Phil Muncaster

# GUIDE DE L'ACHETEUR DES SERVICES DE DÉTECTION ET DE RÉPONSE GÉRÉES

## De quoi s'agit-il et pourquoi en avez-vous besoin?


eset®
Digital Security
Progress. Protected.

# TABLE DES MATIÈRES

# RÉSUMÉ

Les cyberrisques se multiplient pour les entreprises. Le potentiel d'attaque numérique a considérablement augmenté en raison des investissements réalisés lors de la pandémie. Les systèmes en nuage, les travailleurs distraits à la maison, les infrastructures à accès à distance, les terminaux éparpillés et les chaînes d'approvisionnement complexes constituent des cibles importantes et attrayantes pour les auteurs de menaces. En parallèle, le sous-sol de la cybercriminalité se professionnalise en développant ses propres chaînes d'approvisionnement complexes et ses offres de logiciels-services malveillants ainsi qu'en renouvelant ses tactiques, ses techniques et ses procédures (TTP).

Face à cette situation, la prévention des menaces, bien que souhaitable, n'est pas toujours possible. Les organisations doivent donc envisager d'adopter une approche plus holistique basée sur la prévention, la détection et la réponse. En effet, cela permet aux équipes d'empêcher les acteurs malveillants d'accéder à leurs systèmes et de les endommager. Si la prévention échoue, elles disposent également de capacités de détection et de réponse afin de repérer tout événement suspect et de neutraliser les menaces avant qu'il ne soit trop tard.

Cependant, quel outil de détection et de réponse les organisations doivent-elles choisir? Un service de détection et de réponse étendues (XDR) peut s'avérer utile, mais il engendre également des défis supplémentaires, notamment pour la recherche et le financement du personnel d'opérations de sécurité nécessaire afin de les mettre en œuvre, sans toutefois crouler sous les alertes.

Découvrez le service de détection et de réponse gérées (MDR), un type de service de sécurité gérée associant des outils, des technologies et des experts en cybersécurité pour offrir aux organisations de solides capacités de détection et de réponse. Lorsqu'il est correctement mis en place, le MDR permet de gérer plus efficacement les cyberrisques. Cependant, le fournisseur avec lequel les organisations choisissent de s'associer constitue le facteur déterminant.

**Les organisations doivent s'intéresser à des fournisseurs ayant fait leurs preuves en matière de veille sur les menaces et proposant des technologies présentant un taux de détection élevé, un taux de faux positifs bas et une faible empreinte. Elles doivent également tenir compte du service à la clientèle ainsi que de la mesure dans laquelle le MDR peut être adapté à leurs besoins spécifiques.**

# XDR : COMMENT FONCTIONNE-T-IL?

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.

*Source : Forrester, 2021*

# DÉFIS ACTUELS

Dans le cadre de la course à l'armement actuelle de la cybersécurité, on a souvent l'impression que nos adversaires ont une longueur d'avance sur nous. Ils sont soutenus par un réseau de cybercriminalité représentant des milliers de milliards de dollars chaque année qui leur fournit l'intégralité des outils, connaissances et données nécessaires pour lancer des attaques en toute facilité. Des états hostiles hébergent souvent les auteurs des menaces, qui peuvent ainsi lancer des attaques sans craindre de potentielles représailles des forces de l'ordre. De plus, les offres de logiciels-services (SaaS) malveillants permettent de coordonner plus facilement des campagnes audacieuses, même au sein de groupes moins avertis sur le plan technique.

De leur côté, les responsables de la sécurité de l'information (RSI) et leurs équipes sont de plus en plus sollicités dans plusieurs directions à la fois. Les investissements dans la transformation numérique réalisés au cours de la pandémie ont considérablement multiplié les risques de cyberattaques des entreprises. **Les environnements de télétravail** présentent des lacunes particulièrement dangereuses quant à la visibilité et au contrôle, aussi bien en raison des terminaux non protégés que des utilisateurs distraits ou négligents. Pourtant, de nombreuses équipes de sécurité manquent de personnel et sont submergées par un trop grand nombre de solutions ponctuelles inefficaces, ce qui renforce la complexité et réduit la productivité.

Les dommages potentiels, aussi bien financiers qu'en matière de réputation, causés par une grave violation de la sécurité n'ont jamais été aussi importants. Toutefois, la capacité des organisations à limiter efficacement les risques associés à de tels incidents se fragilise. En 2021, les coûts liés aux fuites de données au niveau mondial ont atteint un niveau record, avec une moyenne de plus de 4,2 millions de dollars. Selon un assureur international, un cinquième des entreprises des États-Unis et d'Europe ayant été victimes d'une cyberattaque cette année sont devenues insolvables.

Face à cette situation, une prévention **totale n'est tout simplement pas réaliste**. Un attaquant déterminé trouvera toujours un moyen de compromettre des cibles vulnérables. L'idéal consisterait alors à associer cette approche à des activités de détection et de réponse et, une fois de plus, les organisations sont en retard. En 2021, le temps moyen nécessaire à l'échelle mondiale pour identifier et contenir une violation était de 287 jours.

Le **XDR** utilise des analyses du comportement de l'ensemble des terminaux, du réseau, du nuage, des courriels et d'autres couches pour repérer toute activité suspecte et arrêter les attaquants avant qu'ils ne puissent avoir un impact.

Le **MDR** est en réalité une version externalisée du service de détection et de réponse étendues (XDR) que l'on associe parfois à d'autres outils.

Par conséquent, de nombreuses organisations se sont tournées vers le MDR, un type de service de sécurité gérée associant outils, technologies et experts en cybersécurité. Selon Gartner, la moitié des organisations mondiales utiliseront un MDR pour contenir les menaces d'ici 2025. Alors qu'avec le XDR, le client doit contrôler, détecter les failles et apporter des réponses, avec le MDR, un fournisseur de cybersécurité de confiance se chargera de ces tâches, permettant alors à l'ensemble du personnel de l'organisation de se focaliser sur d'autres tâches de grande valeur.

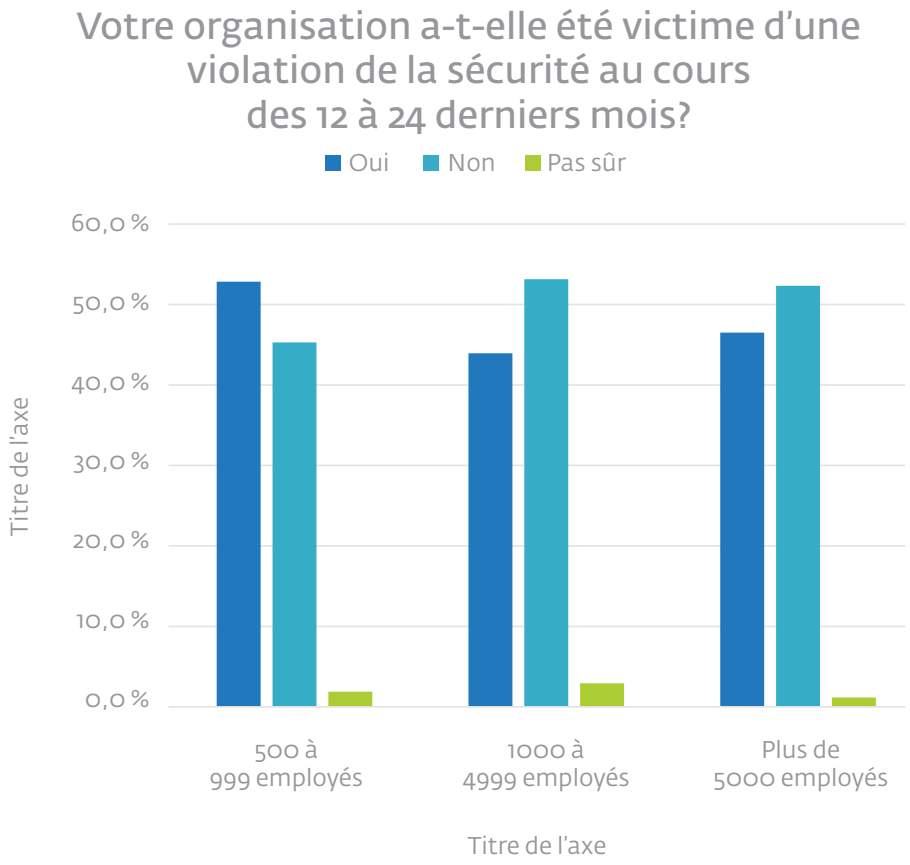
**91 %**

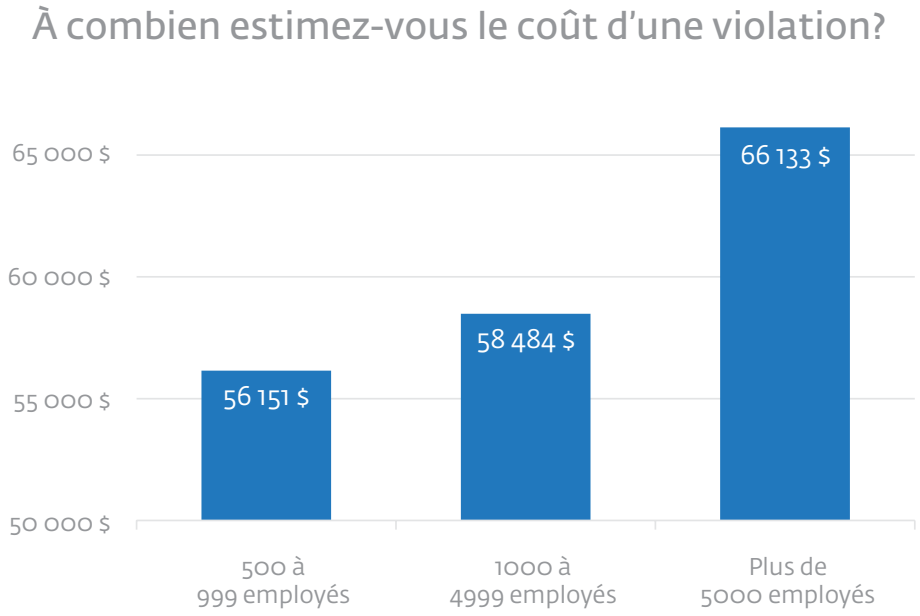
des entreprises dans le monde ont recours ou envisagent d'avoir recours à des services de déploiement, à une assistance technique, à une assistance de cybersécurité ainsi qu'à des services de traque ou de contrôle des menaces en tant que service.

*Source : sondage de recherche interne d'ESET auprès de 404 entreprises.*

# LES VIOLATIONS EXISTENT RÉELLEMENT

IDC




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

# POURQUOI AVEZ-VOUS BESOIN DU MDR?

Bien qu'en 2021, les dépenses en cybersécurité aient doublé pour les entreprises comptant entre 250 et 999 employés et augmenté de 65 % pour les sociétés avec plus de 1000 employés, les violations se produisent aujourd'hui à une échelle monumentale.

En 2021, les États-Unis ont observé un nombre record de fuites de données enregistrées publiquement. En effet, il était 23 % plus élevé que le record antérieur, qui s'élevait à 1506 violations. Au Royaume-Uni, 59 % des moyennes entreprises[1] et 72 % des grandes entreprises[2] ont déclaré avoir détecté des violations ou des cyberattaques en 2021. La menace de rançongiciels est particulièrement grave : un rapport a révélé que plus de 623 millions d'attaques ont été détectées en 2021, soit une augmentation de 105 % par rapport à l'année précédente.

## Expansion du potentiel d'attaque des entreprises

Pourquoi les sociétés ont-elles du mal à repousser leurs adversaires? Cela peut en partie s'expliquer par le fait qu'ils sont plus exposés que jamais auparavant en raison de leurs investissements dans des infrastructures numériques et l'émergence des espaces de travail hybrides. Selon McKinsey, la COVID-19 a poussé de nombreuses organisations à franchir un « point de basculement technologique », modifiant à jamais leur façon de travailler. Dans certains cas, elle a accéléré leur transformation de plusieurs années. Cependant, bien que cette évolution ait permis aux entreprises de devenir plus efficaces et de proposer des expériences innovantes à leurs clients et employés, elle a également considérablement augmenté le potentiel d'attaque numérique. Selon une étude, 43 % des entreprises du mode ont avoué « perdre le contrôle » de leur surface d'attaque numérique. Nous pouvons observer ce phénomène dans :

### L'informatique en nuage

Les infrastructures-services, les plateformes-services et les logiciels-services (IaaS, PaaS, SaaS) offrent d'énormes gains d'agilité informatique et des avantages en matière de coûts. Cependant, les organisations peinent notamment à sécuriser leurs environnements lorsqu'elles utilisent des IaaS et des PaaS. Le fait qu'un grand nombre de ces derniers gèrent plusieurs nuages hybrides rend le tout encore plus complexe. Les mauvaises configurations sont très courantes et elles sont décrites comme la principale cause des incidents de sécurité du nuage en 2021. Les acteurs des menaces recherchent régulièrement des systèmes exposés pour les compromettre.

---

1) Une moyenne entreprise compte entre 50 et 249 employés. Au total, 149 moyennes entreprises ont répondu au sondage.
2) Une grande entreprise compte 250 employés ou plus. Au total, 134 grandes entreprises ont répondu au sondage.

## Travail à distance

De nombreux systèmes domestiques restent dangereusement non protégés. Les employés retardent peut-être de manière irraisonnable l'application des correctifs sur leurs ordinateurs portables professionnels ou laissent l'état de sécurité de leurs périphériques personnels se dégrader. Un rapport de 2021 déclare que 45 % des leaders informatiques ont constaté que des imprimantes compromises étaient utilisées pour organiser des attaques. Les cybercriminels considèrent de plus en plus les espaces de travail domestiques comme un vecteur intéressant afin de compromettre les réseaux de l'entreprise. À présent que les espaces de travail hybrides se démocratisent, les travailleurs mobiles qui se connectent à des connexions Wi-Fi publiques et les ordinateurs partagés sont potentiellement exposés à un plus grand nombre de menaces.

## Employés travaillant à domicile

Bien que les périphériques de travail à distance soient souvent les cibles d'attaques, c'est également le cas de leurs propriétaires. Selon Microsoft, 80 % des professionnels de la sécurité ont observé une augmentation des menaces depuis les débuts du télétravail. Parmi eux, 62 % affirment que les campagnes d'hameçonnage ont augmenté plus que toute autre menace. Les employés travaillant à la maison seraient possiblement plus distraits ou prêts à prendre des risques que leurs collègues au bureau, ce qui en fait une cible parfaite pour l'ingénierie sociale. L'hameçonnage peut constituer une porte d'entrée pour les rançongiciels, les violations de données et d'autres formes de compromission. Plus d'un tiers (35 %) des entreprises affirment qu'elles ont observé des employés contourner ou désactiver des mesures de sécurité.

**« Depuis 2015, on a observé une augmentation de 25 % du nombre de signalements de violations, une hausse de 500 % du nombre de dossiers violés et, depuis 2017, le nombre d'attaques par rançongiciel a augmenté de 231 %. »**

*Best Practice : Security Matters, Now What? Forrester Research Inc, 2 mai 2022*

## Infrastructure à accès à distance

L'arrivée du télétravail de masse est également synonyme d'une hausse de l'utilisation d'outils tels que des réseaux privés virtuels ou le Remote Desktop Protocol (RDP), qui permettent aux personnes se trouvant hors du bureau d'accéder aux ressources internes. Le problème est que, bien souvent, leurs périphériques ne sont pas protégés ou sont mal configurés. Au lieu d'utiliser l'authentification multifacteur afin de renforcer la protection de l'accès, de nombreux comptes RPD ne sont protégés que par des identifiants faibles ou divulgués. Cela permet aux attaquants d'accéder assez aisément aux réseaux de l'entreprise en se faisant passer pour des utilisateurs légitimes. Le RPD représente l'un des trois principaux vecteurs d'attaque pour les rançongiciels : les tentatives de compromission ont atteint un niveau record de plus de 4,5 milliards[3] le 10 janvier 2022.


*Graphique des tendances des tentatives de connexion au RDP et du nombre de clients uniques au cours de la période du T3 2021 au T1 2022, moyenne mobile de sept jours, source : télémétrie d'ESET*

3) Calculé à l'aide d'une moyenne mobile de sept jours

## Chaînes d'approvisionnement

Cela se réfère aussi bien aux écosystèmes physiques ou numériques des partenaires ou fournisseurs. Dans le monde physique, il y a un risque constant que des employés ou des sous-traitants dotés d'un accès au réseau soient incités à communiquer leurs mots de passe ou que des voleurs s'emparent de leurs dispositifs. Au sein de la chaîne d'approvisionnement logicielle, les acteurs malveillants contaminant les mécanismes et les outils utilisés pour développer, déployer et mettre à jour le logiciel en y insérant un logiciel malveillant représentent sans doute une menace encore plus importante. Le fournisseur de logiciels de gestion informatique Kaseya a été compromis par l'opérateur de rançongiciels REvil, qui a profité de cet accès pour envoyer des mises à jour logicielles malveillantes aux clients MSP du fournisseur. Plus de 1000 clients ont été touchés en aval. Les codes sources ouverts, fréquemment utilisés par les équipes de développement et d'opérations pour accélérer le temps de création de valeur, constituent une autre source de préoccupations. En effet, ils peuvent engendrer des risques supplémentaires difficiles à gérer dans le cadre de dépendances logicielles complexes. Selon un rapport, plus de deux cinquièmes (41 %) des organisations n'ont pas confiance en la sécurité du logiciel ouvert qu'elles utilisent et uniquement 49 % d'entre elles déclarent que son utilisation est soumise à un règlement de sécurité.

**49 %**

des organisations disposent d'un règlement de sécurité pour leur logiciel ouvert.

*Source : State of Open Source Security Report, Snyk, 2022*

# Professionnalisation et innovation des auteurs des menaces

En parallèle, les acteurs malveillants prêts à exploiter ces failles de sécurité semblent s'être multipliés au cours des dernières années. Il existe même un marché prêt à l'emploi permettant de vendre des données volées, d'acheter des accès et des outils, et d'embaucher de nouvelles recrues. Il semble y avoir une réserve régulière de talents souhaitant vivre d'activités malveillantes, ce qui n'est pas le cas dans le domaine de la cybersécurité.

Nous observons de nombreuses innovations au sein du réseau de cybercriminalité, ce qui n'est pas de bon augure pour la sécurité des réseaux. Ces dernières comprennent :

## 1 Les rançongiciels en tant que services (RaaS)

Tout comme les SaaS ont popularisé le déploiement de logiciels à partir du nuage, les RaaS ont prospéré en lançant et en gérant des attaques par rançongiciel plus facilement. Les groupes affiliés peuvent obtenir jusqu'à 80 % des recettes des attaques. En retour, ils obtiennent un kit de démarrage comprenant la charge du rançongiciel et l'infrastructure d'attaque, ainsi qu'un site de violation sur lequel publier les données volées.

Tout comme les SaaS ont popularisé le déploiement de logiciels à partir du nuage, les RaaS ont prospéré en lançant et en gérant des attaques par rançongiciel plus facilement. Les groupes affiliés peuvent obtenir jusqu'à 80 % des recettes des attaques. En retour, ils obtiennent un kit de démarrage comprenant la charge du rançongiciel et l'infrastructure d'attaque, ainsi qu'un site de violation sur lequel publier les données volées.

## 2 Une monétisation agressive

La plupart des attaques par rançongiciel d'aujourd'hui impliquent à présent l'exfiltration et la fuite de données pour forcer le paiement. Toutefois, les groupes affiliés font de plus en plus pression sur leurs victimes à l'aide d'un ensemble de tactiques supplémentaires. Ils peuvent par exemple procéder à des attaques par déni de service ou contacter des clients, partenaires et journalistes pour leur faire part de ce qui s'est passé. Un groupe de rançongiciels modifie les sites des entreprises pour y afficher une demande de rançon. Un autre crée des sites de fuites sur mesure pour chacune de ses victimes de manière à ce que les clients et les employés puissent vérifier si leurs données ont été exposées.

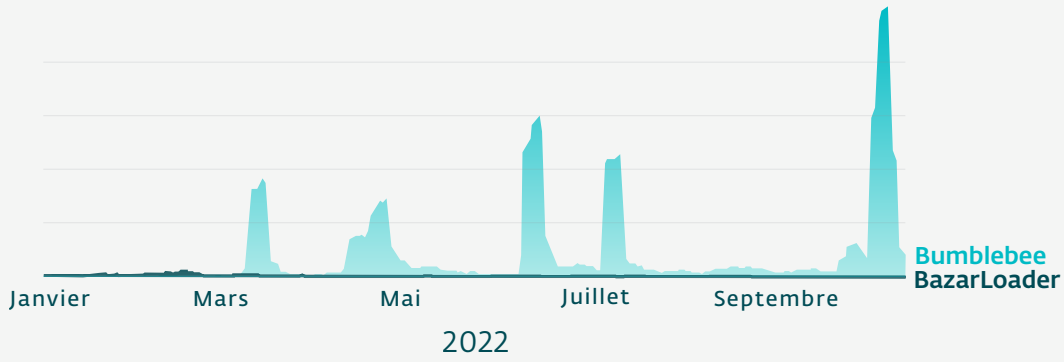
## 3 L'exploitation rapide des vulnérabilités

En 2021, le nombre de vulnérabilités détectées dans la US National Vulnerability Database (base de données de vulnérabilités nationale des États-Unis) a atteint un niveau record. Il est donc de plus en plus difficile pour les administrateurs sécurité de se tenir au courant des très nombreux correctifs publiés. Comme si cela ne suffisait pas, les groupes malveillants sont de plus en plus capables de réagir rapidement en cas de bogues du jour zéro et de les exploiter dans le cadre de leurs attaques. Dans les jours qui ont suivi la diffusion des correctifs de Microsoft Exchange Server destinés à remédier aux vulnérabilités de ProxyLogon, pas moins de 10 groupes de MPA les ont exploitées pour leurs attaques, affectant plus de 5000 serveurs Exchange dans plus de 115 pays.

## 4 La chaîne d'approvisionnement de cybermenaces

Le réseau de cybercriminalité dispose de plus en plus de ressources et se professionnalise progressivement. Des groupes spécialisés apparaissent afin de répondre à des exigences commerciales et opérationnelles spécifiques. Par exemple, en ce qui concerne les accès aux réseaux, on observe une hausse du nombre de courtiers d'accès initial. Ces experts compromettent les cibles avant de revendre ces accès en gros. Une équipe de recherche a constaté une hausse de 57 % du nombre de listes de courtiers d'accès initial publiées sur les forums de cybercriminels en 2021 en comparaison avec l'année précédente. Il y a également Bumblebee, un chargeur conçu pour télécharger et exécuter des charges supplémentaires. Il s'agit d'un des successeurs de TrickBot, un monstre bien connu et très résistant qui a survécu à deux tentatives de démantèlement en 2020 avant d'être fermé par ses opérateurs. Pendant un moment, BazarLoader avait récupéré le flambeau. Le chargeur a été actif jusqu'au début de l'année 2022, avant d'être rapidement devancé par Bumblebee. Bumblebee, fortement soupçonné d'être exploité par les mêmes acteurs malveillants que TrickBot et BazarLoader, est toujours actif à l'heure qu'il est. Le chargeur a lancé ses dernières campagnes à la mi-août 2022.

## TENDANCES DE DÉTECTION DE BUMBLEBEE ET BAZARLOADER




## 5 Outils légitimes et logiciel malveillant sans fichiers

Une fois que les acteurs malveillants se sont infiltrés dans les réseaux cibles, ils utilisent généralement des outils légitimes et un logiciel malveillant sans fichiers pour contourner les outils de sécurité traditionnels. L'idée consiste à utiliser des programmes non malveillants pour mener des activités malveillantes, par exemple pour se répandre dans le réseau, exfiltrer des données, découvrir des processus, voler des identifiants et exécuter des commandes de coque logicielle arbitraires. Ces programmes comprennent PowerShell, PsExec et Cobalt Strike.

## 6 Avancées en matière d'hameçonnage et d'ingénierie sociale

Parfois, les anciennes méthodes sont les plus efficaces. L'hameçonnage représente toujours l'un des trois principaux vecteurs pour les rançongiciels et il a même atteint un niveau record au cours du 1er trimestre 2022. Les acteurs malveillants continuent d'ajuster leurs techniques de manière à maintenir une longueur d'avance sur les filtres de courriels et les programmes de formation en sécurité. L'une des menaces les plus populaires en matière de courriels est le piratage, où les attaquants compromettent une boîte de réception avant de pirater des conversations existantes afin de disséminer des liens d'hameçonnage. Étant donné qu'un message de réponse semble moins suspect qu'un message non sollicité, les utilisateurs ont plus de chances de cliquer sur les liens inclus. L'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 téléphone intelligent et donc plus susceptibles de cliquer. En 2021, un fournisseur a constaté que les tentatives d'hameçonnage par SMS ont doublé aux États-Unis et il a compté plus de 500 campagnes de piratage reliées à 16 familles de logiciels malveillants différentes.

# De la prévention au XDR

Une grande partie des innovations de la cybercriminalité sont certainement en lien avec les rançongiciels. Par conséquent, les rançongiciels représentent dorénavant le cyberrisque le plus important pour les organisations selon les experts en matière de sécurité du gouvernement britannique. On comprend rapidement pourquoi lorsque l'on sait qu'un seul groupe (Conti) a réussi à compromettre au moins 859 organisations en seulement deux ans, dont 40 en seulement un mois, parvenant ainsi à gagner des milliards en cryptomonnaie. Selon une estimation, les détections de rançongiciels auraient augmenté de 148 % d'une année sur l'autre. On en aurait compté 470 millions au cours des trois premiers trimestres de 2021, ce qui en fait la pire année jamais enregistrée.

Toutefois, les rançongiciels sont loin d'être la seule menace à laquelle les organisations sont exposées aujourd'hui. Les vols de données, les logiciels malveillants de cryptominage, les chevaux de Troie bancaires et les logiciels espions, entre autres, jouent également des coudes pour se faire une place.

L'impact cumulé de ces tendances doit mener les leaders de la sécurité informatique à une conclusion inéluctable. **La prévention des menaces doit systématiquement être privilégiée, mais elle n'est pas toujours possible.** Les acteurs malveillants peuvent s'infiltrer de trop nombreuses manières dans les environnements des sociétés sans être détectés. 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, de détection et de réponse (EPDR) d'ESET, en combinant plusieurs couches de technologie de sécurité. Elle cherche dans un premier temps à protéger les entreprises en empêchant les codes et les acteurs malveillants de pénétrer dans le système de l'utilisateur ou de l'endommager. Toutefois, en cas d'échec, cette approche dispose de capacités de détection et de réponse solides afin de limiter les menaces avancées parvenant à compromettre le 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[5] est une évolution de l'EDR, qui optimise la détection, l'enquête, les réponses apportées et la traque des menaces en temps réel.

5) Définition du XDR par Forrester en 2021

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 de se reproduire?**

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

# En quoi le MDR peut-il vous aider?

Toutefois, même avec l'aide du XDR, les équipes des opérations de sécurité rencontrent des défis considérables d'un point de vue organisationnel. La plupart de ces derniers, notamment le manque de connaissances, d'expertise et de ressources en interne, sont particulièrement répandus parmi les PME. Les défis généraux des organisations comprennent :

## Les pénuries de talents

Le secteur de la cybersécurité nécessite actuellement 2,7 millions de travailleurs supplémentaires et les analystes des centres des opérations de sécurité (SOC) sont sans doute parmi les plus difficiles à trouver et à retenir. Le problème est aggravé par le grand nombre d'analystes qui envisagent de démissionner en 2023 en raison du stress et de l'épuisement professionnel associés au trop grand nombre d'alertes. Les généralistes de l'informatique ne peuvent souvent pas consacrer plusieurs heures par jour à la gestion d'une solution XDR. Ces difficultés sont exacerbées au sein des PME, qui manquent généralement des connaissances et de l'expertise nécessaires en interne pour gérer un SOC. Par conséquent, elles pourraient encore plus tirer profit d'un MDR.

## Les coûts

Les leaders de la sécurité ne doivent pas uniquement réfléchir aux coûts liés à l'embauche et au maintien des talents pour la gestion du SOC. Ils doivent également trouver la bonne association d'outils pour fournir à leurs analystes les données dont ils ont besoin. Cela peut représenter une dépense initiale importante et ils devront ensuite prendre en charge les frais des licences.

La charge financière qui pèse sur les organisations qui choisissent de mettre en place un centre des opérations en interne est de plus en plus lourde. Selon une étude, le rendement du capital investi perçu est en baisse dans plus de la moitié des organisations en raison de la gestion de la complexité. Ce rapport indique également que les coûts liés à l'ingénierie de la sécurité avoisinent 3 millions de dollars américains chaque année, mais qu'uniquement 51 % des organisations considèrent ces efforts efficaces.

## Les failles de sécurité

Les outils utilisés ne sont parfois pas à la hauteur. Cela peut entraîner un trop grand nombre d'alertes ainsi que la fatigue qui s'ensuit. Si le personnel du SOC croule sous les faux positifs, ses membres risquent de passer des heures à examiner de fausses alertes et de manquer des alertes légitimes. Lorsque plusieurs outils sont utilisés au sein d'un SOC, ils peuvent également créer des failles.

## La gestion

L'obtention, l'installation et la bonne configuration des produits ne sont que les premières étapes. La gestion de plusieurs outils et de plusieurs analystes du SOC dans plusieurs juridictions peut présenter de nombreux défis. Lorsque les ressources sont déjà sollicitées à l'extrême, certaines tâches importantes peuvent être négligées. On peut facilement perdre pied en luttant contre les menaces émergentes, et ne pas avoir le temps de réfléchir et de planifier notre stratégie.

On peut avoir l'impression que les équipes de sécurité informatique des entreprises veulent et sont tout à fait capables de faire face à ces défis en constante évolution, qu'elles comprennent entièrement le logiciel qu'elles achètent et qu'elles forment des SOC solides pour lutter contre les cybermenaces. En réalité, une étude menée par ESET[4] indique que :

**68 %** **des entreprises préfèrent que leur fournisseur de services de sécurité se charge du déploiement des produits de sécurité**

**75 %** **s'attendent à ce que leur fournisseur de services de sécurité leur offre une assistance vis-à-vis de leurs problèmes de cybersécurité, des conseils et une réponse aux incidents**

**87 %** **souhaitent disposer de services d'assistance disponibles 24 heures sur 24, 7 jours sur 7 et 365 jours par an**

**90 %** **veulent que les fournisseurs offrent des services de surveillance, de traque, de réponse et de correction aux menaces**

4) Sondage de recherche interne d'ESET auprès de 404 entreprises.

# Quels sont les principaux avantages du MDR?

Le MDR présente des avantages considérables pour les organisations qui souhaitent limiter les cyberrisques, mais qui ne disposent pas des ressources nécessaires en interne pour cela. Bien que le MDR puisse varier en fonction du fournisseur, il doit comprendre au moins une variante des éléments suivants :

## Détection de menaces

Les acteurs malveillants peuvent se faufiler à travers les défenses périmétriques d'un nombre incalculable de manières différentes. Toutefois, en menant des analyses du comportement, ces derniers peuvent être rapidement détectés et les organisations pourront prendre des mesures pour mettre fin aux attaques. Une traque proactive des menaces peut également être mise en place afin de détecter des attaques sophistiquées pouvant échapper aux contrôles automatisés.

## Définition des priorités

Les analyses intelligentes fournissent un contexte qui permet aux systèmes MDR de transformer les données en informations exploitables afin de déclencher des alertes plus fiables. Il s'agit d'une phase essentielle du processus du MDR étant donné que des alertes trop nombreuses peuvent souvent mettre en difficulté les équipes des SOC.

**« Les services MDR couvrent déjà une grande partie des objectifs du XDR. Le MDR garantit de meilleurs résultats en matière de sécurité en fournissant des outils et des technologies telles que la veille sur les menaces, une traque des menaces, un contrôle constant 24 heures sur 24 et 7 jours sur 7, des analyses avancées ainsi que le confinement et la résolution d'incidents ou de violations s'il est suspecté ou prouvé que des données ont été exfiltrées ou détruites. Selon IDC, l'offre MDR devrait fournir plus que des conseils et des recommandations. »**

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

## Analyse

L'analyse du comportement automatique s'associe à l'évaluation humaine afin de déterminer si une alerte est légitime et d'identifier les mesures à prendre pour résoudre le problème.

## Réponse

Grâce à la phase d'analyse précédente, le système identifiera le type de réponse nécessaire pour contenir et éliminer la menace, et corriger tout système compromis. Cela 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;
- le fournisseur du service MDR peut également optimiser et gérer la technologie dorsale afin de s'aligner sur le 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 au sein de leur SOC;
- 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.

# QUE 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 :

**L'excellence en matière de recherche :**
Des renseignements de premier ordre fondés sur des capacités de recherche de pointe.

**Un service à la clientèle de haute qualité :**
Comprenant une assistance disponible dans la langue locale ainsi qu'une présence et une disponibilité dans le monde entier.

**Des possibilités de personnalisation :**
Une solution sur mesure et personnalisée en fonction de la taille, de la complexité informatique et du niveau de protection requis de chaque client.

**Des capacités de détection et de réponse de pointe :**
Les produits doivent être testés de manière indépendante et réputés pour leurs taux de détection élevés, leur nombre limité de faux positifs et leur faible empreinte.

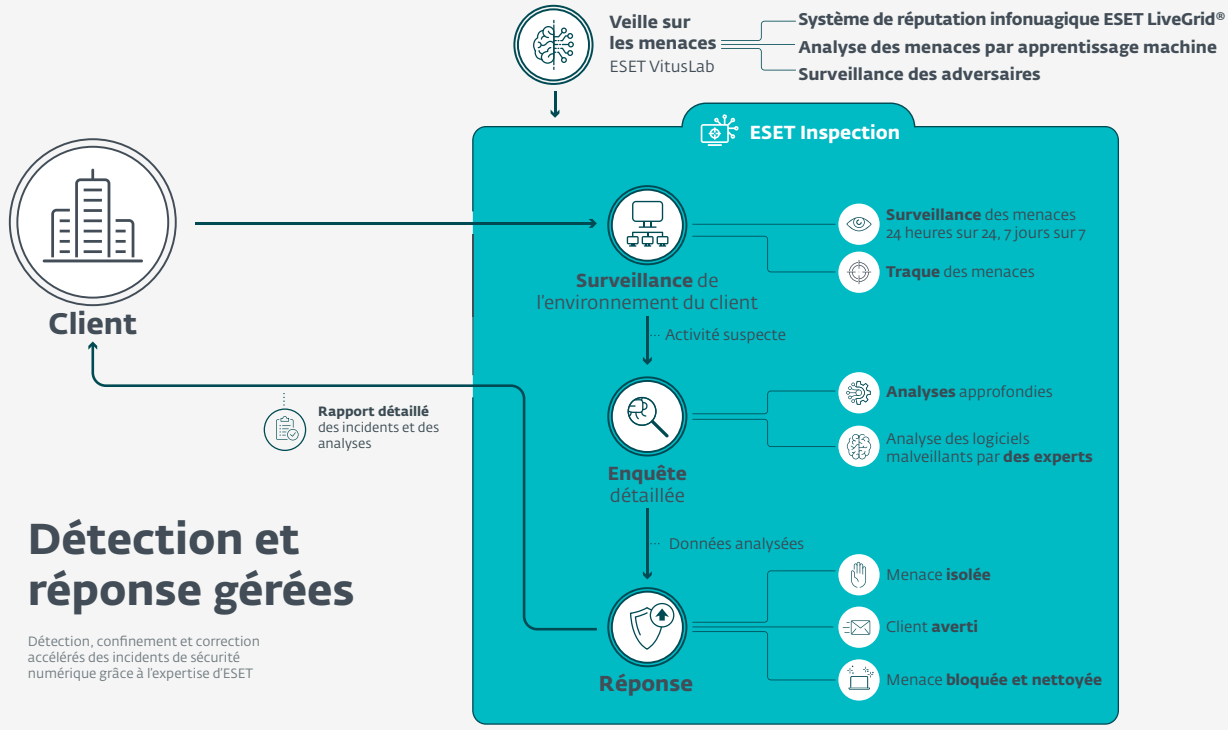
**Une traque des cybermenaces :**
Les analystes experts utilisent des outils avancés ainsi que leur propre expertise pour examiner le réseau et y rechercher de manière proactive des menaces sophistiquées potentiellement non détectées.

**Des services disponibles 24 heures sur 24, 7 jours sur 7, 365 jours par an :**
Les acteurs malveillants opèrent depuis le monde entier et différents fuseaux horaires. Par conséquent, tout service doit être en état d'alerte de manière constante.

# EN QUOI POUVONS-NOUS VOUS AIDER CHEZ ESET AVEC LE MDR?

Les capacités de MDR d'ESET associent des solutions dotées d'une **technologie de pointe**, y compris des solutions de XDR, à des capacités de classe mondiale en matière de recherche sur la sécurité et de veille sur les menaces fondées sur plus de **30 ans d'expertise**. Tout cela aboutit à un SOC adapté aux entreprises et doté des outils nécessaires pour tirer parti de nos **recherches révolutionnaires** sur les logiciels malveillants, l'ingénierie sociale, les techniques d'obscurcissement, les groupes MPA et bien plus encore.

Cependant, ce service peut s'adapter aux différentes organisations. Chaque engagement commence par une évaluation de l'environnement, de l'infrastructure, de la composition de l'organisation et de la culture générale en matière de cybersécurité du client. Cela nous permet de créer un **profil de sécurité individuel** et d'agir comme une extension intégrée à votre fonction de sécurité informatique. En réalité, ESET dispose d'une grande expérience dans la **protection de clients appartenant à divers secteurs** ainsi que d'une expertise spécialisée dans une variété d'industries et de marchés verticaux. En utilisant la technologie d'ESET, nos clients peuvent tirer profit de cette expérience.



Le service MDR d'ESET, ESET Detection and Response Ultimate, fournit une gamme complète de produits et de services multirégionaux comprenant les éléments suivants :

- **Une équipe d'experts en cybersécurité** prête à se charger du déploiement, de l'optimisation, du contrôle quotidien, de la traque périodique des menaces, de l'analyse de logiciels malveillants et des réponses aux incidents pour des organisations de tailles diverses et variées. Les équipes locales travaillent en étroite collaboration avec l'équipe mondiale de veille sur les menaces, qui se situe au cœur du MDR et des autres services que nous proposons.
- **Nos plus de 30 années d'expérience dans la recherche sur les logiciels malveillants** nous dotant d'une expertise qui nous permet de contrôler les environnements de nos clients afin d'y détecter les menaces et les violations. Ces services sont fournis par des experts impliqués dans nos efforts de recherche reconnus mondialement en collaboration avec WeLiveSecurity.
- **Des services d'enquête et de réponse aux incidents**, notamment une analyse basique et détaillée des fichiers, une rétroingénierie, une criminalistique numérique et une assistance afin de répondre aux incidents.
- **Une présence locale à une échelle mondiale** assurée par un large réseau de partenaires, des bureaux régionaux et plusieurs équipes de recherche sur les logiciels malveillants au siège d'ESET et dans le monde entier.
- **Une assistance technique de sécurité des terminaux** pour s'occuper des détections manquantes de logiciels malveillants, des problèmes de nettoyage et des enquêtes en cas de comportement suspect, ainsi que pour limiter les attaques par rançongiciel.
- **L'assistance d'ESET Inspection** pour aider les organisations lorsqu'elles ont des questions concernant notre outil XDR, par exemple sur la création de règles personnalisées et d'exclusions.
- **Un contrôle quotidien des menaces** disponible 24 jours sur 24, 7 jours sur 7 et 365 jours par an pour garantir la propreté et la protection permanente de l'environnement, et s'assurer que les menaces sont détectées le plus tôt possible.
- **Une traque proactive des menaces** effectuée par défaut tous les trois mois afin de veiller à ce que l'environnement soit protégé contre les menaces les plus récentes. Ces enquêtes s'appuient sur les connaissances

approfondies d'ESET en matière d'indicateurs de compromission et les menaces potentielles indiquées par les clients.

- **Un rapport mensuel** résultant de notre contrôle et de notre prestation de services. Il contient également des conseils de nos analystes relatifs à la sécurité. Dans les rapports que nous créons au fil des années, nous pouvons observer une baisse graduelle du nombre de détections et d'incidents lorsque les clients suivent nos conseils. Ces derniers ne portent pas uniquement sur les produits ESET et leur configuration, mais ils indiquent également le type d'activité que nous observons au sein de l'environnement, comme des détections de force brute ou l'hameçonnage ainsi que les utilisateurs spécifiques qui ont tendance à cliquer sur ceux-ci.

Le service MDR d'ESET (Detection and Response Ultimate) est une solution holistique qui peut être achetée dans le cadre de l'offre ESET PROTECTION MDR. Il s'agit d'une option plus exhaustive associant des produits et des services prenant en charge la prévention, la détection et la réponse. Gérés depuis un poste unique, ces derniers comprennent :

- une console de gestion (ESET PROTECTION);
- une plateforme de sécurité des terminaux (ESET Sécurité des terminaux);
- la sécurité du serveur de fichiers (ESET Sécurité des serveurs);
- une protection avancée contre les menaces (ESET LiveGuard avancé);
- une chiffrement de disque complet (ESET Chiffrement du disque entier);
- des services de détection et de réponse étendus (ESET Inspection);
- le service MDR (ESET Detection and Response Ultimate);
- un service d'assistance premium (ESET Premium Support Advanced).

# À QUOI RESSEMBLE UN DÉPLOIEMENT RÉUSSI DU MDR?

## LE CAS DE ROYAL SWINKELS BREWERY

Royal Swinkels, la deuxième plus grande brasserie des Pays-Bas produisant plus de 300 bières dans plus de huit brasseries du monde entier et vendues dans plus de 130 pays, partage son expérience quant au déploiement du MDR d'ESET. De nos jours, la production de bière est un processus très automatisé qui dépend de l'informatique et de l'automatisation de l'industrie. Une violation ou un événement nocif pourraient entraîner une interruption de la chaîne d'approvisionnement, ce qui aurait un impact considérable sur les livraisons et les revenus. Le MDR d'ESET les aide à se protéger contre de tels risques. L'équipe d'ESET gère les détections et les réponses, filtre les alertes et contrôle l'environnement. Il s'agit d'un service assuré 24 heures sur 24 et 7 jours sur 7 par un personnel de sécurité informatique qualifié.

**« De nos jours, toutes les entreprises de notre taille dépendent énormément de l'informatique. D'un côté, notre entreprise n'est pas assez grande pour que nous disposions de notre propre centre des opérations de sécurité, mais de l'autre, elle est trop grande pour que nous puissions nous permettre d'attendre que quelque chose se produise. Nous n'aimions pas cette approche réactive, donc nous avons choisi une approche proactive. C'est pourquoi nous nous sommes tournés vers le MDR afin de pouvoir confier la gestion à ESET. »**

**Robert Heines,**
Royal Swinkels Family Brewers

Pour en savoir plus à propos de la manière dont ESET peut vous aider à renforcer votre approche de prévention, de détection et de réponse, consultez nos ressources sur ESET PROTECTION MDR et nos services de détection et réponse étendues.

# CONCLUSION

Les tendances convergentes actuelles compliquent les prises de décisions en matière de sécurité. Après plusieurs années de crise mondiale, le potentiel d'attaque numérique des entreprises s'est considérablement développé. De leur côté, les acteurs malveillants deviennent plus audacieux et déterminés, et ils disposent de plus en plus de ressources. Les responsables des opérations de sécurité peinent à détourner des attaques plus sophistiquées lorsque les équipes sont sollicitées à l'extrême, les solutions ponctuelles sont inefficaces et les ressources restent rares. Dans ce contexte, seules les plus grandes entreprises peuvent se permettre de financer un SOC complet disponible 24 heures sur 24, 7 jours sur 7 et 365 jours par an.

Les violations sont inévitables, mais elles ne doivent pas nécessairement entraîner de graves dommages financiers et de réputation si les adversaires peuvent être détectés et les incidents résolus rapidement. Le MDR a été conçu pour cela. Il confie les tâches les plus lourdes à un fournisseur spécialisé, ce qui minimise les risques de sécurité pour l'organisation cliente. Ainsi, son personnel peut se consacrer à des tâches de grande valeur et elle peut dépenser ses recettes autrement et de manière stratégique.

**« Les fournisseurs de services peuvent déployer des services MDR en associant les capacités existantes des clients, les outils ou services fournis par les partenaires de cybersécurité et la propriété intellectuelle privée. Ce partenariat forme une puissante association de solutions EDR ainsi que de détection et de réponse étendues (XDR) avancées, d'expertise humaine, de renseignements sur les menaces, de traque des menaces, de consoles améliorées, de tableaux de bord et de rapports, et de diverses formes de propriété intellectuelle développées par le fournisseur du service MDR. »**

*Source : IDC, The Evolution of Managed Security Services, document n° US48459521, décembre 2021, P. D. Harris, CISSP, CCSK*

Indépendance, intégrité, innovation et expertise : voici les valeurs sur lesquelles se fondent les solutions de cybersécurité primées d'ESET.

## Avec ESET, votre organisation pourra bénéficier des éléments suivants :

- une solution sur mesure et personnalisée en fonction de votre taille, de votre complexité informatique et du niveau de protection dont vous avez besoin;
- une couverture complète assurée par les experts en cybersécurité d'ESET agissant comme des partenaires discrets;
- une tranquillité d'esprit de savoir que toute information sensible partagée sera traitée par un partenaire de confiance;
- une assistance disponible en langue locale dans de nombreux pays;
- une excellence en matière de recherche fondée sur 30 ans d'expertise en matière de cybersécurité;
- une assistance intégrée en matière de rançongiciels, une analyse des logiciels malveillants, une criminalistique numérique et une réponse en cas d'incident sans frais supplémentaires;
- une optimisation de premier plan de la sécurité des terminaux pour renforcer les performances tout en offrant de grandes capacités de détection;
- une équipe de recherche sur les logiciels malveillants mettant à disposition des clients des années d'expertise afin de limiter leurs pénuries de compétences.

EN SAVOIR PLUS SUR ESET PROTECTION MDR

# À PROPOS D'ESET

Depuis plus de 30 ans, ESET® développe les meilleurs logiciels et services en sécurité informatique de l'industrie pour fournir une protection multicouche et complète contre les menaces en matière de cybersécurité à des entreprises et des clients du monde entier.

ESET est un précurseur de longue date en matière d'apprentissage machine et de technologies basées sur le nuage afin d'empêcher l'action des logiciels malveillants, de les détecter et d'y répondre. ESET appartient à des intérêts privés et valorise la recherche et le développement scientifiques dans le monde.

## ESET EN CHIFFRES

**Plus de 1 milliard**
d'internautes protégés

**Plus de 400 000**
utilisateurs commerciaux

**Plus de 200**
pays et territoires

**13**
centres internationaux de R et D

APPUYEZ-VOUS SUR UN LEADER TECHNOLOGIQUE MONDIAL POUR PROTÉGER VOTRE ENTREPRISE