Maîtriser la cybersécurité avec MDR :

Le guide ultime du service de détection et de réponse gérées

Sécurité numérique
Protégeons le progrès.

Introduction : Une approche préventive multicouche

La vitesse à laquelle le monde évolue dépasse la capacité de gestion des responsables de la protection des réseaux. Ils sont confrontés à un adversaire agile et déterminé, armé jusqu'aux dents des technologies les plus récentes. Comme le potentiel d'attaque des entreprises s'étend avec chaque nouvel investissement numérique, les risques et les coûts d'une grave violation de la sécurité augmentent. Le coût moyen d'une violation de données au niveau mondial s'élève aujourd'hui à près de 4,9 millions de dollars américains.

Afin de **gérer ces risques croissants**, les organisations devraient envisager d'adopter une **approche proactive**, **axée sur la prévention** conçue pour minimiser le potentiel d'attaque, réduire les coûts et la complexité, et améliorer l'hygiène informatique.

Plus de la moitié des organisations victimes de violations sont confrontées à des pénuries importantes de personnel de sécurité. Ce problème représente une augmentation de

26,2 %

entre 2023 et 2024.
Source : *IBM: Cost of a Data Breach Report 2024*.

Les assaillants n'ont besoin de réussir qu'une seule fois pour causer des dommages importants. C'est pourquoi l'approche la plus mature en matière de cybersécurité combine une prévention multicouche à la détection et à la réponse. Cependant, les défis auxquels sont confrontées de nombreuses organisations sont les suivants :

LES LACUNES EN MATIÈRE DE COMPÉTENCES ET DE CONNAISSANCES ont une incidence sur leur capacité à mener des opérations de sécurité 24 heures sur 24, 7 jours sur 7 et 365 jours par an.

LA COMPLEXITÉ des outils de détection et de réponse signifie que certaines entreprises n'ont peut-être personne en interne pour les utiliser.

LES CYBERMENACES SONT DE PLUS EN PLUS SOPHISTIQUÉES et percutantes, ce qui permet aux assaillants d'atteindre leurs objectifs plus rapidement.

LES BUDGETS SONT LIMITÉS, en particulier pour les gros achats ponctuels d'infrastructures de détection et de réponse et d'opérateurs humains.

LES PRESSIONS EN MATIÈRE DE CONFORMITÉ s'intensifient, amplifiant l'impact négatif des attaques en cas de non-conformité.

C'est pour cette raison que de nombreuses organisations se tournent vers le service de **détection et de réponse gérées** (**MDR**). Ce faisant, elles peuvent accéder à la puissance combinée d'une équipe des opérations de sécurité tierce experte à l'aide d'outils d'IA sophistiqués pour une réponse rapide et un confinement des menaces. Les meilleurs services MDR automatisent le suivi et le signalement afin d'améliorer la conformité et de renforcer en permanence la cyberrésilience. Les équipes internes peuvent ainsi se dédier à des tâches stratégiques de plus grande valeur pour l'entreprise.

4,88
millions de dollars

c'est le coût moyen d'une violation de données en 2024, ce qui représente la plus forte augmentation depuis la pandémie.
Source : *Cost of a Data Breach Report 2024*.

Chapitre 1 : Pourquoi votre entreprise a-t-elle besoin de MDR

Aujourd'hui, les organisations continuent de développer des infrastructures et des applications infonuagiques, de prendre en charge le télétravail et d'étendre leurs chaînes d'approvisionnement numériques et traditionnelles. Cela offre davantage d'opportunités aux assaillants très motivés, qui exploitent de plus en plus l'IA et les outils automatisés, les offres « en tant que service » et plus encore pour se perfectionner, se professionnaliser et intensifier les attaques. Dans ce contexte, **le MDR devient une nécessité pour les entreprises de toutes tailles**.

DE LA PRÉVENTION AU MDR

Les équipes de sécurité internes peinent à gérer le volume, la diversité, la vitesse et, dans quelques cas, la sophistication des menaces auxquelles leur organisation est confrontée. Le rançongiciel fait partie des menaces les plus sérieuses. Les rançongiciels en tant que services (RaaS) sont un « secteur » souterrain hautement compétitif dans lequel les gangs innovent en permanence pour contourner les contrôles de sécurité et accroître leurs profits. Selon les experts en matière de sécurité du gouvernement britannique, la menace devrait s'intensifier à mesure que de plus en plus d'adversaires se procurent des outils d'IA.

La fréquence des attaques de rançongiciel contre les gouvernements, les entreprises, les consommateurs et les périphériques devrait atteindre

toutes les deux secondes d'ici 2031.

Source : *Cybercrime Magazine: Top 10 Cybersecurity Predictions and Statistics For 2024*.

« Les services d'IA facilitent l'accès, augmentent le nombre de cybercriminels et renforcent leurs capacités en améliorant l'ampleur, la vitesse et l'efficacité des méthodes d'attaques existantes. »

James Babbage, Directeur général des menaces à l'Agence nationale de lutte contre le crime.

Les assaillants utilisent ces outils pour réduire le temps qui s'écoule entre l'accès initial et le vol de données ou le déploiement d'un rançongiciel. Il s'agit d'un défi non seulement dans un contexte de rançongiciel, mais aussi de l'ensemble des menaces auxquelles sont confrontées les organisations : des logiciels malveillants et botnets de cryptominage aux chevaux de Troie et logiciels espions bancaires.

L'impact cumulé de ces tendances doit mener les leaders de la sécurité informatique à une conclusion inéluctable. La motivation des mauvais acteurs à réussir est souvent plus grande que la préparation des entreprises à l'aide de mesures préventives. Ils se donnent beaucoup de mal pour s'introduire dans l'environnement de l'entreprise sans être vus. C'est pourquoi les organisations doivent **associer la prévention à la détection et aux mesures de réponse**. C'est ce que fait l'approche de prévention d'ESET, **en combinant plusieurs couches de technologie de sécurité**. Elle cherche à protéger les entreprises en empêchant les codes et les acteurs malveillants de pénétrer dans le système de l'utilisateur ou de l'endommager.

L'hameçonnage était le vecteur d'attaque le plus coûteux et le plus fréquent en 2024, avec un coût de

4,88 millions

et une part de

15 % de d'euros

toutes les attaques.

Source : *IBM: Cost of a Data Breach Report 2024*.

Toutefois, si ces mesures sont contournées par des acteurs perfectionnés, il existe des moyens de détection et de réponse rapides et fiables pour atténuer les menaces avancées qui parviennent à compromettre un système. C'est comme si vous verrouilliez toutes vos portes et fenêtres, mais que vous installiez ensuite des alarmes à détection de mouvement afin de détecter toute activité suspecte dans l'éventualité où quelqu'un parviendrait à s'infiltrer dans la maison.

Le **XDR** est un actif clé dans ce cas. Il permet aux équipes des opérations de sécurité d'obtenir une **visibilité inégalée** sur leur environnement informatique depuis un point de vue unique afin de détecter toute anomalie indiquant des menaces à l'aide d'alertes très fiables. Le XDR est une évolution de l'EDR qui optimise la détection, l'enquête, les réponses apportées et la traque des menaces en temps réel.

Le XDR unifie les détections de terminaux pertinents pour la sécurité avec la télémétrie des outils de sécurité et d'entreprise, comme l'analyse et la visibilité des réseaux, la sécurité des courriels, la gestion des identités et des accès, la sécurité du nuage, et bien plus

encore. Il s'agit d'une plateforme native en nuage et établie sur une infrastructure de mégadonnées afin de fournir de la flexibilité, de l'évolutivité et des possibilités d'automatisation aux équipes de sécurité.

LE XDR VOUS PERMET DE RÉPONDRE À PLUSIEURS QUESTIONS CLÉS EN MATIÈRE DE CYBERATTAQUE :

Comment cela a-t-il commencé?
Où cela a-t-il commencé?
Quand cela a-t-il commencé?
Quels sont les terminaux infectés?
La menace est-elle contenue?
Comment pouvons-nous empêcher cela à l'avenir?

Il vous aide surtout à prendre des mesures correctives rapides pour résoudre les incidents avant qu'ils n'impactent trop lourdement l'organisation.

Toutefois, même avec l'aide du XDR, les équipes des opérations de sécurité rencontrent des **défis considérables** d'un point de vue organisationnel, en particulier les lacunes en matière de compétences, la complexité des outils, les contraintes de budget et de ressources, et l'intégration des outils, sans parler d'évolution rapide du paysage des menaces. **C'est pour cette raison que de nombreuses organisations se sont tournées vers le MDR** : le moyen le plus efficace de détecter et de contenir des menaces sophistiquées en constante évolution.

COMMENT LE MDR RÉPOND AUX MENACES CONTEMPORAINES

Bien que le MDR varie en fonction du fournisseur, il doit comprendre au moins une variante des éléments suivants :

- **Détection et surveillance des menaces 24 heures sur 24 et 7 jours sur 7 :** surveillance continue du réseau d'une entreprise, de ses terminaux et de ses environnements en nuage.

- **Recherche proactive des menaces :** contrairement aux mesures de sécurité traditionnelles qui réagissent aux alertes, le MDR implique une recherche proactive des menaces qui permet d'identifier les menaces persistantes avancées et les vulnérabilités jour zéro.

51 %
est le nombre

d'organisations qui ont formellement établi des méthodes de recherche des menaces en 2024, contre 35 % en 2023.
Source : *SANS: The Evolution of Enterprise Threat Hunting: Detailed Insights from the SANS 2024 Survey*.

- **Analyse et réponse d'experts** :
  l'expertise des professionnels de la sécurité permet une analyse nuancée et une prise de décision rapide, ce qui est essentiel pour faire face à des incidents de sécurité complexes.

- **Veille mondiale sur les menaces** :
  des données de télémesure précises, actuelles et pertinentes collectées dans le monde entier fournissent des informations exploitables pour une réponse rapide aux incidents et une recherche optimisée des menaces.

Les organisations qui utilisent des données de télémétrie peuvent

améliorer de
60 %

leur capacité de gérer les vulnérabilités et les menaces par rapport à celles qui s'appuient uniquement sur des mesures de sécurité traditionnelles.
Source : *Forrester: The Four Steps for More Proactive Security, 2024*.

- **Amélioration continue :**
  en analysant les incidents passés, en utilisant la veille sur les menaces, en se concentrant sur les menaces réelles et en fournissant des bilans et des rapports réguliers sur la sécurité, les services MDR aident à prévenir la récurrence d'attaques similaires en permettant aux équipes d'améliorer leur cyberrésilience.

FONCTIONS CLÉS DU MDR

Le MDR peut apporter des avantages considérables aux organisations qui souhaitent atténuer les cyberrisques, mais qui ne disposent pas des ressources internes nécessaires, en les aidant efficacement à combler les lacunes en matière de compétences, à réduire les coûts et à améliorer la détection et la réponse. Une solution haute performance doit permettre aux organisations d'effectuer les actions suivantes :

Surveiller
Des experts en détection des menaces suivent l'ensemble de l'environnement informatique du client et surveillent activement les logiciels malveillants et les groupes MPA afin de fournir le niveau le plus élevé de connaissance de la situation.

Détecter
Les assaillants peuvent s'infiltrer dans les défenses du périphérique de mille façons, mais en tirant parti de l'analyse du comportement, ils peuvent être repérés et faire l'objet d'une correction rapide.

Trier
Une première évaluation et un classement des alertes permettent de filtrer les faux positifs et de recueillir les informations nécessaires.

Hiérarchiser
Les analyses intelligentes classent ces alertes en fonction de leur gravité afin de s'assurer que les menaces les plus critiques sont traitées en premier. Il s'agit d'une phase essentielle du processus du MDR étant donné que les équipes informatiques peinent souvent à gérer un nombre trop important d'alertes.

Enquêter
Les outils automatisés et l'expertise humaine se combinent pour approfondir les alertes, en effectuant des analyses des données et des journaux afin de comprendre leur nature et leur portée. Il faudra ensuite déterminer si une alerte est légitime ou non, et quelles mesures doivent être prises pour la résoudre.

Répondre
Un service MDR efficace fournira soit des actions de réponse de base pour bloquer et contenir la menace, soit un confinement et une correction complète de tous les systèmes compromis. Cette deuxième option pourrait inclure une réinitialisation de mots de passe, la mise à jour corrective de certains terminaux ou même la reconfiguration d'ordinateurs.

Les avantages de l'externalisation des activités de détection et de réponse sont simples, mais irréfutables :

- le fournisseur du service MDR se charge de toute la gestion de la technologie dorsale, permettant au personnel de se dédier à des tâches stratégiques de grande valeur plutôt que de crouler sous les alertes de sécurité;
- le fournisseur du service MDR peut également optimiser la technologie dorsale afin de s'aligner surle profil de risque et l'infrastructure de chaque client;
- lorsqu'un tiers gère les processus de détection et de réponse, les organisations n'ont pas besoin de proposer de salaires excessivement élevés pour attirer et retenir les meilleurs talents en matière de cybersécurité;
- les clients peuvent bénéficier des économies d'échelle de leur fournisseur, de sa capacité à attirer les meilleurs talents et de sa connaissance des organisations d'autres clients et des environnements de menace.

FONCTIONNALITÉS ESSENTIELLES À RECHERCHER DANS UNE SOLUTION MDR

Avec un si grand nombre de solutions MDR inondant le marché, les organisations peuvent facilement **se sentir perdues**. Envisagez de collaborer avec un fournisseur en mesure de vous offrir au moins les éléments suivants :

Intégration et adaptation rapides
Les règles de détection, les exclusions et les paramètres devront être adaptés à chaque environnement informatique et aux menaces auxquelles l'organisation est confrontée. Il est souhaitable d'accélérer l'intégration, mais pas au détriment des performances de détection, qui doivent être optimisées dès le premier jour.

➜ N'oubliez pas que la protection MDR s'améliore généralement avec le temps.

Vitesse
Réduisez votre temps de détection et de réponse aux incidents de plusieurs mois à quelques minutes avec votre fournisseur du service MDR. Vous devez arrêter l'attaque dans ses premières phases (découverte, déplacement latéral, persistance) avant que la charge utile ne soit exécutée.

Service assuré 24 heures sur 24 et 7 jours sur 7
Les assaillants opèrent à partir de tous les fuseaux horaires et frappent souvent aux premières heures ou pendant les fins de semaine et les jours fériés. Cela signifie que le service MDR doit fonctionner en continu. Les indicateurs de compromission et d'attaque doivent faire l'objet d'une enquête immédiate, en temps réel.

Solution facile à utiliser avec une interface simple et une courbe d'apprentissage réduite
Cela rend la solution accessible même pour les personnes qui débutent dans le domaine de la sécurité informatique. Le tableau de bord, facile à utiliser, donne une vision claire de l'état de la sécurité et des alertes importantes.

Notifications personnalisables et options de signalement avancées
Afin de recevoir automatiquement ou à la demande des rapports sur les incidents, l'état de l'environnement et d'autres mises à jour.

Il est ainsi facile de présenter l'état de la cybersécurité aux cadres, de recevoir des alertes en temps opportun et de générer des rapports exploitables pour les audits et la conformité.

Compatibilité parfaite avec différentes infrastructures
Intégration efficace avec des outils, tels que SIEM, SOAR, les outils de création de tickets et bien d'autres. Que vous ayez des environnements avec plusieurs systèmes d'exploitation, des logiciels de sécurité existants ou des installations locales et dans le nuage, vous voulez une intégration sans problème.

Un chevauchement technologique complet
La technologie sous-jacente est un élément essentiel d'une solution MDR. Elle doit inclure la détection et la réponse au niveau des terminaux ou étendues (XDR), la gestion des informations et des événements de sécurité (SIEM) ainsi que l'orchestration, l'automatisation et la réponse en matière de sécurité (SOAR). Ces éléments doivent être fournis par le fournisseur MDR ou par des outils tiers liés par des API.

Automatisation et IA
L'IA peut jouer un rôle important dansl'identification de comportements anormaux et l'analyse de grands volumes de données pour trouver des signes de compromission ou d'attaque.

L'automatisation permet également d'exécuter rapidement une série d'actions afin d'isoler les systèmes et de contenir les menaces. Toutefois, ces méthodes doivent toujours être considérées comme une

assistance et non comme un substitut à l'expertise des analystes humains.

Intelligence humaine
Bien que l'IA et l'automatisation soient importantes, elles ont des limites que seuls les experts humains peuvent traiter efficacement. Les professionnels expérimentés de la cybersécurité peuvent ajouter une compréhension contextuelle aux anomalies comportementales signalées par l'IA afin de déterminer si une alerte est réellement malveillante.

➜ Cela permet de réduire les faux positifs. Les humains sont également plus à même de s'adapter en temps réel aux menaces nouvelles et émergentes.

Veille sur les menaces
Des flux de veille sur les menaces régulièrement mis à jour, générés par le fournisseur MDR ou par des tiers, sont un élément clé de tout service de MDR efficace. Les mises à jour doivent être collectées à partir de données de télémétrie et traitées par des équipes d'experts en veille sur les menaces afin de révéler les méthodes d'attaque et les contre-mesures efficaces.

Recherche des menaces
Une recherche continue et systématique des menaces doit faire partie de l'offre standard de tout service de MDR, afin d'éradiquer les attaques les plus évasives.

Correction
Aucune règle n'a été établie quant à la question de savoir si c'est le fournisseur de service ou le client qui doit s'occuper de la correction ou de l'atténuation une fois qu'une menace a été découverte. Les acheteurs de services informatiques doivent rechercher l'offre qui correspond le mieux à leurs besoins et à leurs capacités internes.

Alignement
Assurez-vous que le service de MDR s'aligne de manière opérationnelle avec le reste de l'environnement informatique, par exemple en vérifiant si les résultats s'intègrent aux systèmes de gestion des billets et aux flux de travail internes.

Un fournisseur doit être capable de générer des rapports et des mises à jour de l'état des incidents pour une transparence totale.

Conformité
Les service de MDR doit être en mesure de respecter toutes les exigences du client en matière de confidentialité, de résidence ou de conservation des données, ainsi que toutes les précisions exigées par les assurances.

Le marché de MDR devrait croître à un taux de croissance annuel composé (TCAC) d'environ

24 %

entre 2024 et 2029.
Source : *MarketsAndMarkets: Managed Detection and Reponse (MDR) Market, 2024*.

Chapitre 2 : Mise en place de MDR avec ESET

ESET offre l'un des services de MDR les plus rapides et les efficaces du marché. La clé de sa puissance réside dans une combinaison gagnante entre l'homme et la machine. Cela se traduit par une recherche en sécurité et une veille sur les menaces de calibre mondial, reposant sur plus de 30 ans d'expertise et 11 centres de R et D, et des capacités d'IA de premier plan pour identifer les comportements anormaux qui pourraient échapper à l'œil humain.

De plus, les équipes de prestation de services de MDR d'ESET sont réparties dans le monde entier, ce qui aide les clients à surmonter les éventuels obstacles linguistiques et améliore l'ensemble de l'expérience.

Pour les utilisateurs commerciaux : ESET propose deux niveaux de MDR. ESET MDR est un service puissant, mais abordable conçu pour répondre aux besoins de PME à partir de 25 postes. ESET MDR Ultimate est un service hautement personnalisé, adapté aux exigences spécifiques et au profil de sécurité des clients d'entreprise.

Il fonctionne comme une extension transparente de la fonction informatique du client, quel que soit son secteur d'activité, et offre une réponse complète aux incidents par criminalistique numérique (DFIR). Le résultat est un service de MDR de qualité professionnelle conçu pour voir plus et agir plus vite, afin d'arrêter et de contenir les menaces de manière proactive avant qu'elles ne causent des dommages.

Pour les fournisseurs de services gérés : ESET comprend que votre entreprise peut également souffrir d'un manque de ressources, en particulier lorsqu'il s'agit d'aider des centaines de clients potentiels sur une surface d'attaque croissante. Votre organisation est une cible de plus en plus attrayante, par exemple, comme moyen pour les assaillants d'accéder à distance aux environnements des clients.

Avec ESET MDR, vous pouvez diversifier votre gamme grâce à une détection et une réponse rapides (potentiellement en 20 minutes seulement) et optimiser vos ressources internes pour continuer à offrir le meilleur service possible à vos clients.

MDR DANS LE CADRE D'UNE SÉCURITÉ GLOBALE

Les services ESET MDR ou ESET MDR Ultimate peuvent être achetés dans le cadre d'abonnements ESET PROTECT spécifiques afin d'assurer une sécurité globale multicouche. Ces services sont des options plus exhaustives associant des produits et des services prenant en charge la prévention, la détection et la réponse. Gérés depuis un poste unique, ces derniers comprennent :

ESET PROTECT MDR

Idéal pour les PME

- Console de gestion
- Protection moderne des terminaux
- Sécurité serveur
- Défense avancée contre les menaces
- Chiffrement du disque entier
- Gestion des correctifs et des vulnérabilités
- Détection et réponse étendues
- Authentification multifacteur
- **Service MDR**
- **Service d'assistance premium**

ESET PROTECT MDR Ultimate

Idéal pour les organisations de niveau entreprise

- Console de gestion
- Protection moderne des terminaux
- Sécurité serveur
- Défense avancée contre les menaces
- Chiffrement du disque entier
- Gestion des correctifs et des vulnérabilités
- Détection et réponse étendues
- Authentification multifacteur
- **Service MDR ultime**
- **Service d'assistance Premium Ultimate**

Conclusion

La cybersécurité est un élément essentiel des opérations informations des organisations. Pourtant, dans la plupart des cas, ce n'est pas leur principale préoccupation, et cela ne devrait pas l'être. Elles doivent pouvoir se concentrer sur leurs tâches principales et laisser aux experts le soin de lutter contre un groupe diversifié, déterminé et croissant d'assaillants. C'est là qu'interviennent les partenaires de confiance en matière de sécurité, qui apportent des ressources étendues et des décennies d'expertise dans le secteur.

Le MDR peut offrir une solution complète en intégrant la prévention, la protection, la détection et la réponse. Des services personnalisés sont disponibles pour répondre aux différents besoins des organisations, qu'il s'agisse de PME, de MSP ou de grandes entreprises. Il est temps d'éliminer les cyberrisques avec l'aide d'un expert.

EN SAVOIR PLUS SUR MDR

À QUOI RESSEMBLE UN DÉPLOIEMENT RÉUSSI DE MDR?

Electrical Consultants, Inc.

ECI est une société de conseil en conception et en ingénierie de premier plan, spécialisée dans les projets d'infrastructure et de services publics d'électricité. Avec plus de 37 bureaux régionaux à travers les États-Unis et le Canada, ECI prend en charge l'ingénierie et la construction d'installation haut voltage, en veillant à ce que chaque projet soit abordé avec innovation, précision et dévouement à l'excellence.

ECI a été confrontée à un défi important en matière de personnel, avec seulement une petite équipe dédiée à la gestion de la cybersécurité, ce qui a rendu particulièrement difficile la surveillance en dehors des heures de bureau et la réponse rapide aux menaces. L'organisation avait besoin d'un moyen fiable et rentable de surveiller les menaces et d'y répondre 24 heures sur 24 afin de protéger ses actifs et ses opérations.

Pour ECI, l'implémentation d'ESET MDR a été simple et n'a nécessité qu'un minimum d'ajustements. L'équipe de sécurité d'ESET a procédé à une évaluation initiale approfondie et a affiné les paramètres d'alerte afin d'optimiser la détection des menaces. Tout au long du processus de configuration, un ingénieur d'ESET a fourni une assistance pratique, garantissant une transition fluide et efficace.

« ESET MDR a permis de détecter un grand nombre de menaces et d'incidents que nous aurions manqués ou auxquels nous n'aurions pas répondu en temps utile. Dans au moins un cas, la détection et la réponse de MDR ont permis d'éviter qu'un petit incident ne devienne un problème beaucoup plus important pour notre entreprise. »

Voici ESET

Protection proactive. Notre activité consiste à minimiser la surface d'attaque.

Gardez une longueur d'avance sur les cybermenaces connues et émergentes grâce à notre **approche axée sur la prévention, alimentée par l'IA et l'expertise humaine**.

Bénéficiez d'une protection de premier ordre grâce à nos **renseignements internes sur les cybermenaces**, compilés et examinés depuis plus de 30 ans, qui alimentent notre vaste réseau de recherche et développement dirigé par des chercheurs reconnus par le secteur. ESET protège votre entreprise afin qu'elle puisse exploiter tout le potentiel de la technologie.

Priorité à la prévention multicouche

L'IA de pointe rencontre l'expertise humaine

Veille sur les menaces de renommée mondiale

Assistance personnalisée et hyperlocale

ESET®
Sécurité numérique
Protégeons le progrès.