Integrity360

your **security** in mind

CyberFire MDR

CyberFire MDR

Le **service CyberFire MDR d'Integrity360 est une solution clé en main managée de détection & réponse**, conçue pour offrir aux organisations une protection continue et silencieuse contre les cybermenaces.

Ce service se distingue par sa plateforme propriétaire CyberFire, développée en interne, qui confère un niveau d'efficacité et de précision supérieur à celui des solutions MDR classiques.

En intégrant CyberFire à vos sources de logs, systèmes d'alerte et environnements critiques, nous garantissons une couverture complète et homogène de votre sécurité.

Nos experts exploitent un large éventail de données et des systèmes de détection de pointe pour identifier avec précision les activités suspectes et hiérarchiser les menaces réelles.

Face à l'évolution constante et à la sophistication croissante des cyberattaques, les entreprises doivent adopter une approche proactive de la détection et de la réponse.

Les capacités de CyberFire MDR vont bien au-delà de la simple génération d'alertes : nos analystes différencient rapidement les alertes exploitables des faux positifs, afin de ne remonter que les menaces avérées.

Cette approche ciblée **libère les ressources internes** du traitement d'événements non pertinents et **renforce l'efficacité opérationnelle.**

Dès qu'une menace est confirmée, nos analystes mènent une enquête approfondie et fournissent des recommandations de réponse immédiate, assurant ainsi un confinement et une remédiation rapides.

Notre priorité : vous protéger du bruit inutile, tout en maintenant une transparence totale et une collaboration fluide avec vos équipes, pour qu'elles puissent se concentrer sur leurs missions stratégiques.

CyberFire MDR évolue en permanence pour anticiper les nouvelles techniques d'attaque, grâce à l'amélioration continue de ses règles de détection, de ses capacités d'analyse et de son renseignement sur la menace.

En choisissant Integrity360, vous bénéficiez d'une solution MDR de classe mondiale, alliant expertise humaine, technologies propriétaires et approche proactive de la cyberdéfense.

Qu'est-ce que le MDR ? Quels en sont les bénéfices ?

La Détection & Réponse Managée (MDR) est un service de cybersécurité proactif qui renforce la capacité d'une organisation à détecter, analyser et répondre aux menaces en temps réel. Contrairement aux solutions traditionnelles, le MDR assure une surveillance continue, une détection avancée des menaces et une réponse pilotée par des experts, permettant de neutraliser les attaques avant qu'elles n'aient un impact.

Principaux avantages :

- **Détection et réponse rapides :** identification et neutralisation des menaces avant leur propagation.
- **Votre équipe reste concentrée :** suppression automatique des faux positifs pour se concentrer sur les véritables incidents.
- **Amélioration continue :** adaptation dynamique aux nouvelles menaces grâce à l'actualisation permanente des règles et scénarios de détection.
- **Analyse et investigation expertes :** une équipe de spécialistes cybersécurité dédiée à l'investigation et à la remédiation.
- **Accompagnement à la mise en conformité :** gestion centralisée des journaux, traçabilité des incidents et reporting conforme aux cadres réglementaires (DORA, NIS2, ISO 27001, PCI DSS, etc.).
- **Surveillance 24h/24, 7j/7, 365 jours/an :** protection en continu contre les menaces.
- **Allègement des charges internes :** réduction des tâches opérationnelles quotidiennes pesant sur vos équipes et votre budget.
- **Visibilité renforcée :** un tableau de bord unifié pour suivre les incidents et leur résolution.
- **Optimisation des coûts :** diminution des dépenses liées à la sécurité interne tout en augmentant la couverture et la qualité du service.

Comment choisir un service et partenaire MDR

Gestion de projet solide

Diverses parties prenantes peuvent être impliquées lors de la mise en œuvre d'une solution MDR (incluant le déploiement, la configuration et le processus d'onboarding.

Un pilotage de projet dédié, incluant une équipe de déploiement MDR, garantit une mise en œuvre fluide, une communication claire et une intégration rapide des capacités opérationnelles. L'équipe en charge de la gestion de projet assure le lien opérationnel client-partenaire MDR durant l'initialisation du service, garantissant une montée en valeur fluide et accélérée des fonctionnalités MDR.

Flexibilité et évolutivité

Si s'affranchir de la dépendance à un fournisseur demeure prioritaire, le choix d'un prestataire MDR doit cependant garantir l'évolutivité du service selon les besoins et la croissance de l'organisation. Même si certains services ne sont pas requis actuellement, cela évoluera inévitablement avec la transformation du paysage des cybermenaces.

L'analyse des modèles tarifaires - qu'ils reposent sur les terminaux, les événements par seconde, l'ingestion de logs ou la couverture géographique - conditionne directement la capacité d'adaptation et l'optimisation budgétaire des investissements sécuritaires à long terme.

Déploiement et onboarding rapides

La rapidité d'intégration est essentielle : plus le service est opérationnel tôt, plus vite votre organisation bénéficie d'une détection active. Le déploiement et la configuration de l'infrastructure de sécurité MDR pour détecter les incidents cyber dans l'environnement réseau spécifique du client peut nécessiter quelques semaines.

Cela englobe l'ensemble du processus, depuis la consultation initiale jusqu'à la mise en œuvre opérationnelle.

Renseignement sur la menace (Threat Intelligence)

Les fournisseurs MDR disposent d'un accès à diverses sources de renseignement sur les menaces, internes et externes en temps réel. L'accès continu aux flux de threat intelligence permet au prestataire MDR d'identifier et de détecter de nouvelles menaces en temps réel. Le fournisseur MDR doit élaborer une threat intelligence qualifiée permettant un enrichissement contextuel des mécanismes de détection.

Visibilité sur le cloud

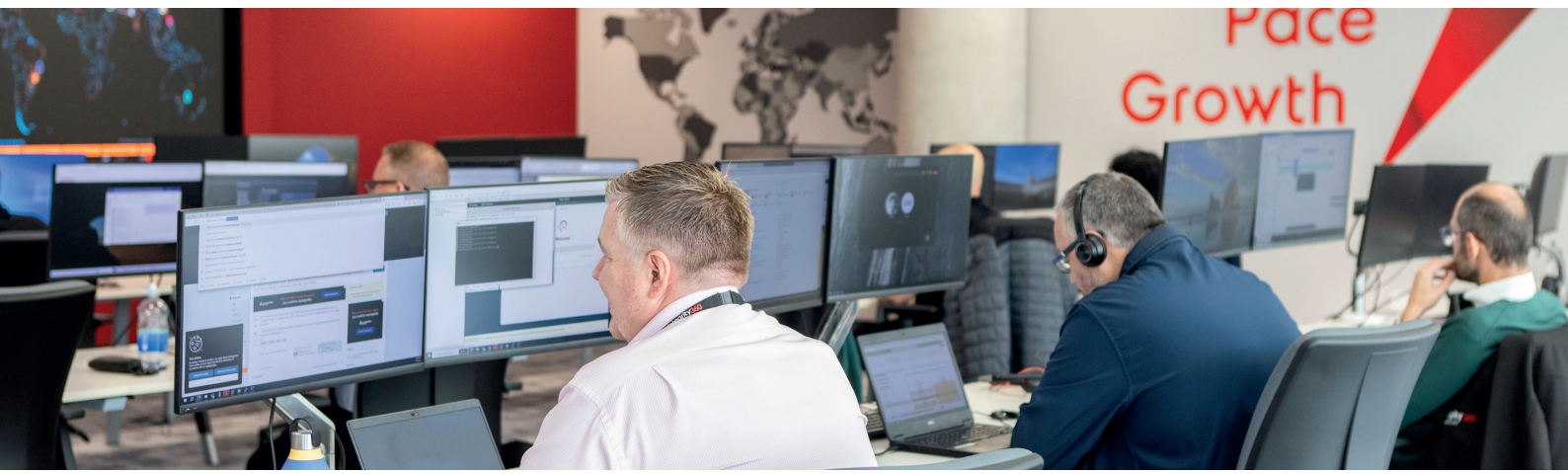
Les processus métier critiques s'appuyant sur des infrastructures cloud nécessitent des capacités MDR multi-cloud. Cela doit englober une visibilité transparente sur les environnements on-premise, cloud public et cloud privé.

Disponibilité et transparence 24/7

La transparence sur les capacités de détection hors heures ouvrables et la disponibilité 24/7 des équipes MDR constituent des prérequis non négociables pour une couverture sécuritaire continue.

Gestion de la conformité et reporting

Le prestataire MDR doit garantir la visibilité et l'accès requis aux données de sécurité pour la production de rapports de conformité. Il doit proposer des rapports réglementaires pré-configurés, automatiquement alimentés par les métriques de sécurité de l'organisation et adaptés aux spécificités de son environnement. Dans un contexte réglementaire en constante évolution, un fournisseur MDR capable d'accompagner les audits de conformité et les obligations de reporting permet à l'organisation de réaliser des économies substantielles en temps et en ressources.



L'offre CyberFire MDR d'Integrity360

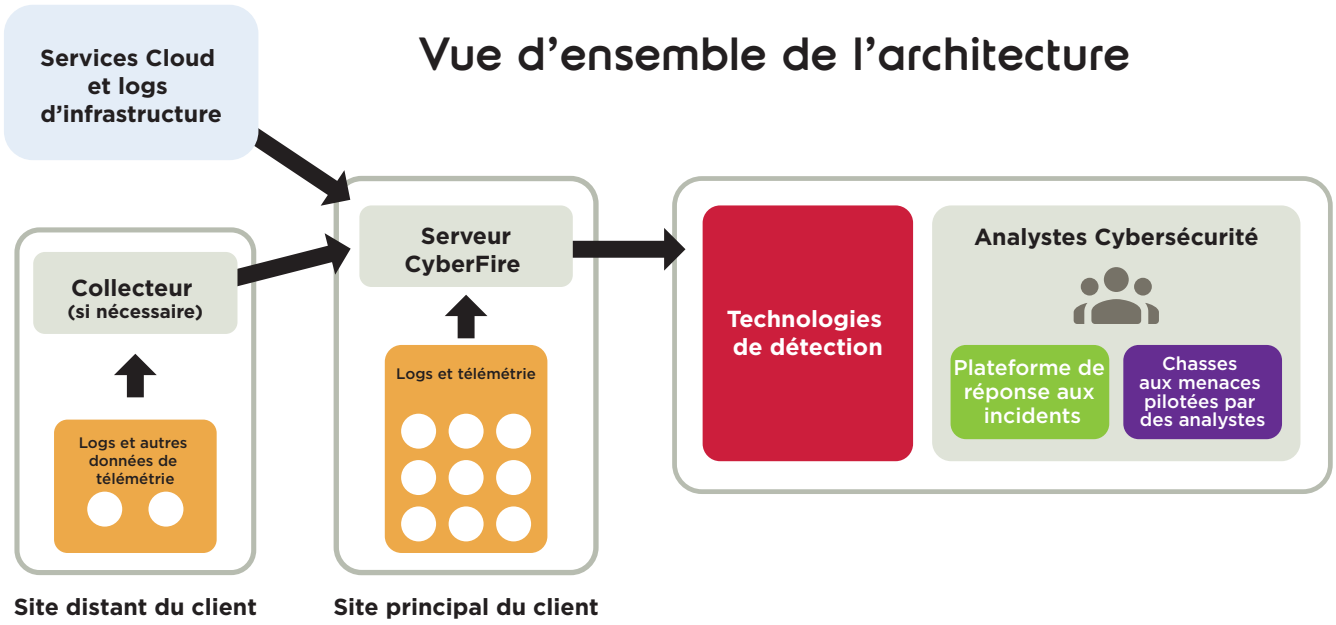
Une solution entièrement managée, conçue pour renforcer votre posture de sécurité et accélérer votre capacité de réponse aux menaces.

Principales fonctionnalités :

- **Déploiement clé en main :** intégration rapide dans tout environnement de sécurité existant.
- **Plateforme CyberFire exclusive :** agrégation et corrélation des logs, sans besoin de SIEM client – Stockage de l'ensemble des logs inclus dans le service CyberFire MDR sans nécessité de SIEM client.
- **Détection des menaces haute fidélité :** ingénierie de détection avancée et règles de détection innovantes exclusives à CyberFire MDR et prise en charge des détections tierces
- **Déploiement et surveillance d'honeypots** inclus en standard pour la détection précoce d'attaques
- **Triage, analyse et réponse :** filtrage des faux positifs et réponse rapide aux incidents – faible bruit garanti.
- **Threat Hunting proactif :** recherche active de menaces latentes et d'activités anormales.
- **Améliorations et enrichissements continus** des capacités de détection pour devancer l'évolution des techniques d'attaque.
- **Support d'incidents critiques :** assistance en temps réel lors d'incidents majeurs.
- **Reporting technique et exécutif exhaustif** pour une transparence totale.
- **Portail client 24/7 :** accès à l'historique complet des alertes, recommandations et rapports.
- **Accompagnement pour le renforcement de la sécurité :** conseil continu et suivi des menaces défensives, améliorations sécuritaires pour un renforcement continu de la posture de sécurité.
- **Reporting étendu :** support optionnel pour des rapports approfondis et avancés, l'archivage de logs à long terme et le mise en conformité réglementaire.
- **Détection de fuites d'identifiants :** scanning optionnel du dark web pour repérer les mentions du domaine client et fuites d'identifiants.

Fonctionnement de CyberFire MDR

Le schéma d'architecture ci-dessous illustre la manière dont CyberFire collecte les données au sein d'un environnement type. Il est possible d'installer plusieurs collecteurs CyberFire si nécessaire, notamment dans les contextes où la bande passante entre des sites distants est limitée.



Toutes les alertes MDR déclenchées par les détecteurs sont analysées : un dossier est ouvert si nécessaire, et des actions correctives sont proposées.

Lorsque l'intervention des équipes internes du client est requise, les ingénieurs de réponse CyberFire fournissent des instructions claires pour mise en œuvre, à destination des ingénieurs, administrateurs ou collaborateurs du client, y compris ceux disposant d'une expérience limitée en cybersécurité.

L'objectif de CyberFire MDR est d'accompagner chaque client jusqu'à la résolution complète de chaque incident.

Tous les cas investigués doivent être clôturés ; les ingénieurs de réponse CyberFire sont responsables du suivi et de la fermeture des dossiers.

Les cas clos peuvent être classés comme :

- Vrai positif, avec ou sans impact métier
- Faux positif
- Indéterminé, lorsqu'aucune cause racine n'a pu être identifiée
- Autre, lorsque l'origine est liée à une erreur de configuration, un test de sécurité ou tout autre événement ne relevant pas d'un vrai ou faux positif.

La valeur ajoutée de CyberFire MDR par Integrity360

Integrity360 est l'un des principaux spécialistes européens de la cybersécurité et de la conformité PCI, présent au Royaume-Uni, en Irlande, en Bulgarie, en Italie, en Suède, en Espagne, en France, en Lituanie, en Ukraine, en Afrique du Sud et dans les Caraïbes. Nos six centres opérationnels de sécurité (SOC) situés à Madrid, Dublin, Sofia, Stockholm, Naples et Le Cap nous permettent d'assurer une détection et une réponse continues, 24 h/24 et 365 jours par an, garantissant une couverture complète pour votre organisation.

Ce qui différencie CyberFire MDR

- **Solution clé en main :** déploiement rapide et économique dans tout type d'environnement client.
- **Aucun coût variable de collecte SIEM :** un modèle tarifaire basé sur le nombre d'endpoints, sans imprévisibilité liée au volume de logs.
- **Détection avancée :** des règles d'ingénierie exclusives et innovantes assurent une identification précise des menaces.
- **Évolution continue du service :** des mises à jour régulières renforcent les capacités de détection et la posture de sécurité face aux menaces émergentes.
- **Réduction du bruit et contrôle qualité :** seules les alertes pertinentes et à forte valeur de détection sont remontées au client – aucune surcharge d'alertes inutiles.
- **Amélioration continue de la sécurité :** suivi des menaces et recommandations proactives pour renforcer durablement la posture de sécurité.
- **Expert dédié à la réussite client :** un interlocuteur attitré assure un accompagnement rapproché et un suivi constant des améliorations de sécurité.
- **Déploiement rapide :** une solution MDR prête à l'emploi, intégrable sans effort dans tout environnement.
- **Réduction des coûts :** tarification claire et prévisible, sans frais d'ingestion SIEM imprévus.
- **Détection et réponse accélérées :** alertes de haute qualité, investigation et assistance à la réponse en temps réel.
- **Amélioration continue :** CyberFire évolue en permanence pour offrir des détections toujours plus précises et une sécurité renforcée.
- **Perturbations minimisées :** CyberFire vous protège de la surcharge d'alertes en ne remontant que les menaces réellement critiques.
- **Renforcement de la posture de sécurité :** identification et remédiation proactives des vulnérabilités avant qu'elles ne deviennent des incidents.

Pourquoi choisir Integrity360?

Choisir un partenaire en cybersécurité est une décision stratégique pour toute entreprise. Voici quelques-unes des raisons de faire confiance à Integrity360 :

- **Expérience :** plus de 420 experts en cybersécurité, ingénieurs et analystes, disposant d'une expérience internationale pour protéger votre organisation contre les menaces les plus complexes et évolutives.
- **Réputation :** nous avons gagné la confiance de milliers d'entreprises dans le monde grâce à notre expertise technique reconnue, notre approche orientée client et notre expérience éprouvée dans la conduite de projets de sécurité complexes.
- **Solutions sur mesure :** une approche personnalisée de la cybersécurité, fondée sur une compréhension fine des besoins de chaque client et la recommandation des solutions les plus adaptées.
- **Passion et engagement :** une équipe animée par la passion de la cybersécurité et engagée à délivrer une protection optimale aux organisations que nous accompagnons.
- **Certifications :** le plus haut niveau de certifications techniques et de compétences du marché.
- **Partenariats :** des relations solides avec les principaux éditeurs et partenaires technologiques.
- **Reconnaissance :** classé par Gartner dans quatre de ses Market Guides.
- **Présence internationale :** six SOC répartis en Irlande, en Italie, en Espagne, en Suède, en Bulgarie et en Afrique du Sud.

integrity360.com
info@integrity360.com

Londres, UK
+44 20 3397 3414

Kiev, Ukraine
+38 504 701 125

Stockholm, Suède
+46 8 514 832 00

Paris, France
contact@holiseum.com

Dublin, Irlande
+353 1 293 4027

Madrid, Espagne
+34 910 767 092

Sofia, Bulgarie
+359 2 491 0110

Zurich, Suisse
+41 44 421 3336

Ludwigsburg, Allemagne
+49 7141 48799 80

Le Cap, Afrique du Sud
+27 21 100 3774