Technologies de sécurité MDR : Développeur vs revendeur/intégrateurs

Devolutions

L'ÉCOSYSTÈME DES ENTREPRISES QUI OFFRENT DES SERVICES DE SUPERVISION DE LA SÉCURITÉ EST TRÈS DIVERSIFIÉ

L'écosystème des entreprises qui offrent des services de supervision de la sécurité est très diversifié. Par exemple, il existe des compagnies d'impartition TI qui offrent des services de sécurité (en plus d'autres services TI en réseautique, ou autres), des entreprises spécialisées uniquement en services de cybersécurité et enfin des développeurs de technologies de cybersécurité. Dû au fait que leurs expertises ne sont pas les mêmes, les services de sécurité qu'ils offrent sont très souvent différents et il peut être mêlant de faire un choix pour un non-initié. Certains vont offrir des services de sécurité de base appelés SOC, tandis que d'autres vont offrir des services plus avancés tels que le MDR.

Mais quelle est la meilleure option? Choisir du SOC ou du MDR? Travailler avec un fournisseur MDR qui dispose d'une technologie ou non?

Le SOC (Security Operation Center) externe

Le premier type de service de supervision que l'on retrouve sur le marché, mais aussi le plus ancien, est le SOC externe. Un SOC externe s'appuie principalement sur un outil de gestion de logs et d'événements de sécurité (SIEM) pour surveiller la sécurité des réseaux de ses clients. Via le SIEM, les analystes en sécurité créent des scénarios de surveillance de sécurité (use cases) et les surveillent afin d'identifier des cas similaires qui seront pris en charge et traités. Des exemples de use cases sont :

- Création de comptes administrateurs dans le réseau
- Tentatives de connexion multiples échouées venant de la même source
- Connexion via un compte administrateur en dehors des heures de travail

La supervision de la sécurité via un SIEM est passive et peu efficace au regard de l'évolution des cybermenaces. En effet, chaque jour, de nouvelles attaques apparaissent et il n'est pas réaliste pour une équipe de SOC d'ajouter constamment autant de nouveaux use cases. Au final, plusieurs attaques passent en dessous des radars de l'équipe du SOC, ce qui augmente vos risques de piratage.

Au regard de la faible capacité des SIEM à faire face aux cyberattaques actuelles, nous ne recommandons pas ce service aux entreprises qui souhaitent externaliser la sécurité de leur réseau.

Le MDR comme solution pour pallier les insuffisances du SOC

Pour pallier les limitations de la supervision de la sécurité via un SOC est apparu le service de Détection et Réponse Gérée (DRG ou MDR en anglais). Ce service fournit aux organisations des services de détection de cybermenaces et de leur élimination une fois qu'elles sont découvertes. Le service DRG/MDR combine à la fois technologie et expertise humaine afin d'assurer la défense des clients. Ainsi, les analystes de l'équipe de MDR prennent en charge les moindres mouvements suspects identifiés dans le réseau et les analysent en profondeur afin d'éviter qu'ils se transforment en problème. Avec un service MDR, vous avez de véritables chasseurs de cybermenaces qui s'allient à la technologie pour gérer votre sécurité de façon proactive.

Profil des compagnies qui offrent le service MDR

Il existe deux (2) types de compagnies qui offrent les services MDR. Nous allons comparer ces deux offres.

MDR offert par des compagnies qui ne développent pas de technologie

Ce service MDR est offert par les compagnies d'impartition TI ou des compagnies spécialisées en cybersécurité, dont le développement de produits de sécurité n'est pas le cœur de métier.

Bien que ces entreprises puissent développer une grande expertise en MDR, elles sont freinées par les contraintes liées au fait qu'elles n'ont aucun contrôle sur l'évolution et l'efficacité des technologies de sécurité qu'elles utilisent pour offrir leur service. Elles ne peuvent pas être proactives, ce qui est souvent un frein à la gestion efficace de la sécurité.

Dans un cas constaté, un fournisseur de service MDR a identifié un outil malicieux non détecté par la solution qu'elle utilise et l'a signalé au fournisseur de la solution. Ce dernier a mis environ un mois avant de réagir. Pendant ce temps, le réseau surveillé était à risque.

Malgré leur bonne volonté, il peut arriver que ces fournisseurs ne soient pas en mesure de vous offrir une sécurité optimale.

Quant aux compagnies d'impartition TI qui offrent le service MDR ou SOC, elles font souvent face au dilemme de remonter à leurs clients les vulnérabilités et failles de sécurité des réseaux qu'ils ont eux-mêmes mise en place. Cela les met souvent dans une position inconfortable. Pour éviter tout conflit d'intérêts, il est approprié de séparer les tâches et de ne pas confier la supervision de la sécurité de votre réseau à son impartition TI.

MDR offert par des compagnies qui ont développé leur propre technologie de sécurité

Ce service MDR est offert par les compagnies dont le développement de produits de sécurité est le cœur de leur métier. Par exemple : des éditeurs de systèmes de détection d'intrusion ou d'antivirus.

Ces fournisseurs ont plus de flexibilité et peuvent rapidement créer des signatures ou des profils de détection lorsqu'une attaque ou un outil malicieux inconnu est identifié dans votre réseau.

Dû au fait qu'elles ont l'expertise requise pour développer des technologies de sécurité, ces compagnies comprennent mieux le comportement des pirates et sont constamment à l'affût des nouvelles techniques de piratage pour mieux vous protéger. À titre d'exemple, les analystes MDR de ces entreprises sont capables d'analyser un nouveau virus, créer sa signature, puis l'injecter dans leur technologie, ce qui n'est pas le cas des compagnies qui offrent un service MDR sans avoir leur propre technologie.

Conclusion

En conclusion, le service SOC classique est peu efficace pour faire face à l'évolution actuelle des cybermenaces et nous ne le recommandons pas. La meilleure chose à faire est de choisir un fournisseur de service MDR ayant développé sa propre technologie, car ses analystes ont une expertise beaucoup plus avancée que ceux des fournisseurs qui n'ont pas d'expertise en développement de technologie de sécurité.

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.