EDR : pourquoi l'externalisation gagne du terrain

L'EDR s'impose pour protéger les postes de travail et les serveurs contre les attaques et les ransomware. Pour les exploiter, les entreprises, en particulier celles de taille moyenne, se tournent de plus en plus vers un spécialiste des services managés.

Le marché des logiciels d'EDR (Endpoint Detection and Response) a littéralement explosé ces dernières années. Avec un taux de croissance annuel de 22,3 %, il va passer de 1,41 milliard $ en 2019 à près de 7 milliards en 2027 selon le cabinet Reports & Data.

Beaucoup de grandes entreprises se sont équipées et ont connecté cette nouvelle source de données à leur SOC. Mais placer un expert cyber devant une console en 24/7 est un luxe que bien peu d'entreprises moyennes – ETI et PME- peuvent se permettre. De nombreux DSI cherchent maintenant à externaliser cette charge.

Le marché des EDR managés ou Managed Detection and Response (MDR) se répartit essentiellement entre les MSSP (Managed Security Service Provider) qui distribuent les EDR et en assurent l'exploitation pour leurs clients et certains éditeurs qui fournissent eux-mêmes des services à haute valeur ajoutée au-dessus de leur stack logiciel.

C'est le cas de l'éditeur finlandais F-Secure qui, avec son offre *EDR Countercept* propose le service *Rapid Detection & Response*, un SOC qui analyse les menaces remontées par son EDR chez ses clients, filtre les alertes et déclenche l'alerte si l'incident est sérieux.

Benoît Meulin, expert cybersécurité chez F-Secure France met clairement l'accent sur cet élément humain comme différenciant clé de l'offre EDR : « Si elle comporte de l'intelligence artificielle, de l'UBA et d'autres technologies de pointe, c'est pour permettre à nos Threat Hunters de réaliser leur mission dans les meilleures conditions pour rendre le meilleur service. Ils ont la mentalité et les compétences des attaquants, ils savent ainsi « sentir » le prochain mouvement de l'adversaire et ainsi mieux s'en défendre. C'est vraiment l'alliance de la technologie et de la compétence humaine qui rend Countercept si efficace. »

Un mix de technologies et de compétences humaines

L'éditeur affirme sécuriser plusieurs dizaines de millions de endpoints avec ses différentes solutions, dont 50 000 bénéficient de la surveillance active de *Countercept*.

Chez Kudelsky Security, la part de l'offre managée *Managed Detection & Response* (MDR) est considérable, car seulement 5 % des clients de l'éditeur optent pour l'EDR seul.
Celui-ci compte 220 clients pour l'offre MDR, soit environ 400 000 postes protégés. « Notre approche vis-à-vis des services de sécurité managés a toujours été de se focaliser sur l'objectif de protection et non sur les technologies, confie Philippe Borloz, vice-président Sales & General Manager EMEA de Kudelski Security. Cela nous a amenés à définir une offre de service qui est

attractive tant pour des petites entreprises de moins de 100 personnes que pour des groupes internationaux de plus de 100 000 employés. Notre offre de service nous permet de cibler la plupart des secteurs d'activité du marché. »

Le leader suisse de la cybersécurité estime qu'en appréhendant les objectifs de sécurité de ses clients au sens large et en proposant des outils sur mesure, les services qu'il délivre peuvent être mis en œuvre et adaptés à de multiples environnements.

Les éditeurs cherchent à développer rapidement leur écosystème de MSSP, notamment pour conquérir le midmarket. C'est notamment le cas de Bitdefender qui veut surfer sur la montée en puissance des MSSP.

« Dans l'univers du cloud, près de 20 % des acteurs proposent aujourd'hui des activités de MSSP. Ils n'étaient que 14 % il y a 18 mois », explique Magali Mauduit, Cloud & MSP Business Development Manager pour l'Europe du Sud.

Pour l'éditeur de l'EDR *Gravityzone*, s'appuyer sur les MSSP est un moyen de toucher les PME/TPE : « À l'heure actuelle, environ 80 % des attaques informatiques sont dirigées contre les TPE et PME. Et ce pour une raison simple : elles manquent de ressources pour faire face aux défis de la cybersécurité. C'est pourquoi le modèle MSSP devient de plus en plus pertinent. »

Le service public est aussi concerné

L'éditeur a mis en place une équipe dédiée « Cloud & MSP Team » qui se compose de commerciaux, d'experts techniques et marketing, dédiée aux offres cloud et MSP de Bitdefender. Et annonce avoir constitué un écosystème de plus de 100 MSP/MSSP à qui il propose son offre de SOC pour les aider à monter une offre managée.

Éditeur pionnier des EDR, Cybereason mise lui aussi sur les partenaires MSSP afin d'accéder aux marchés qu'il n'adresse pas encore. « Nos MSSP ciblent le secteur public qui manque réellement de ressources de sécurité, le midmarket avec des offres packagées et les grands comptes souhaitant confier le pilotage de leur EDR à un expert. Ils s'adressent à la fois à une cible nationale et internationale », explique Guillaume Leseigneur, directeur régional, ventes aux entreprises de Cybereason.

En France, Cybereason s'appuie sur quatre grands partenaires MSSP et protège 150 clients pour 400 000 assets.
L'éditeur privilégie les partenaires offrant un SOC et parmi eux, figure Advens.
Le spécialiste compte 30 clients à son offre d'EDR managé, avec de 10 000 à 150 000 agents par client.

Tristan Savalle, responsable stratégie et produit SOC chez Advens, explique sa méthode qui le différencie de celle d'un éditeur : « Notre démarche est d'adapter l'outil au contexte du client : partant du risque, nous ajustons l'utilisation de l'outil au plan de surveillance (et pas l'inverse). Notre approche service by design' vise à apporter une capacité de détection et de réaction, et non un outil. Pour nous, la mise en œuvre d'un EDR n'est qu'une première étape vers l'instauration d'un SOC couvrant un périmètre plus large (Cloud, App, AD, etc.) », conclut-il.

Lire aussi : Interview de Paul Lemesle, CISO du groupe Lactalis, sur son choix de déployer un EDR managé