Détection des incidents de sécurité : pourquoi faudrait-il choisir entre vision systèmes et écoute réseau ?

Charles BLANC ROLIN
RSSI
Centre hospitalier de Moulins-Yzeure

Lors de la dernière édition des RIAMS, ce prestigieux évènement imaginé et conçu en 2005 par Michel Van Den Berghe, deux questions soulevées par des RSSI de grands groupes français m'ont interpellé sur la compréhension que nous pouvons avoir de certains outils, cachés derrière des acronymes dont on perd parfois la définition et des propagandes commerciales parfois malhabiles.
Lors d'un retour d'expérience sur le thème de la détection réseau, le cofondateur d'une entreprise française éditrice de plusieurs solutions de sécurité, dont une sonde de détection réseau qualifiée par l'ANSSI, s'est vu interpellé sur l'intérêt d'une telle solution :

« Je dispose déjà d'un EDR, que pourrait bien m'apporter de plus votre solution ? »

D'un point de vue technique, ce sont des solutions totalement différentes qui ne devraient pas être mises en concurrence selon moi. Elles apportent toutes les deux des informations précieuses et complémentaires. Faire le choix entre EDR et NDR par exemple, reviendrait à choisir entre l'ouïe et la vue. Dans la mesure du possible évidemment, il est tout de même plus confortable de disposer des deux. Comble du luxe, pour améliorer notre compréhension de la menace, nous pourrions les interconnecter et rapprocher les informations que ces deux solutions renvoient dans un SIEM, que l'on pourrait comparer au cerveau pour pousser l'allégorie un peu plus loin.

Même si les solutions évoquées ne s'arrêtent pas à la détection et la collecte d'informations, nous nous intéresserons ici, uniquement à cette partie.

Là où le rôle de l'EDR va être de détecter des actions suspectes dans logs systèmes et applicatifs remontés par l'agent installé sur les postes et serveurs, des processus malicieux en mémoire, des modifications du système, des changements de permissions, etc.

Celui de l'IDS, et désormais du NDR si nous souhaitons aller un peu plus loin, est de détecter des comportements anormaux ou suspects sur le réseau, tels que des connexions vers un serveur C2, des exploitations de vulnérabilités, des déplacements latéraux, etc.

Évidemment certaines informations peuvent se rejoindre, et c'est tout l'intérêt pour permettre une détection plus rapide et plus fiable d'un incident, dans le but de tenter de le contenir. De la même manière, dans une phase d'investigation, disposer d'informations en lien avec ce qui a pu se passer sur une machine potentiellement compromise et les corréler avec celles relatives à ce qui s'est passé sur le réseau, pourra permettre de mieux comprendre la chronologie des faits, et les chemins empruntés par l'attaquant.

Si les informations collectées sur les machines (logs, processus en mémoire, mft…) permettent

généralement d'apporter plus de clarté sur les actions réalisées par le ou les attaquant(s), et qu'il ne faut donc surtout pas s'en dispenser lorsque nous pouvons les avoir, je vois deux principaux avantages à la détection réseau.
Tout d'abord, il est beaucoup plus difficile pour un attaquant de supprimer les traces qu'il va laisser, ou «faire mentir» le réseau. Je n'ai jamais vu, ce qui ne veut pas dire que cela ne s'est jamais produit, de rapports sur une compromission dans laquelle l'attaquant aurait volontairement généré du bruit sur le réseau pour tenter de dissimuler ses traces, car cela représenterait un risque supplémentaire de détection pour lui. Pour supprimer ses traces, il faudrait qu'il trouve la ou les sondes IDS et /ou la solution NDR, le collecteur de logs et/ou le SIEM et qu'il arrive à les compromettre, mission quasiment impossible.
Deuxième avantage, l'écoute réseau est possible sans avoir à déployer d'agent, et lorsque l'on se trouve sur des réseaux industriels, techniques ou biomédicaux, dans lesquels il n'est pas possible de déployer un agent sur les dispositifs, le réseau reste notre meilleur allié pour nous remonter des informations.

La seconde question bonus posée lors du RETEX était :

« Aujourd'hui, la majorité des flux est chiffrée, si votre solution ne les déchiffre pas, elle ne verra rien passer ? »

Là encore, c'est à mon sens une fausse idée reçue.
Pour commencer, tous les flux ne sont pas chiffrés, et notamment dans le cadre de certaines attaques. Ensuite, l'écoute des flux chiffrés via SSL/TLS permet malgré tout de remonter des informations qui peuvent s'avérer intéressantes, telles que le nom d'hôte de la machine contactée, l'ensemble des informations relatives au certificat présenté par le serveur, les empreintes JA3 et JA3S pouvant permettre d'identifier de manière plus ou moins précise clients et serveurs. Clients pouvant être reconnus comme malveillants. On l'oublie également, mais une simple connexion vers une adresse IP, lorsqu'elle est connue comme fréquemment ou fraîchement utilisée dans le cadre d'attaques, est une information importante. Tout comme une requête DNS.

Il sera également possible de détecter des anomalies sur les protocoles, des attaques connues, des déplacements latéraux... suivant où est placée la sonde.

Pour conclure, si j'ai le choix, je préfère ne pas avoir à choisir entre les deux solutions et les utiliser ensemble.