Devolutions

Le MDR est-il la bonne solution pour votre entreprise?

LA SOLUTION MDR EST UN SERVICE EXTERNALISÉ DE GESTION DE LA CYBERSÉCURITÉ

La solution MDR est un service externalisé de gestion de la cybersécurité qui fournit aux organisations une visibilité à 360 degrés de la sécurité, des services de détection proactive des cybermenaces et de leur élimination une fois découvert. Le MDR combine à la fois une technologie et l'expertise humaine afin d'assurer la défense des clients.

Que fait le service MDR pour une organisation?

Résout le défi des RH

Le MDR résout un problème important qui touche de plus en plus d'entreprises : le manque de compétences en matière de sécurité. Bien que la formation et la mise en place d'équipes de sécurité apte à chasser les menaces à plein temps puissent être jouables pour les grandes organisations, la plupart des entreprises trouveront cette proposition difficile étant donné leurs ressources limitées. C'est particulièrement vrai pour les PME qui sont souvent la cible de cyberattaques, mais qui manquent de main-d'œuvre pour de telles équipes.

Même les organisations qui sont prêtes à dépenser du temps et de l'argent peuvent avoir de la difficulté à trouver le personnel approprié. Les compétences requises pour pouvoir reconnaître les signaux reliés à une attaque informatique se font rares même parmi les spécialistes en sécurité informatique.

Aplatit la courbe d'apprentissage

Il existe aussi une réalité quant à l'incapacité des entreprises à jongler avec une variété d'outils de sécurité qui demande des connaissances uniques. Les organisations se retrouvent donc avec une série d'outils de sécurité ayant une configuration inadéquate pour répondre à leur besoin de sécurité. Le service MDR utilise sa propre technologie et offre toujours une configuration optimale pour le client. StreamScan a développé sa propre technologie d'intelligence artificielle pour maximiser les taux de détection chez ses clients.

Élimine la surcharge d'alertes

Le volume important d'alertes que les équipes de sécurité reçoivent est souvent négligé. Un grand nombre de ces alertes ne peuvent pas être facilement identifiées comme étant malveillantes et doivent être vérifiées individuellement. Les équipes de sécurité doivent donc corréler ces menaces afin de relever si des indicateurs apparemment insignifiants s'additionnent dans le cadre d'une attaque plus vaste. Cela peut submerger les petites équipes de sécurité, leur enlever du temps et des ressources précieuses pour leurs autres tâches.

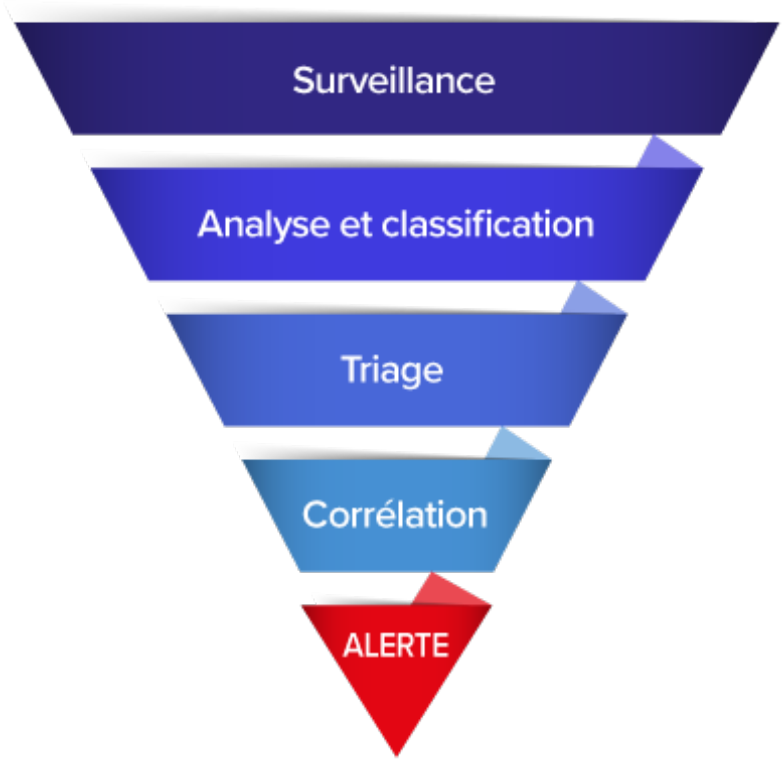
Notre solution MDR vise à résoudre ce problème non seulement en détectant les menaces, mais aussi en analysant tous les facteurs et indicateurs impliqués dans une alerte. Le MDR fournit également des recommandations et des changements aux organisations en fonction de l'interprétation des événements liés à la sécurité. L'une des compétences les plus importantes à avoir est la capacité de contextualiser et d'analyser les indicateurs de compromission afin de mieux positionner l'entreprise contre de futures attaques. Les technologies de sécurité ont peut-être la capacité de bloquer les menaces… mais afin d'approfondir le « comment, le pourquoi et le quoi » des incidents, cela exige une touche humaine.

Comble le déficit de compétences

Le MDR est conçu pour résoudre le problème du manque de compétences d'une organisation en matière de cybersécurité. Il aborde la question des menaces plus avancées qu'une équipe informatique interne ne peut pas traiter, idéalement à un coût inférieur à ce que l'entreprise devra dépenser pour construire sa propre équipe de sécurité spécialisée.

Comment fonctionne le service MDR de StreamScan?

Notre équipe MDR fonctionne 24/7 s'assurant que votre réseau est sécurisé et agit comme une extension de votre équipe TI interne. Cette équipe est composée de plusieurs personnes ayant diverses expertises permettant de couvrir la gestion des cyberattaques : détection/prévention d'intrusions, réponse aux incidents, rétro-ingénierie de codes malicieux, investigation numérique et collecte de preuve, etc. Les activités réalisées par notre équipe MDR sont les suivantes :



SURVEILLANCE : 30 %

À distance, l'équipe de StreamScan surveille en permanence les signaux, les alertes et les événements de sécurité générés par la technologie CDS ainsi que les outils de sécurité dans la portée de la supervision de votre réseau. Le moindre comportement suspect détecté par le CDS (ou par les autres outils) est isolé et pris en charge par nos analystes.

ANALYSE & CLASSIFICATION : 30 %

Véritables chasseurs en cybermenaces (***threat hunter***), nos analystes investiguent sur les cas suspects identifiés, afin de confirmer s'il y a un enjeu de sécurité. L'objectif est de traiter les cas suspects en amont avant qu'ils ne se transforment en problème. L'analyse aboutit à la classification des signaux en deux catégories : les vraies menaces et les faux positifs.

TRIAGE : 10 %

Suite à cette analyse, un billet est créé dans le système CDS de StreamScan pour permettre une investigation approfondie des cas problématiques. Ils seront classifiés selon leur niveau de sévérité et leur impact (FAIBLE, MOYEN, ÉLEVÉ ou CRITIQUE). La riposte est automatique pour les cas ÉLEVÉ et CRITIQUE.

CORRÉLATION : 20 %

Lorsque l'équipe StreamScan fait face à un cas complexe, elle analyse en profondeur les signaux d'attaques collectés, croise les multiples informations et enquête sur certains phénomènes. Parfois, nous faisons de la rétro-ingénierie de code malicieux où nous reproduisons le scénario de l'attaque afin d'en maîtriser tous les paramètres. Cela permet d'anticiper le prochain coup et de le contrecarrer rapidement.

ALERTE ET TICKET : 10 %

Nous notifions nos clients et proposons une intervention en profondeur afin de résoudre le problème le plus

rapidement et efficacement possible. La notification est faite par téléphone ou courriel selon le niveau de sévérité des cybermenaces.

Nous comprenons que les équipes TI de nos clients sont très occupées. Nous fournissons donc toutes les informations nécessaires pour prendre des mesures, sans que ces équipes aient à faire des recherches additionnelles. Par exemple, nous allons jusqu'à fournir le lien où les équipes TI doivent télécharger le correctif d'une vulnérabilité identifiée.

Note : en plus des activités réalisées par notre équipe MDR, le CDS dispose de fonctionnalités lui permettant de bloquer automatiquement certains types de cyberattaques. Il dispose aussi de fonctions de notification par courriel et SMS. La combinaison du CDS et de l'expertise humaine de notre équipe MDR permet une gestion proactive de la cybersécurité, ce qui est adapté à la réalité des cyberattaques d'aujourd'hui.

Rapports périodiques

Nous fournissons un rapport mensuel de la supervision de votre réseau incluant un résumé des activités de sécurité observées dans votre réseau, des mesures de réponse prises ainsi que des recommandations de rehaussement de la sécurité. Ce rapport sert au rehaussement en continu de votre sécurité.

Le Cloud et le réseau interne sont couverts

Notre service MDR couvre votre réseau interne ainsi que vos systèmes et applications dans le Cloud (par exemple : Microsoft 365). L'objectif est d'avoir une visibilité à 360 degrés de votre réseau et de gérer sa sécurité en un seul endroit.

Notre technologie CDS peut s'installer dans le Cloud, sur un environnement virtuel (serveur virtuel) ou sous forme de serveur physique.

Le MDR : une valeur inestimable

Comme vous l'aurez constaté, notre solution MDR combine la technologie et l'humain pour une gestion efficace de votre sécurité. Tout en vous donnant accès à plusieurs ressources ayant divers profils, nos services et solution MDR coûte une fraction de ce que vous auriez payé pour déployer vos propres technologies de sécurité et les gérer au quotidien.

Présentation de l'auteur

Karim Ganame, Fondateur et Président, StreamScan

Avec plus de 20 ans d'expérience, Karim, docteur en cybersécurité, est un chercheur, un enseignant ainsi qu'un leader expérimenté dans le domaine de la cybersécurité et de l'IA. Karim est un leader réputé, un conférencier et commentateur reconnu sur tout ce qui touche à la cybersécurité au Québec. Depuis la dernière décennie, Karim est à la tête du développement de l'unique technologie de surveillance de réseau, le CDS et du service de détection et de réponse gérée de StreamScan.