le cabinet a choisi CyberFire MDR.

La plateforme offrait une réponse immédiate et évolutive à un défi bien connu : volumes massifs de données de sécurité, ressources internes limitées et besoin constant d'une détection et d'une réponse rapides face aux menaces réelles.

Ce choix a marqué le début d'un partenariat durable, fondé sur l'expertise humaine des analystes, une intégration flexible des journaux (logs) et une trajectoire claire vers la maturité cyber pour les environnements clients du cabinet.

Les critères de sélection

Le cabinet a découvert CyberFire MDR lors de l'audit d'un client particulièrement performant qui l'avait déjà déployé.

Convaincue par cette expérience, l'équipe a mené des recherches supplémentaires et échangé avec d'autres clients de CyberFire MDR. Un point revenait systématiquement : ce n'est pas seulement la technologie qui fait la différence, mais les personnes derrière le service.

"J'auditionnais leur processus et j'ai vu à quel point il fonctionnait bien.

Secteur

Services (Conseil)

Le Défi

Le cabinet devait assurer la cybersécurité d'un portefeuille diversifié de clients, issus de multiples secteurs. Nombre de ces organisations ne disposaient ni des ressources, ni des compétences internes, ni de la capacité à opérer leur propre Security Operations Centre (SOC).

Un exemple typique : un client grand compte ne comptait que deux collaborateurs dédiés à la sécurité opérationnelle et utilisait un SIEM basique et inefficace.

Pour obtenir une visibilité immédiate et une capacité de réponse rapide, le cabinet avait besoin d'un partenaire MDR fiable, capable de fournir une détection de menaces haute fidélité et d'agir comme une véritable extension de son équipe cyber interne.

> ***"Le SIEM ne nous apportait aucune valeur. L'ingestion des logs était faible, et nous ne tirions rien d'utile des données."***
>
> Directeur Associé

Integrity360
your security in mind

ÉTUDE DE CAS :
Comment CyberFire MDR a renforcé la résilience cyber d'un cabinet de conseil de premier plan

Je n'avais jamais été exposé à une solution MDR auparavant, mais l'impact était évident. Et le fait que le prestataire possède une expérience régionale solide a rendu la solution encore plus pertinente." – Directeur Associé

La solution d'Integrity360

- **Mise en œuvre rapide du SOC :** CyberFire a permis au cabinet de court-circuiter les cycles d'achat traditionnels et de fournir une visibilité et une réponse immédiates aux menaces pour ses clients.

"Nous devions passer de zéro à une visibilité complète. Construire notre propre SOC n'était pas envisageable — nous avions besoin d'une solution opérationnelle immédiatement." – Directeur Associé

- **Alertes exploitables et validées par des analystes :** Plutôt que de simples notifications génériques, CyberFire MDR a fourni des alertes contextualisées et hautement fiables, accompagnées de conseils d'experts.

"Même les tickets de priorité moyenne étaient souvent d'une précision remarquable. Si quelque chose attirait notre attention, nous pouvions obtenir le contexte complet instantanément auprès des analystes." – Directeur Associé

- **Support à l'investigation et à l'escalade :** Le soutien de niveau 3 et la collaboration avec les analystes CyberFire ont permis de comprendre et traiter pleinement les alertes complexes.

Résultats et bénéfices

- **Agilité & personnalisation :** La plateforme permet un développement rapide de nouvelles analyses et une adaptation agile aux besoins spécifiques des clients.

> ***"On n'est pas bloqués par un ensemble de règles figées — CyberFire MDR évolue au rythme de nos environnements."***
>
> Directeur Associé

- **Accès à de vrais experts :** L'interaction directe avec les analystes permet un triage plus rapide, une meilleure contextualisation et des conseils stratégiques au moment où ils sont nécessaires.

> ***"Il suffit d'un appel pour échanger avec quelqu'un qui maîtrise vraiment la technologie et le paysage des menaces."***
>
> Directeur Associé

- **Amélioration continue :** Grâce à un suivi des améliorations de service et à des recommandations basées sur les menaces réelles, CyberFire MDR renforce continuellement la couverture de détection.

> ***"Nous avons eu des alertes phishing classées faible priorité, mais elles étaient parfaitement justifiées, basées sur du renseignement provenant d'autres environnements. Ce niveau de précision est rare."***
>
> Directeur Associé

Integrity360
your security in mind

ÉTUDE DE CAS :
Comment CyberFire MDR a renforcé la résilience cyber d'un cabinet de conseil de premier plan

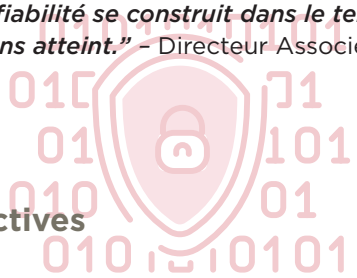
"Nous demandons souvent la télémétrie complète d'un événement. Ces informations supplémentaires nous aident à faire la corrélation en interne et à reconstituer l'incident dans son ensemble." – Directeur Associé

- **Accompagnement dans la montée en maturité des clients :** À mesure que de nouvelles sources de logs et technologies étaient intégrées, CyberFire MDR a guidé leur exploitation et leur optimisation pour garantir une valeur maximale.

"Nous ne savons pas toujours quels journaux il est pertinent d'intégrer. CyberFire MDR nous aide à faire les bons choix et à identifier nos zones de couverture insuffisante." – Directeur Associé

- **Préparation à l'automatisation :** Grâce à la fiabilité élevée des alertes phishing de CyberFire MDR, l'équipe a pu envisager l'automatisation sécurisée de certaines actions.

"Le niveau de confiance est tel que nous envisageons d'automatiser certaines réponses. Ce degré de fiabilité se construit dans le temps, et nous l'avons atteint." – Directeur Associé



Perspectives

À mesure que les environnements clients gagnent en complexité, le partenariat avec CyberFire MDR s'est approfondi. Il permet désormais une adoption plus rapide des technologies avancées, une meilleure détection des menaces et une feuille de route claire pour l'amélioration continue.

Avec une intégration renforcée des cadres tels que MITRE ATT&CK et une optimisation autour de la réponse automatisée, CyberFire MDR reste un pilier stratégique de la démarche cybersécurité du cabinet — soutenue par la technologie, portée par l'humain.

"Nous avons des échanges transparents avec l'équipe CyberFire MDR sur nos orientations futures. Ils sont ouverts, agiles et en constante amélioration."– Directeur Associé

À propos d'Integrity360

Integrity360 est l'un des principaux spécialistes européens de la cybersécurité et de la conformité PCI. Présente en Irlande, au Royaume-Uni, en Bulgarie, en Italie, en Suède, en Espagne, en France, en Lituanie, en Ukraine, en Afrique du Sud et dans les Caraïbes, l'entreprise exploite six Security Operations Centres (SOCs) situés à Dublin, Sofia, Stockholm et Le Cap.

Avec plus de 550 experts en cybersécurité, Integrity360 propose une offre complète de services professionnels, managés et de support, couvrant l'ensemble du cycle de gestion du risque cyber — de l'identification et la prévention, jusqu'à la détection, la réponse et la remédiation.

2500+
Clients professionnels

550+
Professionnels en Cybersécurité

ISO 9001 CERTIFICATION EUROPE™
ISO 27001 CERTIFICATION EUROPE™
ISO 20000-1 CERTIFICATION EUROPE™