Guide de l'acheteur

Comprendre les services de MDR

Qu'est-ce que c'est et pourquoi en avez-vous besoin ?

Phil Muncaster

Digital Security
Progress. Protected.

Digital Security
Progress. Protected.

© 1992–2023 ESET, spol. s r.o. – Tous droits réservés. Les marques commerciales utilisées dans ce document sont des marques commerciales ou des marques déposées d'ESET, spol. s.r.o. ou d'ESET North America. Tous les noms et toutes les autres marques apparaissant dans ce document sont des marques déposées appartenant à leurs entreprises respectives.

Table des matières

Introduction 4

Chapitre 1 : Défis actuels 7

Chapitre 2 : Pourquoi le MDR ? 9

- La surface d'attaque des entreprises s'étend
- Les auteurs de menaces se professionnalisent et innovent
- De la prévention à l'XDR
- Quel est l'apport du MDR
- Quel est l'apport du MDR
- Quels sont les avantages du MDR ?
- Que rechercher dans une solution de MDR ?

Chapitre 3 : Comment ESET peut vous aider 21

- À quoi ressemble un déploiement réussi ?

Conclusion 25

Introduction

Le paysage du cyber-risque des entreprises évolue rapidement. Les surfaces d'attaque numériques se sont considérablement élargies grâce aux investissements réalisés durant la pandémie de COVID. Les systèmes dans le Cloud, les télétravailleurs distraits, les infrastructures d'accès à distance, les endpoints distribués et les chaînes d'approvisionnement complexes constituent d'importantes cibles attrayantes pour les auteurs de menaces. En parallèle, la cybercriminalité se professionnalise. Elle se dote de ses propres chaînes d'approvisionnement complexes, d'offres de malwares sous forme de services, et développe des tactiques, techniques et procédures (TTP) innovantes.

Dans ce contexte, la prévention des menaces, bien que souhaitable, n'est pas toujours possible. C'est pourquoi les entreprises devraient envisager de faire évoluer leur approche et d'adopter une réponse plus globale, basée sur la prévention, la détection et le traitement. Les équipes ont ainsi la possibilité d'empêcher les acteurs malveillants de pénétrer dans leurs systèmes et de les endommager. Et si la prévention échoue, elles disposent toujours de moyens avancés de détection et de traitement pour repérer les événements suspects et résoudre les menaces avant qu'elles ne puissent s'aventurer trop loin.

Quel outil de détection et de traitement les entreprises doivent-elles choisir ? Un outil de détection et le traitement étendus (XDR) peut être utile, mais il ajoute d'autres problématiques telles que la recherche et le financement du personnel de sécurité nécessaire à son utilisation, sans être surchargé d'alertes.

C'est là qu'intervient la détection et le traitement managés (MDR). Il s'agit d'un type de service de sécurité managé qui combine des outils, des technologies et des experts en cybersécurité pour fournir aux entreprises des moyens robustes de détection et de traitement. Lorsqu'il est bien implémenté, le service de MDR offre un moyen plus efficace de gérer les cyber-risques. Mais le facteur critique est de savoir avec quel prestataire s'associer.

Les entreprises doivent s'adresser à des fournisseurs de renseignements sur les menaces et de technologies de haute qualité qui ont fait leurs preuves, avec un taux de détection élevé, un faible taux de faux positifs et une empreinte légère. Elles doivent également tenir compte du service client et du degré d'optimisation du MDR pour leurs besoins spécifiques.

Comment fonctionne l'XDR ?

L'XDR est une évolution de l'EDR, qui optimise la détection, l'investigation, le traitement et la recherche de menaces en temps réel. L'XDR unifie les détections pertinentes pour la sécurité sur les endpoints avec la télémétrie des outils de sécurité et d'entreprise, tels que l'analyse et la visibilité du réseau (NAV), la sécurité de la messagerie, la gestion des identités et des accès, la sécurité du Cloud, etc. Il s'agit d'une plateforme native dans le Cloud reposant sur une infrastructure de big data pour fournir aux équipes de sécurité de la flexibilité, de l'évolutivité et des possibilités d'automatisation.

Source : *Forrester, 2021*

Chapitre 1 : Défis actuels

Dans cette course aux armements qu'est la cybersécurité, il semble souvent que nos adversaires aient toutes les cartes en main. Ils sont soutenus par des réseaux cybercriminels souterrains au rythme de plusieurs milliers de milliards de dollars par an, qui fournissent tous les outils, les connaissances et les données nécessaires pour lancer des attaques avec facilité. Les auteurs de menaces sont souvent sponsorisés par des États hostiles, ce qui leur permet de déclencher des attaques sans crainte de représailles de la part des forces de police. Les offres de malwares sous forme de services (SaaS) ont par ailleurs démocratisé la possibilité de coordonner des campagnes audacieuses, même pour des groupes ayant moins de connaissances techniques.

Les responsables de la sécurité des systèmes d'information (RSSI) et leurs équipes sont de plus en plus tiraillés dans plusieurs directions à la fois. Les investissements dans la transformation digitale pendant la pandémie ont considérablement élargi la surface de cyberattaque des entreprises. **Les environnements de travail en distanciel** représentent une lacune particulièrement dangereuse en matière de visibilité et de contrôle, qu'il s'agisse d'endpoints non protégés ou d'utilisateurs distraits ou négligents. De nombreuses équipes de sécurité manquent de personnel et sont submergées par un trop grand nombre de solutions individuelles inefficaces, qui ajoutent de la complexité et réduisent la productivité.

Les dommages potentiels sur les finances et la réputation causés par une grave faille de sécurité n'ont jamais été aussi élevés. En ce sens, la capacité des entreprises à atténuer efficacement les risques associés à de tels incidents est, au mieux, en train de diminuer.

Les coûts des atteintes à la sécurité des données dans le monde sont désormais à un niveau record de plus de 4,2 millions de dollars US en moyenne en 2021. Et selon un grand assureur international, un cinquième des entreprises américaines et européennes qui ont subi une cyberattaque cette année-là ont failli devenir insolvables.

Dans ce contexte, **une prévention à 100 % n'est tout simplement pas réaliste**. Un attaquant déterminé trouvera toujours un moyen de compromettre des cibles vulnérables. Il est donc nécessaire de compléménter cette approche par la détection et le traitement. Pourtant, les entreprises prennent là aussi du retard. Le délai moyen nécessaire pour identifier et contenir une faille de sécurité en 2021 était de 287 jours.

L'XDR

analyse les comportements sur les endpoints, le réseau, le Cloud, la messagerie et d'autres couches pour repérer les activités suspectes et stopper les attaquants avant qu'ils ne puissent avoir un impact.

Source : *Forrester, 2021*

Le MDR

est effectivement une version externalisée de la détection et du traitement étendus (XDR), parfois combinée à d'autres outils.

Source : *Forrester, 2021*

C'est pourquoi de nombreuses entreprises se tournent vers le MDR, un type de service de sécurité managé combinant outils, technologies et experts en cybersécurité. selon Gartner, la moitié des entreprises dans le monde utiliseront le MDR pour contenir les menaces d'ici 2025. Cependant, alors que l'XDR exige du client qu'il se charge de la surveillance, de la détection et du traitement, avec le MDR, un prestataire de cybersécurité de confiance se charge du travail, afin que le personnel interne puisse se consacrer à d'autres tâches à forte valeur.

91 %

des entreprises dans le monde utilisent ou prévoient d'utiliser des services de déploiement, d'assistance technique, de cybersécurité, et de recherche/surveillance des menaces sous forme de services.

Source : *Enquête interne d'ESET Research auprès de 404 personnes interrogées dans de grandes entreprises.*

Les failles sont une réalité



Source : *IDC, Security Services Market Update, 1Q22, doc. n° US48907622, mars 2022.*

Chapitre 2 : Pourquoi le MDR ?

Bien que les dépenses moyennes en cybersécurité ait doublé en 2021 pour les entreprises de 250 à 999 collaborateurs[1], et ont augmenté de 65 % pour les entreprises de plus de 1 000 collaborateurs[2], les atteintes à la sécurité se produisent aujourd'hui à une échelle monumentale.

Aux États-Unis, l'année 2021 a connu un volume record de fuites de données annoncées publiquement, soit 23 % de plus que le précédent record historique de 1 506. Au Royaume-Uni, 59 % des entreprises de taille moyenne et 72 % des grandes entreprises ont déclaré avoir détecté des failles de sécurité ou des cyberattaques en 2021. La menace des ransomwares est particulièrement sérieuse : un rapport révèle que plus de 623 millions d'attaques ont été détectées en 2021, soit une augmentation de 105 % par rapport à l'année précédente.

LA SURFACE D'ATTAQUE DES ENTREPRISES S'ÉTEND

Pourquoi les entreprises ont-elles des difficultés à repousser les adversaires ? En partie parce qu'elles sont plus exposées qu'elles ne l'ont jamais été en raison des investissements dans les infrastructures numériques et de l'émergence du lieu de travail hybride. Selon McKinsey, COVID-19 a poussé de nombreuses entreprises à franchir un « tournant technologique », transformant à jamais leur façon de travailler. Dans certains cas, la transformation numérique a été accélérée de plusieurs années. Mais si cela a contribué à rendre ces entreprises plus efficaces et offrir des expériences innovantes aux clients et aux collaborateurs, cela a également considérablement augmenté leur surface d'attaque numérique. Selon une étude, 43 % des entreprises mondiales admettent que leur surface d'attaque numérique est « en train d'échapper à tout contrôle ». Nous pouvons le constater dans :

LE CLOUD

Les infrastructures, les plateformes et les logiciels sous forme de services (IaaS, PaaS, SaaS) offrent des avantages considérables en termes d'agilité et de coûts. Lorsqu'elles utilisent notamment des IaaS et des PaaS, les entreprises ont des difficultés à sécuriser leurs environnements, et le fait que beaucoup d'entre elles gèrent plusieurs Clouds hybrides ne fait qu'ajouter à la complexité. Les mauvaises configurations sont si courantes qu'elles sont considérées comme étant la première cause d'incidents de sécurité dans le Cloud en 2021. Les auteurs de menaces recherchent régulièrement des systèmes exposés qu'ils peuvent compromettre.

LE TRAVAIL EN DISTANCIEL

De nombreux systèmes personnels sont toujours mal protégés, ce qui est inquiétant. Les collaborateurs peuvent retarder indûment l'installation de correctifs sur leurs ordinateurs portables professionnels ou laisser l'état de la sécurité de leurs appareils personnels s'altérer. Un rapport de 2021 affirme que 45 % des responsables informatiques ont constaté l'utilisation d'imprimantes compromises pour mener des attaques. L'environnement de travail à domicile est de plus en plus considéré par les cybercriminels comme un vecteur d'attaque attrayant pour compromettre les réseaux d'entreprise. Et maintenant que le lieu de travail hybride prend forme concrètement, les travailleurs mobiles qui se connectent via des points d'accès Wifi publics et des ordinateurs partagés peuvent représenter une menace supplémentaire.

1) Une entreprise de taille moyenne comporte entre 50 et 249 salariés. Au total, 149 entreprises de taille moyenne ont été interrogées.
2) Une grande entreprise comporte 250 salariés ou plus. Au total, 134 grandes entreprises ont été interrogées.

LES TÉLÉTRAVAILLEURS

Si les appareils professionnels utilisés en distanciel sont souvent la cible d'attaques, il en va de même pour leurs propriétaires. Selon Microsoft, 80 % des professionnels de la sécurité ont constaté une augmentation des menaces pour la sécurité depuis le passage au télétravail. Et parmi ceux-ci, 62 % affirment que les campagnes d'hameçonnage ont augmenté plus que toute autre menace. On estime que les télétravailleurs sont plus distraits et plus enclins à prendre des risques que leurs collègues de bureau, ce qui en fait une cible parfaite des attaques d'ingénierie sociale. L'hameçonnage peut être une porte d'entrée amenant à des ransomwares, des fuites de données et d'autres formes de compromission. Plus d'un tiers (35 %) des entreprises déclarent avoir vu des collaborateurs contourner ou désactiver des mesures de sécurité.

« Depuis 2015, le nombre de failles de sécurité signalées a augmenté de 25 %, le nombre de dossiers fuités a augmenté de 500 %, et depuis 2017, le nombre d'attaques de ransomwares a augmenté de 231 %. »

Bonnes pratiques : la sécurité est importante, mais quoi faire ? Forrester Research Inc, 2 mai 2022.

L'INFRASTRUCTURE D'ACCÈS À DISTANCE

L'avènement du télétravail de masse a également entraîné une forte augmentation de l'utilisation d'outils tels que les réseaux privés virtuels et le protocole d'accès à distance (RDP) qui permettent aux collaborateurs à l'extérieur des bureaux d'accéder aux ressources internes. Le problème est qu'ils sont souvent mal configurés ou insuffisamment actualisés. Plutôt que d'utiliser l'authentification multifacteur pour protéger davantage l'accès, de nombreux comptes RDP sont sécurisés par des identifiants faibles ou fuités. Cela permet aux attaquants d'accéder assez facilement aux réseaux d'entreprise en se faisant passer pour des utilisateurs légitimes. RDP est l'un des trois principaux vecteurs d'attaque de ransomwares : les tentatives de compromission ont atteint un niveau record de plus de 4,5 milliards[3] le 10 janvier 2022.

Les tentatives d'exploitation des vulnérabilités de RDP ont atteint un niveau record le 10 janvier 2022



Graphique des tendances des tentatives de connexion RDP et du nombre de clients uniques durant T3 2021 et T1 2022, moyenne mobile sur sept jours.
(source : télémétrie ESET)

3) Calculé en utilisant une moyenne mobile sur sept jours

LES CHAÎNES D'APPROVISIONNEMENT

Il peut s'agir des écosystèmes physiques ou numériques des partenaires et des fournisseurs. Dans le monde physique, le risque que les collaborateurs et les prestataires ayant accès au réseau soient amenés à communiquer leurs mots de passe ou se faire voler leur machine est permanent. Dans la chaîne d'approvisionnement logicielle, la menace est sans doute encore plus grande lorsque des acteurs malveillants altèrent les mécanismes et les outils utilisés pour développer, déployer et actualiser les logiciels en y insérant des malwares. L'éditeur de logiciels de gestion informatique Kaseya a été compromis par le groupe de ransomwares REvil, qui a exploité son accès pour envoyer des mises à jour malveillantes aux clients MSP de l'éditeur. Plus de 1 000 clients ont été touchés en aval. Le code open source couramment utilisé par les équipes de DevOps pour réduire le délai de rentabilisation est également une autre source d'inquiétude, car il peut introduire un risque supplémentaire difficile à gérer au milieu de dépendances logicielles complexes. Plus de deux cinquièmes (41 %) des entreprises ne font pas confiance à la sécurité des logiciels open source qu'elles utilisent, et seulement 49 % affirment avoir une politique de sécurité pour leur utilisation, selon un rapport.

49 %

des entreprises ont une politique de sécurité spécifique aux logiciels libres.

Source : *Rapport sur l'état de la sécurité des logiciels libres, Snyk, 2022*

LES AUTEURS DE MENACES SE PROFESSIONNALISENT ET INNOVENT

Le nombre de cybercriminels prêts à tirer parti de ces failles de sécurité semble également avoir augmenté ces dernières années. Il existe même des places de marché pour vendre des données volées, acheter des accès et des outils, et embaucher de nouvelles recrues. Contrairement à la profession de cybersécurité, il semble qu'il y ait un flux constant de talents désireux de vivre de leurs activités néfastes.

L'innovation est omniprésente dans la cybercriminalité, ce qui est une mauvaise nouvelle pour les défenseurs des réseaux. Elle comprend :

1. **Les ransomwares sous forme de services (RaaS) :** Tout comme les SaaS ont popularisé le déploiement de logiciels dans le Cloud, les RaaS ont facilité le lancement et la gestion des attaques de ransomwares. Des affiliés peuvent gagner jusqu'à 80 % des revenus générés par les attaques. En échange, ils reçoivent un kit comprenant un ransomware et l'infrastructure d'attaque, ainsi qu'un site sur lequel publier les données volées.

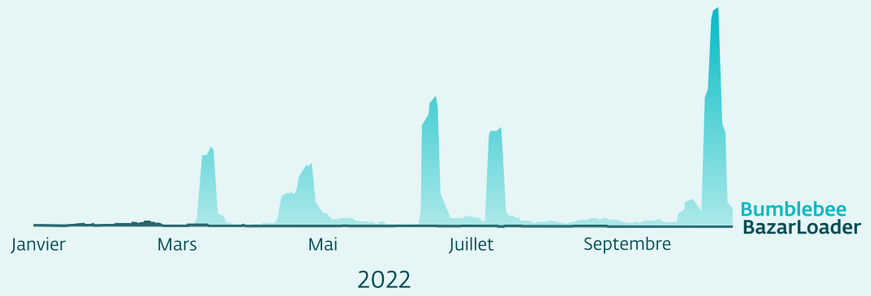
Tout comme les SaaS ont popularisé le déploiement de logiciels dans le Cloud, les RaaS ont facilité le lancement et la gestion des attaques de ransomwares. Des affiliés peuvent gagner jusqu'à 80 % des revenus générés par les attaques. En échange, ils reçoivent un kit comprenant un ransomware et l'infrastructure d'attaque, ainsi qu'un site sur lequel publier les données volées.

2. **La monétisation agressive :** La plupart des attaques de ransomwares impliquent aujourd'hui l'exfiltration et la publication des données pour forcer le paiement de la rançon. Les affiliés font de plus en plus monter la pression sur leurs victimes via différentes tactiques supplémentaires, notamment des attaques de déni de service distribué, ou en contactant les clients, les partenaires et les journalistes pour dévoiler ce qui s'est passé. Un groupe de ransomwares affiche la note de rançon directement sur le site web des victimes. Un autre crée un site spécifique à chaque victime, afin que les clients et les salariés puissent vérifier si leurs données ont été exposées.

3. **L'exploitation très rapide des vulnérabilités** : Le nombre de vulnérabilités répertoriées dans la base de données nationale américaine sur les vulnérabilités (NVD) a atteint un niveau record en 2021. Il est donc de plus en plus difficile pour les administrateurs de la sécurité de suivre le rythme du nombre impressionnant de correctifs publiés. Comme si cela n'était pas déjà assez difficile, les groupes de pirates sont de plus en plus capables d'exploiter rapidement les bugs zero day dans des attaques. Quelques jours après la publication de correctifs pour les vulnérabilités ProxyLogon sur Microsoft Exchange Server, pas moins de 10 groupes de pirates les ont exploitées dans leurs attaques, touchant plus de 5 000 serveurs Exchange dans plus de 115 pays.

4. **La chaîne d'approvisionnement des cybermenaces** : La cybercriminalité clandestine dispose de plus en plus de ressources et de professionnels. Des groupes spécialisés apparaissent pour répondre à des besoins commerciaux et opérationnels spécifiques. Par exemple, afin d'obtenir un accès au réseau, on assiste à une augmentation du nombre de courtiers d'accès initial, qui sont des experts qui compromettent des cibles puis vendent cet accès à d'autres. Une équipe de recherche a repéré une augmentation de 57 % du nombre d'annonces de courtiers d'accès initial publiées sur des forums cybercriminels en 2021 par rapport à l'année précédente. Comme autre exemple, Bumblebee est un chargeur conçu pour récupérer et exécuter des malwares supplémentaires. Il est le successeur de TrickBot, un malware bien connu et très résistant qui a survécu à

Tendances de détection de Bumblebee et DE BazarLoader



deux tentatives de démantèlement en 2020, avant sa mise hors service par ses opérateurs. La relève de TrickBot a été revendiquée par BazarLoader, qui a été actif jusqu'au début de l'année 2022 mais qui a rapidement été éliminé au profit de Bumblebee. Le chargeur Bumblebee, qui semble être exploité par l'équipe de TrickBot et de BazarLoader, est actif à ce jour, et ses dernières campagnes remontent à la mi-août 2022.

5. **Des outils légitimes et des malwares sans fichiers** : Dès qu'ils ont réussi à pénétréer dans les réseaux ciblés, les auteurs de menaces utilisent généralement des outils légitimes et des malwares sans fichiers pour contourner les outils de sécurité traditionnels. L'idée est d'utiliser des programmes non malveillants pour mener des activités malveillantes telles que le mouvement latéral, l'exfiltration de données, la découverte de processus, la récupération d'identifiants et l'exécution de commandes arbitraires. Ces programmes comprennent PowerShell, PsExec et Cobalt Strike.

6. **Des progrès dans l'hameçonnage et l'ingénierie sociale** : Les anciennes méthodes sont parfois les plus efficaces. L'hameçonnage reste l'un des trois principaux vecteurs d'attaque des ransomwares, atteignant un niveau record au premier trimestre 2022. Les criminels ne cessent de perfectionner leurs techniques pour devancer les filtres de messagerie et les programmes de formation à la sécurité. L'une des plus populaires est le détournement de fils de discussion par email, qui consiste pour les attaquants à compromettre une boîte de messagerie et détourner les conversations existantes afin de diffuser des liens d'hameçonnage. Comme un message de réponse semble plus authentique qu'un message non sollicité, les liens inclus ont plus de chances d'être cliqués. Le smishing (hameçonnage par SMS) est une autre technique qui mise sur le fait que les utilisateurs sont plus distraits lorsqu'ils regardent l'écran de leur smartphone, et donc plus susceptibles de cliquer. Un éditeur a noté une multiplication par deux du nombre de tentatives de smishing et plus de 500 campagnes de détournement de fils de discussion aux États-Unis en 2021, liées à 16 familles de malwares différentes.

DE LA PRÉVENTION À L'XDR

Les ransomwares sont à l'origine de nombreuses innovations dans le domaine des malwares. Selon des experts en sécurité du gouvernement britannique, ils sont devenus le principal cyber-risque pour les entreprises. Il est ainsi facile de comprendre comment un seul groupe (Conti) a réussi à compromettre au moins 859 entreprises en deux ans, dont 40 en seulement un mois, et engranger des milliards de dollars en cryptomonnaie au cours de ces attaques. Selon une estimation, les détections de ransomwares ont grimpé de 148 % d'une année sur l'autre pour atteindre 470 millions au cours des trois premiers trimestres de 2021, ce qui en fait la pire année jamais enregistrée.

Mais les ransomwares sont loin d'être la seule menace qui pèse aujourd'hui sur les entreprises internationales. Le vol de données, les extracteurs de cryptomonnaie, les chevaux de Troie bancaires et les logiciels espions, entre autres, se bousculent pour se faire une place.

L'impact cumulé de ces tendances devrait attirer l'attention des responsables de la sécurité informatique sur une vérité inéluctable : **la prévention des menaces devrait toujours être privilégiée, mais parfois ce n'est pas possible**. Il existe tout simplement trop de moyens pour les pirates de s'introduire dans l'environnement des entreprises sans être vus. C'est pourquoi elles doivent équilibrer la prévention avec la détection et le traitement. C'est sur cela que se concentre l'approche de prévention, de détection et de traitement d'ESET (EPDR), en combinant plusieurs couches de sécurité. Elle protège tout d'abord en empêchant les malwares et les acteurs malveillants de pénétrer dans le système d'un utilisateur ou de l'endommager. Mais si cela échoue, une puissante technologie de détection et de traitement atténue 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[3] est une évolution de l'EDR, qui optimise la détection, l'investigation, la réponse et la chasse aux 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 l'analyse et la visibilité du réseau (NAV), la sécurité de la messagerie, la gestion des identités et des accès, la sécurité du Cloud, etc. Il s'agit d'une plateforme native dans le Cloud s'appuyant 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 commencée ?**
- **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.

5) Définition de l'XDR par Forrester, 2021

QUEL EST L'APPORT DU MDR ?

Cependant, même avec l'aide de l'XDR, les équipes de SecOps sont confrontées à des défis majeurs d'un point de vue organisationnel. Bon nombre de ceux-ci, notamment le manque de connaissances, d'expertise et de ressources en interne, sont particulièrement prononcés chez les PME. Les défis pour les entreprises sont généralement les suivants :

PÉNURIE DE TALENTS

Le secteur de la cybersécurité connaît actuellement un déficit de 2,7 millions de travailleurs, et les analystes des centres d'opérations de sécurité (SOC) sont sans doute parmi les plus difficiles à trouver et fidéliser. De nombreux analystes comptent démissionner en 2023 en raison du stress et de l'épuisement liés au volume d'alertes, ce qui aggravera le problème. Les informaticiens généralistes ne peuvent souvent pas consacrer plusieurs heures par jour à la gestion d'une solution d'XDR. Le problème est particulièrement critique pour les PME, qui ne disposent généralement pas des connaissances et de l'expertise internes nécessaires pour gérer un SOC, et qui pourraient donc bénéficier le plus du MDR.

COÛTS

Les responsables de la sécurité ne doivent pas seulement penser au coût de l'embauche et de la fidélisation du personnel du SOC. Ils doivent également trouver la bonne combinaison d'outils pour fournir les informations dont leurs analystes ont besoin. Cela peut représenter un coût important au départ, ainsi que des frais de licence récurrents par la suite.

La charge financière qui pèse sur les entreprises qui choisissent d'internaliser les SecOps est de plus en plus lourde. Selon une étude, le retour sur investissement perçu est en baisse dans plus de la moitié des entreprises en raison de la complexité de leur gestion. Le même rapport indique que les coûts de l'ingénierie de la sécurité s'approchent des 3 millions de dollars US par an, mais que seulement 51 % des personnes interrogées considèrent que ces efforts sont efficaces.

LACUNES DE SÉCURITÉ

Les outils ne sont parfois pas à la hauteur. Cela peut entraîner un volume élevé d'alertes et une lassitude consécutive. Si le personnel du SOC est submergé de faux positifs, il peut finir par passer des heures sur de fausses pistes et manquer les signaux légitimes, et lorsque plusieurs outils alimentent le SOC, cela peut également entraîner des disparités dans la couverture.

ADMINISTRATION

L'acquisition, l'installation et la configuration correcte des produits ne sont que les premières étapes. Gérer plusieurs outils et analystes dans plusieurs domaines peut représenter un défi important. Lorsque les ressources sont déjà sollicitées au maximum, des tâches importantes sont parfois oubliées. Il est facile de s'épuiser à combattre les menaces qui se présentent, pour au final manquer de temps pour la réflexion et la planification stratégiques.

On a l'impression que les équipes de sécurité informatique des entreprises veulent et sont tout à fait capables trapidement, qu'elles comprennent parfaitement les logiciels qu'elles achètent, et qu'elles bâtissent des SOC internes matures pour faire face aux cybermenaces. En fait, les études menées par ESET montrent que :

68 %

des entreprises préfèrent que leurs produits de sécurité soient déployés par leur prestataire de sécurité

75 %

s'attendent à ce que leur prestataire de sécurité offre une assistance et des conseils, et traite les incidents de cybersécurité

87 %

souhaitent des services d'assistance à la cybersécurité 24 heures sur 24 et 7 jours sur 7

90 %

souhaitent que les prestataires proposent des services de surveillance, de recherche et de remédiation des menaces

4) Enquête interne d'ESET Research auprès de 404 personnes interrogées dans de grandes entreprises.

QUELS SONT LES AVANTAGES DU MDR ?

C'est là que le MDR peut apporter des avantages considérables aux entreprises qui souhaitent atténuer les cyber-risques, mais qui ne disposent pas des ressources internes pour le faire efficacement. Bien qu'il puisse varier d'un prestataire à l'autre, le service de MDR devrait inclure au moins les éléments suivants :

DÉTECTION DES MENACES

Les auteurs de menaces disposent d'innombrables moyens de se faufiler à travers les défenses du périmètre. Mais grâce à l'analyse des comportements, il est possible de les repérer rapidement afin que les entreprises puissent prendre des mesures pour résoudre les attaques. La recherche proactive des menaces peut également être utilisée pour localiser des attaques sophistiquées susceptibles d'avoir échappé aux contrôles automatisés.

HIÉRARCHISATION DES PRIORITÉS

L'analyse intelligente génère un contexte qui permet aux systèmes de MDR de transformer les données en informations exploitables et de signaler les alertes avec une plus grande fiabilité. Il s'agit d'une phase critique du workflow de MDR, étant donné que de nombreuses équipes SOC sont confrontées à un volume d'alertes trop important.

« Les services de MDR couvrent déjà une grande partie de ce que l'XDR aspire à faire. Le MDR permet d'obtenir de meilleurs résultats de sécurité en fournissant des outils et des technologies tels que les renseignements sur les menaces, la recherche de menaces, la surveillance constante 24 heures sur 24 et 7 jours sur 7, l'analyse avancée, ainsi que le confinement et l'élimination des brèches ou des incidents par lesquels des données ont été exfiltrées ou détruites. IDC estime qu'une offre de MDR devrait aller au-delà de la fourniture de conseils et de recommandations. »

Source : IDC, Global Security Products Analysis: From Power Point to Power Product, Where Is XDR Right Now, doc. n° US47705821, 8 février 2022, Ch. Kissel, M. Suby, F. Dickson

ANALYSE

L'analyse automatisée des comportements se combine à l'évaluation humaine pour déterminer si une alerte est légitime et quelles mesures doivent être prises pour résoudre un problème.

TRAITEMENT

Grâce à la phase d'analyse précédente, le système comprendra quel type de traitement est nécessaire pour endiguer et éliminer la menace, et remédier à tout système compromis. Il peut s'agir de réinitialiser un mot de passe, d'appliquer des correctifs à des endpoints spécifiques, ou même de réinstaller des ordinateurs.

LES AVANTAGES DE L'EXTERNALISATION DE LA DÉTECTION ET DU TRAITEMENT 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
- Le prestataire du service de MDR peut également optimiser et gérer la technologie du back-end pour s'aligner sur le profil de risque et l'infrastructure de chaque client
- La détection et le traitement étant gérés par un tiers, il ne sera pas nécessaire de verser des salaires élevés pour attirer et fidéliser les meilleurs talents pour le SOC
- 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 menacesAccès aux analystes des menaces

QUE 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 :

EXCELLENCE DE LA RECHERCHE :

Une solution sur mesure, adaptée à la taille, à la complexité informatique et au niveau de protection requis de chaque client.

SERVICE CLIENTÈLE DE HAUTE QUALITÉ :

Notamment un support hyperlocal combiné à une présence et une mise en œuvre mondiales.

PERSONNALISATION

Une solution sur mesure, adaptée à la taille, à la complexité informatique et au niveau de protection requis de chaque client.

DÉTECTION ET TRAITEMENT DE POINTE :

Testés de manière indépendante, ces produits sont réputés pour leur taux de détection élevé, leur faible taux de faux positifs et leur empreinte légère

RECHERCHE DE CYBERMENACES :

Les analystes experts utilisent des outils avancés et leur propre expertise pour rechercher de manière proactive les menaces sophistiquées qui peuvent se cacher dans le réseau sans être détectées.

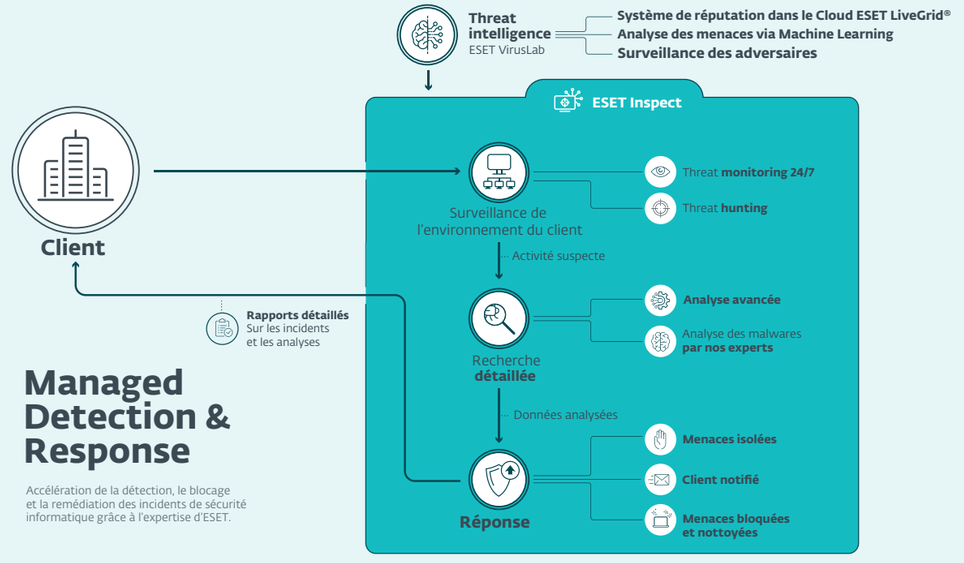
OPÉRATIONS 24 HEURES SUR 24 ET 7 JOURS SUR 7 :

Les auteurs de menaces opèrent dans le monde entier et dans de multiples fuseaux horaires. Le service doit donc être en état d'alerte élevé 24 heures sur 24.

Chapitre 3 : Comment ESET peut vous aider

Le service de MDR d'ESET combine des **technologies de pointe**, notamment l'XDR, avec des recherches et des renseignements sur les menaces s'appuyant sur plus de **30 ans d'expertise**. Le SOC de haut niveau qui en résulte est équipé d'outils permettant de tirer parti de nos **études de pointe** sur les malwares, l'ingénierie sociale, les techniques d'obscurcissement, les groupes de pirates, et bien plus encore.

Il ne s'agit pourtant pas d'une solutions toute faite. Chaque prestation commence par une évaluation de l'environnement, de l'infrastructure, de la composition organisationnel et de la culture générale de cybersécurité. Cela nous permet de créer un **profil de sécurité individuel du client** et d'agir comme une extension transparente de votre fonction de sécurité informatique. En fait, ESET possède une expérience significative d**e la protection des clients dans tous les secteurs**, et une expertise spécialisée dans différentes industries. L'utilisation de la technologie ESET permet aux clients de tirer parti de cette expérience.



Le service de MDR d'ESET, appelé ESET Detection and Response Ultimate, fournit une suite complète et multirégionale de produits et de services offrant **:**

- **Une équipe d'experts en cybersécurité** prête à prendre en charge le déploiement, l'optimisation, la surveillance quotidienne, la recherche périodique de menaces, l'analyse des malwares et le traitement des incidents pour un large éventail de tailles d'entreprises. Les équipes locales travaillent en étroite collaboration avec l'équipe mondiale de renseignements sur les menaces, qui est au cœur du MDR et de nos autres services managés.
- **Les trois dernières décennies passées à étudier des malwares** nous ont apporté l'expertise nécessaire pour surveiller les environnements des clients. Ce sont nos experts, qui partagent ces études mondialement reconnues sur WeLiveSecurity, qui fournissent le service.
- **Investigation et traitement des incidents,** avec analyse de base et analyse détaillée des fichiers, reverse engineering, enquêtes numériques et assistance pour le traitement.
- **Une présence locale** assurée par un réseau étendu de partenaires, de bureaux régionaux, et plusieurs équipes d'études de malwares au siège d'ESET et à travers le monde.
- **Assistance pour la sécurité des endpoints** afin de remédier au manque de détection des malwares, aux problèmes de désinfection, à l'investigation de comportements suspects et à l'atténuation des attaques de ransomwares.
- **Support ESET Inspect** pour répondre à toute question relative à notre outil d'XDR, comme l'aide à la création de règles personnalisées et d'exclusions.
- **Surveillance quotidienne des menaces** disponible 24 heures sur 24 et 7 jours sur 7, afin de garantir un environnement sûr et protégé en permanence, et détecter les menaces le plus tôt possible.
- **Recherche proactive des menaces** Une fois tous les trois mois par défaut pour garantir que l'environnement soit protégé contre les toutes dernières menaces. Ces enquêtes tirent parti de la connaissance approfondie qu'a ESET des menaces potentielles et des indicateurs de compromis remontés par les clients.
- **Le rapport mensuel** est le résultat de notre suivi et de notre prestation de services. Il contient également des avis de sécurité émis par nos analystes de sécurité. Dans les rapports que nous avons créés au fil des ans, nous constatons que le nombre de détections et d'incidents diminue au fur et à mesure que les clients suivent ces avis. Ils ne sont pas seulement liés à la configuration et aux produits ESET, mais contiennent des conseils pratiques sur le type d'activité que nous observons dans l'environnement, comme les détections de tentatives de force brute ou d'hameçonnage, et les utilisateurs spécifiques qui ont tendance à cliquer dessus.

Le service ESET MDR (Detection and Response Ultimate) est une solution holistique peut être acquise dans le cadre de l'offre ESET PROTECT MDR. Il s'agit d'une option plus complète combinant des produits et des services de prévention, de détection et de traitement. Managés via une interface unique, ils comprennent :

- Console d'administration (ESET PROTECT)
- Plateforme de protection des endpoints (ESET Endpoint Security)
- Sécurité des serveurs de fichiers (ESET Server Security)
- Défense contre les menaces avancées (ESET LiveGuard Advanced)
- Chiffrement complet des disques (ESET Full Disk Encryption)
- Détection et traitement étendus (ESET Inspect)
- Service MDR (ESET Detection and Response Ultimate)
- Service d'assistance premium (ESET Premium Support Advanced)

À quoi ressemble un déploiement réussi ?

LE CAS DE LA BRASSERIE ROYAL SWINKELSMDR ?

Royal Swinkels, la seconde plus grande brasserie des Pays-Bas fabriquant plus de 300 bières dans plus de huit brasseries à travers le monde, qui sont vendues dans plus de 130 pays, fait part de son expérience avec le déploiement du service de MDR d'ESET. De nos jours, la fabrication de la bière est un processus hautement automatisé qui s'appuie sur des technologies informatiques et industrielles (automatisation industrielle). Une faille de sécurité ou un événement négatif pourrait entraîner une perturbation de la chaîne d'approvisionnement, et avoir un impact conséquent sur la production et les revenus. Le service de MDR d'ESET aide l'entreprise à se protéger contre de tels risques. L'équipe ESET gère les détections et les interventions, filtre toutes les alertes, surveille l'environnement, 24 heures sur 24 et 7 jours sur 7 à l'aide d'un personnel qualifié en sécurité informatique.

Pour en savoir plus sur la manière dont ESET peut vous aider à améliorer la prévention, la détection et le traitement, consultez nos ressources sur ESET PROTECT MDR et la détection et le traitement étendus.

« De nos jours, toute entreprise de notre taille est fortement tributaire de l'informatique. D'une part, nous ne sommes pas assez grands pour posséder notre propre centre d'opérations de sécurité, mais d'autre part, nous ne sommes pas si petits que nous pouvons simplement nous permettre d'attendre que quelque chose se passe. Nous n'aimions pas cette approche réactive, nous avons donc choisi une approche proactive et c'est pourquoi nous avons choisi le MDR, afin d'en confier la gestion à ESET. »

Robert Heines : Royal Swinkels Family Brewers

Conclusion

Les décideurs en matière de sécurité sont confrontés à une période difficile de convergence des tendances. Au sortir des années de la pandémie mondiale, la surface d'attaque numérique des entreprises s'est considérablement étendue. Les auteurs de menaces sont de plus en plus enhardis, déterminés et dotés de ressources importantes. Les responsables des opérations de sécurité s'efforcent de repousser des attaques de plus en plus sophistiquées alors que les équipes sont sollicitées au maximum, que les solutions individuelles ne sont pas suffisamment efficaces et que les ressources restent rares. Dans ce contexte, le financement d'un véritable SOC 24 heures sur 24 et 7 jours sur 7 est hors de portée de toutes les entreprises,à l'exception des plus grandes.

Les atteintes à la sécurité sont inévitables, mais elles ne doivent pas nécessairement entraîner de graves dommages sur les finances et la réputation lorsque les adversaires peuvent être découverts et les incidents résolus rapidement. Le MDR a été conçu pour cela. Il confie les tâches les plus lourdes à un prestataire spécialisé, ce qui minimise le risque pour l'entreprise cliente tout en libérant le personnel pour qu'il se consacre à des tâches à forte valeur ajoutée et en dégageant des budgets qui pourront être stratégiquement affectés ailleurs.

« Un service de MDR forme une puissante combinaison de solutions avancées d'EDR/de détection et de traitement étendus (XDR), d'expertise humaine, de renseignements sur les menaces, de recherche de menaces, de consoles, de tableaux de bord et de rapports étendus, et de différentes formes de propriété intellectuelle développées par le prestataire de services de MDR. »

Robert Heines : The Evolution of Managed Security Services, doc. N° US48459521, décembre 2021, P. D. Harris, CISSP, CCSK

Indépendance, intégrité, innovation, expertise : ce sont les fondements sur lesquels ESET a bâti ses solutions de cybersécurité primées.

AVEC ESET, VOTRE ENTREPRISE PEUT BÉNÉFICIER DE :

- Une solution sur mesure adaptée à votre taille, à la complexité de votre système informatique et au niveau de protection requis
- Une couverture complète par les experts en cybersécurité d'ESET agissant en tant que partenaires silencieux
- La tranquillité d'esprit de savoir que toute information sensible partagée sera traitée par un partenaire de confiance
- Une assistance hyperlocale dans de nombreux pays
- afin de remédier au manque de détection des malwares, aux problèmes de désinfection, à l'investigation de comportements suspects et à l'atténuation des attaques de ransomwares.
- L'excellence de la recherche repose sur 30 ans d'expertise en cybersécurité
- Une assistance intégrée sur les ransomwares, l'analyse des malwares, l'analyse et le traitement des incidents sans frais supplémentaires
- Une protection des endpoints optimisée pour être performante tout en offrant une forte capacité de détection
- Une équipe de recherche sur les malwares offrant des décennies d'expertise pour atténuer la pénurie des compétences des clients

À propos d'ESET

Quand la technologie engendre le **progrès**, ESET est là pour **le protéger**.

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique de pointe pour offrir une protection complète et multicouche contre les menaces de cybersécurité aux entreprises et aux particuliers du monde entier.

ESET est depuis longtemps un pionnier des technologies de machine learning et dans le Cloud qui préviennent, détectent et traitent les malwares. ESET est une société privée qui encourage la recherche et le développement scientifiques dans le monde entier.

Canon

protégé par ESET depuis 2016
plus de 32 000 endpoints

partenaire FAI depuis 2008
2 millions d'utilisateurs

Allianz Suisse

protégé par ESET depuis 2016
plus de 4 000 boîtes mail

MITSUBISHI MOTORS
Drive your Ambition

protégé par ESET depuis 2017
plus de 9 000 endpoints

+ 30
années d'expertise

+ 1 Mrd
d'internautes protégés

+ 400 k
entreprises clientes

195
pays et territoires

13
centres de recherche



Plus de 30 ans
d'innovation continue



1er éditeur
Européen de solutions
de sécurité



Focus continu sur la
technologie



Croissance continue
depuis sa création

www.eset.com/fr