EDR ou MDR : les critères pour choisir

Quentin Perceval, Manager Cybersécurité chez Wavestone

« Le choix d'un EDR ou d'une offre MDR se fait au cas par cas. Il faut intégrer la nationalité du fournisseur, dont beaucoup sont américains ou israéliens. Ces solutions sont coûteuses et facturées au nombre de postes. C'est un budget très significatif lorsqu'on veut sécuriser un parc de 50 à 70 000 postes. En outre, tous les EDR n'offrent pas la même couverture. Si tous les postes sont de type Windows cela ne pose pas de problème, mais s'il faut protéger des postes MacOS ou de différentes distributions Linux, tous les éditeurs ne les supportent pas.

Enfin, un autre point d'attention doit être accordé au volet réaction. Quand on sait qu'une attaque NotPetya est capable de chiffrer des postes en 1 à 2 heures, il est extrêmement important d'être en capacité de réagir dès qu'une attaque est détectée. Les équipes de production sont très réticentes à confier cette capacité de réaction à un tiers, l'entreprise doit se structurer pour une réponse rapide ou accorder plus de droits à son prestataire pour le faire à sa place. »

Thierry Gourdin, Kaspersky Lab France & Afrique du Nord

« L'effervescence du marché français pour le MDR s'explique de plusieurs façons. Il y a certainement eu un effet Covid avec des entreprises confrontées à un télétravail massif et qui ont cherché des solutions pour mieux sécuriser tous ces postes distants.

L'autre facteur est plus structurel : les EDR sont des outils complexes et si l'IA permet des automatisations, cette complexité va aller encore en s'accroissant avec l'arrivée des XDR. Ceux-ci vont multiplier les sources de données analysées et le pas à franchir est important pour les entreprises.

Certains de nos clients ont une équipe SOC, mais elles optent pour une offre MDR afin de faire un premier tri des incidents.

La problématique de l'EDR en général, c'est de générer énormément d'alertes. S'appuyer sur une

offre MDR, c’est pouvoir laisser aux équipes Kaspersky le traitement de toutes ces alertes mineures pour se concentrer sur les alertes réellement critiques et la réponse à incident. Soit nous adressons la totalité des incidents pour le compte de PME ou des partenaires qui n’ont pas de compétences en cybersécurité, soit nous nous plaçons en premier niveau pour les entreprises qui disposent d’un SOC. »