Maîtriser la cybersécurité avec le MDR :

Le guide ultime de la détection et de la réponse managées

ESET Digital Security
Progress. Protected.

Table des matières

Introduction : une approche multicouche préventive

Le monde évolue plus vite que ne le peuvent les défenseurs des réseaux. Ils sont confrontés à des adversaires agiles et déterminés, armés jusqu'aux dents des technologies les plus récentes. Comme la surface d'attaque des entreprises s'étend avec chaque nouvel investissement numérique, les risques et les coûts d'une grave faille de sécurité augmentent également. Le coût moyen d'une atteinte à la sécurité des données au niveau mondial s'élève aujourd'hui à près de 4,9 millions de dollars.

Afin de **gérer ces risques croissants**, les organisations devraient envisager d'adopter une approche **proactive** et **préventive** conçue pour minimiser la surface d'attaque, réduire les coûts et la complexité, et améliorer la cyber-hygiène.

Plus de la moitié des organisations victimes de failles de sécurité sont confrontées à un manque important de personnel de sécurité. Cette problématique a augmenté de

26,2%

entre 2023 et 2024.

Source : *IBM : Rapport de 2024 sur le coût d'une atteinte à la sécurité des données*.

Les auteurs de menaces n'ont besoin d'aboutir qu'une seule fois pour causer des dommages importants. C'est pourquoi l'approche la plus mature en matière de cybersécurité d'entreprise associe une prévention multicouche à la détection et la réponse. Cependant, le défi auquel sont confrontées de nombreuses organisations est le suivant :

LES LACUNES EN MATIÈRE DE COMPÉTENCES ET DE CONNAISSANCES ont une incidence sur leur capacité à mener des opérations de sécurité (SecOps) 24/7/365.

LA COMPLEXITÉ des outils de détection et de réponse peut rendre leur utilisation difficile pour certaines entreprises, faute de ressources internes qualifiées.

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

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

LES EXIGENCES DE CONFORMITÉ s'accentuent et amplifient l'impact négatif des attaques en cas de non-conformité.

C'est pourquoi de nombreuses organisations se tournent vers **la détection et la réponse managées** (**MDR**). Ce faisant, elles ont accès à l'expertise et l'efficacité d'une équipe de SecOps tierce utilisant des outils d'IA sophistiqués pour intervenir et endiguer rapidement les menaces. Les meilleurs services de MDR automatisent le suivi et le reporting afin d'améliorer la conformité et renforcer en permanence la cyber-résilience. Les équipes internes peuvent ainsi se concentrer sur des tâches stratégiques de plus grande valeur pour l'entreprise.

4,88 M$

Le coût moyen mondial d'une atteinte à la sécurité des données en 2024, ce qui représente la plus forte augmentation depuis la pandémie.

Source : *Rapport de 2024 sur le coût d'une atteinte à la sécurité des données*.

Chapitre 1 : pourquoi votre entreprise a besoin du MDR

Les entreprises aujourd'hui continuent de développer des infrastructures et des applications dans le Cloud, de prendre en charge le travail à distance, et d'étendre leurs chaînes d'approvisionnement numériques et traditionnelles. Cela offre davantage d'opportunités aux auteurs de menaces très motivés, qui exploitent de plus en plus l'IA et des outils automatisés, des offres « sous forme de services » et plus encore pour perfectionner, professionnaliser et amplifier leurs 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 s'efforcent de gérer le volume, la variété, la vitesse et, dans certains cas, la sophistication des menaces auxquelles leur organisation est confrontée. Les ransomwares sont parmi les plus graves. Les ransomwares sous forme de services (RaaS) sont une « industrie » souterraine hautement compétitive dans laquelle les gangs innovent en permanence pour contourner les contrôles de sécurité et augmenter leurs profits. Selon les experts en sécurité du gouvernement britannique, la menace devrait enfler de plus en plus à mesure que les adversaires se procurent des outils d'IA.

La fréquence des attaques de ransomwares contre les gouvernements, les entreprises, les consommateurs et les appareils devrait augmenter pour passer à une attaque

toutes les 2 secondes d'ici à 2031

Source : *Cybercrime Magazine : Les 10 principales prévisions et statistiques de cybersécurité pour 2024*.

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

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

Les auteurs de menaces utilisent ces outils pour réduire le délai entre l'accès initial et le vol de données ou le déploiement d'un ransomware. Il s'agit d'un défi non seulement dans le contexte des ransomwares, mais également de l'ensemble des menaces ciblant les organisations : malwares d'extraction de cryptomonnaie, botnets, chevaux de Troie bancaires et logiciels espions.

L'impact cumulé de ces tendances devrait attirer l'attention des responsables de la cybersécurité sur une vérité inéluctable : la motivation des cybercriminels à atteindre leurs objectifs dépasse souvent de loin la préparation des entreprises via des mesures préventives. Ils se donnent beaucoup de mal pour s'introduire dans l'environnement des entreprises sans être vus. C'est pourquoi ces dernières devraient **équilibrer la prévention avec la détection et la réponse**. C'est sur cela que se concentre l'approche de prévention d'ESET, **en combinant plusieurs couches de technologies de sécurité**. Elle a pour objectif de protéger en empêchant les malwares et les acteurs malveillants de pénétrer dans le système d'un utilisateur et de l'endommager.

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

4,8 M$

et une part de

15 %

de toutes les attaques.

Source : *IBM Rapport de 2024 sur le coût d'une atteinte à la sécurité des données*.

Toutefois, si ces mesures sont contournées par des acteurs sophistiqués, il existe des moyens de détection et de réponse rapides et fiables pour atténuer les menaces avancées qui parviennent à compromettre un système. Il s'agit non seulement de verrouiller toutes les portes et les fenêtres, mais également d'installer des alarmes pour détecter tous les mouvements suspects si quelqu'un pénètre à l'intérieur de la maison.

L'**XDR** est un atout essentiel à cet égard. Il permet aux équipes chargées des opérations de sécurité (SecOps) de bénéficier d'une **visibilité inégalée** sur leur environnement informatique via une seule et même interface, et de repérer les anomalies grâce à des alertes hyper fiables. L'XDR est une évolution de l'EDR, qui optimise la détection, l'investigation, la réponse et la recherche de menaces en temps réel.

Il unifie les détections pertinentes pour la sécurité sur les endpoints avec la télémétrie des outils de sécurité et d'entreprise, tels que la visibilité et l'analyse du réseau, la sécurité de la messagerie, la gestion des identités et des accès, la sécurité du Cloud, etc. Il s'agit d'une plateforme conçue pour le Cloud qui repose sur une infrastructure de big data pour fournir aux équipes de sécurité de la flexibilité, de l'évolutivité et des possibilités d'automatisation.

L'XDR VOUS PERMET DE RÉPONDRE À PLUSIEURS QUESTIONS CLÉS SUR UNE CYBERATTAQUE :

Comment a-t-elle commencé ?
Où a-t-elle commencée ?
Quand a-t-elle commencée ?
Quels sont les endpoints infectés ?
Est-elle maîtrisée ?
Comment pouvons-nous l'éviter à l'avenir ?

Plus important encore, il peut vous aider à prendre des mesures correctives rapides pour résoudre les incidents avant qu'ils n'aient un impact grave sur l'entreprise.

Cependant, même avec l'aide de l'XDR, les équipes de SecOps sont confrontées à des **défis majeurs** d'un point de vue organisationnel, en particulier les lacunes en matière de compétences, la complexité des outils, les contraintes de budgets et de ressources, l'intégration des outils, ainsi que l'évolution rapide du paysage des menaces. **C'est pourquoi beaucoup se tournent vers le MDR**, qui est le moyen le plus efficace de détecter et de contenir des menaces sophistiquées en constante évolution.

COMMENT LE MDR RÉPOND AUX MENACES ACTUELLES

Bien qu'il puisse varier d'un prestataire à l'autre, un service de MDR devrait inclure au moins les éléments suivants :

- **Surveillance et détection des menaces 24/7** :
  Surveillance en continu du réseau, des endpoints et des environnements Cloud d'une organisation.

- **Recherche proactive des menaces** :
  Contrairement aux mesures de sécurité traditionnelles qui réagissent aux alertes, le MDR implique une recherche proactive qui permet d'identifier les menaces persistantes avancées (APT) et les vulnérabilités zero-day.

51 %
Le nombre

d'organisations qui ont formellement mis en place des méthodologies de recherche de menaces en 2024, contre 35 % en 2023.

Source : *SANS : L'évolution de la chasse aux menaces en entreprise : Details de l'enquête SANS de 2024*.

- **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.

- **Threat Intelligence globale** :
  Des données télémétriques précises, actuelles, pertinentes, et collectées dans le monde entier, fournissent des informations utiles pour une réponse rapide aux incidents et une recherche optimisée des menaces.

Les organisations qui utilisent la télémétrie peuvent obtenir jusqu'à

60 % d'amélioration

de leur capacité à traiter les vulnérabilités et les menaces par rapport à celles qui s'appuient uniquement sur des mesures de sécurité traditionnelles.

Source : *Forrester: Les quatre étapes d'une sécurité plus proactive, 2024*

- **Améliorations constantes** :
  En analysant les incidents passés, en utilisant des renseignements avancés sur les menaces, en se concentrant sur les menaces réelles et en fournissant des bilans et des rapports réguliers sur la sécurité, les services de MDR aident à prévenir la récurrence d'attaques similaires en permettant aux équipes d'améliorer la cyber-résilience.

FONCTIONS CLÉS DU MDR

Le MDR peut apporter des avantages considérables aux organisations qui souhaitent atténuer les cyber-risques, mais qui ne disposent pas des ressources internes nécessaires, en les aidant efficacement à combler les lacunes en matière de compétences, réduire les coûts, et améliorer la détection et la réponse. Une solution performante doit permettre aux organisations de :

Superviser

Des chasseurs de menaces expérimentés surveillent activement l'ensemble de l'environnement informatique du client ainsi que les malwares et les groupes de pirates afin de fournir des connaissances de haut niveau sur la situation.

Détecter

Les auteurs de menaces utilisent d'innombrables méthodes pour se faufiler à travers les défenses du périmètre, mais avec l'analyse comportementale, ils peuvent être repérés et rapidement bloqués.

Trier

Une première évaluation et une catégorisation des alertes permettent de filtrer les faux positifs et recueillir les informations nécessaires.

Hiérarchiser

Des analyses intelligentes classent ces alertes en fonction de leur gravité afin de veiller à ce que les menaces les plus critiques soient traitées en premier. Il s'agit d'une phase critique du workflow de MDR, étant donné que de nombreuses équipes informatiques sont confrontées à un volume d'alertes trop important.

Enquêter

Les outils automatisés et l'expertise humaine se combinent pour approfondir l'analyse des alertes à partir des données et des journaux afin de comprendre leur nature et leur portée. Ils doivent déterminer si une alerte est réellement positive ou non, et quelles mesures doivent être prises pour la résoudre.

Répondre

Un service de MDR efficace fournit soit des actions de réponse de base pour bloquer et contenir une menace, soit un confinement et une remédiation complète de tous les systèmes compromis. Il peut s'agir de réinitialiser un mot de passe, appliquer des correctifs à des endpoints spécifiques, ou même réinstaller des ordinateurs.

Les avantages de l'externalisation de la détection et de la réponse sont simples mais impressionnants :

- Le prestataire du service de MDR se charge de gérer la technologie du back-end, ce qui permet au personnel de se concentrer sur des tâches stratégiques de grande valeur plutôt que de crouler sous les alertes de sécurité.
- Le prestataire du service de MDR peut également optimiser la technologie du back-end pour s'aligner sur le profil de risque et l'infrastructure de chaque client.
- La détection et la réponse étant gérées par un tiers, il n'est pas nécessaire de verser des salaires élevés pour attirer et fidéliser les meilleurs talents.
- Les clients peuvent bénéficier des économies d'échelle de leur prestataire, de sa capacité à attirer les meilleurs talents, ainsi que de sa connaissance des autres entreprises clientes et des environnements de menaces.

FONCTIONNALITÉS ESSENTIELLES À RECHERCHER DANS UNE SOLUTION DE MDR

Avec le grand nombre de solutions de MDR qui inondent le marché, il peut être difficile de savoir **par où commencer**. Recherchez un prestataire capable de proposer au moins les éléments suivants :

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

Vitesse
Réduisez le délai de détection et de réponse aux incidents de plusieurs mois à quelques minutes avec votre fournisseur de MDR. Vous devez stopper l'attaque dans ses phases initiales (découverte, mouvement latéral, persistance) avant que la charge utile ne soit déclenchée.

Service 24/7
Les auteurs de menaces opèrent à partir de tous les fuseaux horaires et frappent souvent aux premières heures du jour ou pendant les week-ends et les jours fériés. Cela signifie que le MDR doit être opérationnel jour et nuit. 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
La solution doit donc être accessible même aux novices de la sécurité informatique. Le tableau de bord, facile à utiliser, apporte une vision claire de l'état de la sécurité et des alertes importantes.

Notifications personnalisables et options de reporting avancées
Afin de recevoir automatiquement ou à la demande des rapports sur les incidents, l'état de l'environnement et d'autres informations. Il est ainsi facile de présenter l'état de la cybersécurité aux dirigeants, recevoir des alertes en temps utile et générer des rapports utiles pour les audits et la conformité.

Prise en main et réglage rapides
Les règles de détection, les exclusions et les paramètres devront être adaptés à chaque environnement informatique et aux menaces auxquelles l'entreprise 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.

Compatibilité sans faille avec différentes infrastructures
Intégration efficace avec des outils de SIEM, de SOAR, des outils de ticketing, et bien d'autres. Vous devez pouvoir intégrer sans problème vos environnements mêmes s'ils comprennent plusieurs systèmes d'exploitation, des logiciels de sécurité existants ou des infrastructures sur site et dans le Cloud.

Une infrastructure technologique complète
La technologie sous-jacente est un élément clé d'une solution de MDR. Elle devrait inclure la détection et la réponse au niveau des endpoints ou étendues (XDR), la gestion des informations et des événements de sécurité (SIEM), ainsi que l'orchestration de la sécurité et la réponse (SOAR). Ces moyens devraient être fournis par le fournisseur de la solution de MDR ou par des outils tiers reliés par des API.

Automatisation et IA
L'IA peut jouer un grand rôle dans l'identification des 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 visant à isoler les systèmes et contenir les menaces. Elles doivent cependant toujours être considérées comme une aide et non comme un substitut à l'expertise des analystes humains.

L'intelligence humaine
Aussi importantes que soient l'IA et l'automatisation, elles ont des limitations que seuls des experts humains peuvent adresser 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 aux nouvelles menaces émergentes en temps réel.

Threat Intelligence
Des flux de renseignements sur les menaces régulièrement mis à jour, générés par le fournisseur de services de MDR ou par des tiers, sont un élément clé de tout service de MDR efficace. Les informations devraient être collectées à partir de la télémétrie et analysées par des équipes d'experts en Threat Intelligence afin de révéler les méthodes d'attaque et les contre-mesures efficaces.

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

Remédiation
Aucune règle établie ne spécifie qui du fournisseur de services ou du client doit s'occuper de la remédiation/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 leurs capacités internes.

Harmonisation
Veillez à ce que le service de MDR s'aligne sur le reste de l'environnement informatique, notamment en ce qui concerne l'intégration des informations produites dans les systèmes de gestion des tickets et les flux de travail internes. Le fournisseur doit être en mesure de générer des rapports d'incidents et des informations sur l'état d'avancement pour une transparence totale.

Conformité
Le 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 stipulations exigées par les polices d'assurance.

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

24 %

de 2024 à 2029.

Source : *MarketsAndMarkets : Marché de la détection et de la réponse managées (MDR), 2024*.

Chapitre 2 : mise en œuvre du MDR avec ESET

ESET propose l'un des services de MDR les plus rapides et les plus efficaces du marché. Sa puissance réside dans l'association gagnante de l'homme et de la machine, qui permet un haut niveau de recherche et de veille sur les menaces, reposant sur plus de 30 ans d'expertise et 11 centres de R&D, ainsi que des capacités d'IA de pointe pour identifier les comportements anormaux que l'œil humain pourrait manquer.

Les équipes de prestation du service ESET MDR sont réparties dans le monde entier, ce qui aide les clients à surmonter les barrières linguistiques potentielles et rend l'expérience plus fluide.

Pour les entreprises clientes : ESET propose le MDR en deux niveaux. ESET MDR est un service puissant mais abordable conçu pour répondre aux besoins des PME à partir de 25 postes. ESET MDR Ultimate est un service hautement personnalisé, adapté aux exigences spécifiques et au profil de sécurité des grandes entreprises.

Il fonctionne comme une extension transparente de la fonction informatique du client, quel que soit son secteur d'activité, et fournit des enquêtes DFIR. Le résultat est une solution de MDR de haut niveau conçue pour voir plus et agir plus vite, afin de stopper et contenir les menaces de manière proactive avant qu'elles ne causent des dommages.

Pour les MSP : ESET comprend les contraintes de votre entreprise en termes de ressources, en particulier lorsqu'elle travaille au service de centaines de clients potentiels sur une surface d'attaque croissante. Votre organisation est une cible de plus en plus attrayante, par exemple en tant que moyen pour les auteurs de menaces d'accéder à distance aux environnements des clients.

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

LE MDR COMME ÉLÉMENT D'UNE SÉCURITÉ GLOBALE

Les services ESET MDR et ESET MDR Ultimate peuvent être achetés dans le cadre de niveaux d'abonnement ESET PROTECT spécifiques pour prendre en charge une sécurité multicouche holistique. Ce sont des options plus complètes combinant des produits et des services de prévention, de détection et de réponse. Managés via une interface unique, ils comprennent :

ESET PROTECT MDR

Idéal pour les petites et moyennes entreprises

- Console d'administration
- Protection pour endpoints
- Sécurité des serveurs
- Défense contre les menaces avancées
- Chiffrement intégral des disques
- Gestion des vulnérabilités et des correctifs
- Détection et réponse étendues
- Authentification multifacteur
- **Service MDR**
- **Service Premium Support**

ESET PROTECT MDR Ultimate

Idéal pour les grandes entreprises

- Console d'administration
- Protection pour endpoints
- Sécurité des serveurs
- Défense contre les menaces avancées
- Chiffrement intégral des disques
- Gestion des vulnérabilités et des correctifs
- Détection et réponse étendues
- Authentification multifacteur
- **Service MDR Ultimate**
- **Service Premium Support Ultimate**

Conclusion

La cybersécurité est un élément essentiel des opérations informatiques des organisations. Pourtant, dans la plupart des cas, ce n'est pas leur centre d'intérêt principal, et cela ne devrait pas l'être. Elles doivent pouvoir se concentrer sur leur cœur de métier et laisser aux experts le soin de lutter contre une cohorte diversifiée, déterminée et croissante d'auteurs de menaces. C'est là qu'interviennent les partenaires de confiance, qui apportent des ressources étendues et des décennies d'expertise dans le secteur de la sécurité.

Le MDR peut offrir une solution complète en intégrant la prévention, la protection, la détection et la réponse. Des services sur mesure 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 cyber-risques avec l'aide d'un expert.

EN SAVOIR PLUS SUR LE MDR

À QUOI RESSEMBLE UN DÉPLOIEMENT EFFICACE DU MDR ?

Electrical Consultants, Inc.

ECI est une société de conseil en conception et en ingénierie, spécialisée dans les projets d'infrastructure et de services publics d'électricité. Avec plus de 37 bureaux régionaux aux États-Unis et au Canada, ECI prend en charge l'ingénierie et la construction d'installations à haute tension et à grande échelle, en veillant à ce que chaque projet soit abordé avec innovation, précision et un dévouement envers l'excellence.

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

La mise en œuvre d'ESET MDR s'est faite simplement et n'a nécessité que des ajustements minimes. L'équipe de sécurité d'ESET a procédé à une évaluation initiale approfondie et a affiné les paramètres d'alertes pour optimiser la détection des menaces. Tout au long du processus de mise en œuvre, un ingénieur d'ESET a fourni une assistance pratique, garantissant une transition fluide et efficace.

« ESET MDR a détecté de nombreuses menaces et incidents que nous aurions manqués ou auxquels nous n'aurions pas réagi aussi rapidement. Dans au moins un cas, ESET MDR a permis d'éviter qu'un petit incident ne devienne un problème majeur pour notre entreprise. »

À propos d'ESET

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

Prenez une longueur d'avance sur les cybermenaces connues et émergentes grâce à notre **approche préventive reposant sur l'IA et l'expertise humaine**.

Bénéficiez d'une protection de haut niveau grâce à notre **Threat Intelligence** interne, compilée et examinée depuis plus de 30 ans, qui alimente notre vaste réseau de R&D dirigée par des **chercheurs reconnus**. ESET protège votre organisation afin qu'elle puisse maximiser le potentiel de la technologie.

Prévention multicouche

IA de pointe associée à une expertise humaine

Threat Intelligence de renommée mondiale

Support hyperlocal et personnalisé

eset®
Digital Security
Progress. Protected.