Integrity360
your security in mind

ÉTUDE DE CAS :
CyberFire MDR facilite une transition MDR fluide pour un leader du crédit à la consommation

Le Client

Leader du secteur du crédit à la consommation, cette organisation permet à ses clients d'acquérir des biens ménagers – téléviseurs, appareils électroménagers, etc. – grâce à des solutions de crédit structurées. Propriété de l'un des groupes bancaires européens les plus importants, l'entreprise opère dans un environnement fortement réglementé, soumis à des exigences strictes de conformité telles que le Digital Operational Resilience Act (DORA).

La fonction cybersécurité interne, dirigée par une équipe dédiée rattachée au responsable Groupe IT Governance, Risk & Compliance, joue un rôle central dans la protection de l'entreprise. Ses missions couvrent la gestion des incidents, la sensibilisation cyber, la gouvernance des risques, et l'alignement des contrôles opérationnels sur les exigences du groupe.

"J'aime le côté résolution de problèmes en cybersécurité — connecter les personnes, les processus et la technologie pour réduire le risque. C'est là que CyberFire MDR nous a permis de garder une longueur d'avance." — Responsable Risques et Conformité

Les critères de sélection

Le processus d'appel d'offres (RFP) était particulièrement exigeant, évaluant plusieurs prestataires selon des critères métiers et techniques clés :

Secteur

Services financiers aux particuliers

Le Défi

Avant de collaborer avec CyberFire MDR, l'entreprise faisait appel à un autre fournisseur MDR, mais plusieurs obstacles limitaient fortement son efficacité opérationnelle :

- **Surcharge d'alertes :** le service précédent enregistrait presque chaque événement comme un incident, provoquant une fatigue d'alerte et un manque de priorisation.
- **Complexité on-premise :** l'entreprise reposant principalement sur des infrastructures sur site, elle avait besoin d'un partenaire MDR capable d'intégrer profondément ces environnements sans dépendre excessivement du cloud.
- **Pression réglementaire mondiale :** la maison mère européenne imposait un cadre de détection SOC structuré, devant être répliqué localement de manière traçable et auditée.
- **Urgence :** en raison de difficultés avec le fournisseur précédent, la transition complète devait être achevée en moins de deux mois, sans interruption d'activité.

> *"Nous n'avions aucune marge de manœuvre. Le processus de gestion des incidents ne pouvait pas s'arrêter, même une seule journée."*
>
> Responsable Risques et Conformité

Integrity360
your security in mind

ÉTUDE DE CAS :
CyberFire MDR facilite une transition MDR fluide pour un leader du crédit à la consommation

- Présence locale garantissant un support direct, réactif et une connaissance approfondie du secteur
- Expertise dans la gestion d'environnements hybrides et 100 % on-premise
- Capacité à aligner les détections CyberFire sur le cadre SOC global de la maison mère
- Souplesse dans l'adaptation des rapports, indicateurs et processus pour répondre aux exigences de gouvernance du client
- Compatibilité culturelle avec une équipe évoluant sous forte pression et supervision constante

"Nos exigences globales étaient strictes : si vous ne répondiez pas au niveau attendu, vous étiez éliminé. CyberFire a non seulement répondu aux critères, mais les a dépassés." – Responsable Risques et Conformité

La solution d'Integrity360

CyberFire a déployé un environnement MDR sur mesure en seulement six semaines, incluant les validations de conformité et approbations internes.

Principaux volets du dispositif :

- **Détections mappées :** alignement des capacités de détection CyberFire avec un cadre européen rigoureux de "use cases" pour assurer la traçabilité et la conformité.
- **Supervision humaine en continu :** un SOC 24/7 animé par des analystes experts contextualisant chaque alerte avant escalade.

> ***"Ce n'est pas la quantité d'alertes qui compte, c'est leur qualité. CyberFire nous a permis de réduire le bruit et de nous concentrer sur ce qui importe vraiment. Leur équipe connaît nos personnes, nos processus et notre environnement. Ce contexte fait toute la différence."***
>
> Responsable Risques et Conformité

Résultats & Bénéfices

- Déploiement MDR complet en six semaines, sans interruption du processus de gestion des incidents
- Réduction significative des faux positifs, libérant du temps pour les opérations à forte valeur ajoutée
- Alignement transparent avec les exigences de reporting SOC internes et externes
- Détection de menaces auparavant non identifiées grâce à un ajustement avancé des règles de détection
- Revue de service régulière et processus d'amélioration continue assurant pertinence et performance
- Partenariat solide fondé sur la réactivité, la compréhension métier et la confiance mutuelle

> ***"La capacité de CyberFire à s'ajuster et reconfigurer ses processus pour suivre nos mises à jour de politiques, parfois à très court terme, en fait une véritable extension de notre équipe."***

ÉTUDE DE CAS :
CyberFire MDR facilite une transition MDR fluide pour un leader du crédit à la consommation

- **Reporting personnalisé :** les rapports mensuels ont été enrichis de métriques et KPI spécifiques aux exigences d'audit du client.
- **Flexibilité continue :** CyberFire a su s'adapter rapidement à l'évolution des politiques internes, notamment concernant la conservation des journaux (logs) et le format de reporting.

Perspectives

Le client collabore désormais avec CyberFire pour étendre la détection et la réponse aux journaux applicatifs métiers — notamment les plateformes web développées en interne et les systèmes transactionnels. Cette nouvelle phase permettra une analyse plus fine des comportements utilisateurs et une détection renforcée des menaces non conventionnelles au niveau applicatif.

"Notre environnement évolue, tout comme nos risques. CyberFire a démontré sa capacité à évoluer avec nous." – Responsable Risques et Conformité

CyberFire continue de jouer un rôle essentiel dans la stratégie de cybersécurité de l'organisation, en renforçant les équipes, en faisant progresser la gouvernance et en s'adaptant en permanence à un paysage de menaces en mutation.

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™