# XDR : la naissance d'un véritable écosystème de renseignement cyber dans l'entreprise

Lorsque le cabinet Gartner décrivait le XDR (eXtended Detection & Response) en mars 2020, il faisait référence à des solutions fermées, contrôlées par un seul éditeur et hébergées dans le Cloud. À peine quelques mois plus tard, en septembre, la définition s'était déjà élargie pour intégrer des stratégies XDR associant des outils dits « best of breed », c'est-à-dire issus d'éditeurs différents sélectionnés pour leur efficacité dans un rôle précis.

Cela prouve deux choses : que la notion de XDR est une tendance forte en rapide évolution, et que — comme l'on pouvait s'y attendre — dans la vraie vie les entreprises ont rarement un seul fournisseur pour tous leurs besoins de sécurité. Et donc qu'une approche centrée sur un seul acteur — a fortiori purement dans le Cloud — n'est tout simplement pas réaliste.

Mais après tout, comment pourrait-il en être autrement ? L'approche XDR consiste à fédérer de nombreuses sources d'informations afin de dessiner une vision claire et actionnable des menaces auxquelles fait face l'entreprise, dans le but d'y répondre plus rapidement et plus efficacement.
Or, ces menaces peuvent provenir aussi bien de l'interne que de l'externe, et les signaux qui permettent de les qualifier également (entre la fusion de flux de Threat Intelligence commerciaux et la collecte d'événements sur les machines et les équipements du SI interne et ceux du SI dans le Cloud, tels Azure AD ou 0365).

Finalement, lorsque l'on parle de XDR, l'on parle donc surtout de créer un véritable écosystème de renseignement cyber au sein de l'entreprise, de la collecte à l'analyse, et cela ne peut être qu'un projet ouvert, capable de travailler avec toutes les sources d'information disponibles où qu'elles se trouvent, et adapté au contexte de l'entreprise (avec, donc, une mémoire historique). Nous sommes ainsi bien loin d'une approche intégrée, fermée et liée à un seul fournisseur !

## Un projet XDR, à petits pas

Évidemment, cela pose la question du démarrage d'une telle aventure. Par quel bout prendre un projet aussi transverse ? Peut-être d'abord par celui du poste de travail. L'EDR (Endpoint Detection & Response) est un premier bon capteur d'information, car il est particulièrement bien distribué au sein de l'entreprise (souvent sur la totalité des postes de travail et une majorité de serveurs).

Mais attention, si pour beaucoup l'EDR sera la première et la dernière étape, ça serait passer à côté des gains à terme d'un vrai projet de XDR. Car la vision serait alors limitée à ce qui se passe sur les postes de travail, sans aucune vision sur le réseau, notamment. Et puis, surtout, la tour de contrôle de l'ensemble serait alors limitée à la console propriétaire de l'EDR, qui ne permet ni de fusionner d'autres sources, ni de réellement créer et exploiter une « mémoire » des menaces propre à l'entreprise (pas de capitalisation de l'information).

Quelle est alors la bonne formule ? Facile : XDR = EDR + NDR + CDR (Cloud Detection & Response) + tous les autres outils de sécurité + un référentiel central qui permettra de capitaliser toute cette précieuse information dans le temps !

Reprenons donc : après avoir déployé et bien pris en main l'EDR, la visibilité est retrouvée sur les postes de travail. Toutefois, le trafic réseau demeure dans l'ombre. C'est là le rôle du NDR, qui va s'intéresser aux échanges réseau. La visibilité est alors étendue et il devient désormais possible de pivoter efficacement (mais manuellement…) d'un indicateur local (par exemple un malware sur le poste de travail) à un indicateur réseau (un trafic suspect) et inversement.

On se rapproche du XDR, mais ce n'est pas encore tout à fait ça. Il manque notamment de la visibilité sur la portion du SI hébergée dans le Cloud : les applications SaaS, bien sûr, mais également les différents services IaaS ou PaaS sur lesquels l'entreprise peut bâtir ses propres applications métiers. C'est évidemment nécessaire afin de ne pas laisser d'angle mort qu'un attaquant pourrait exploiter (par exemple en s'arrogeant des droits depuis un Azure AD, en exploitant une synchronisation ADFS ou en ajoutant des règles de redirections illégitimes sur un Outlook 365).

Mais en même temps, plus on intègre des sources, plus les opportunités de pivoter d'un élément issu d'une source à l'autre augmentent, plus la connaissance du contexte local s'enrichit, et il serait dommage de ne pas exploiter ces connaissances.

## *DR… et tout le reste !

Alors, c'est bon ? Après avoir acquis, déployé et ajusté un EDR, un NDR et un CDR, on peut raisonnablement estimer être entré de plain-pied dans le nouveau monde du XDR ?

Pas tout à fait, même si, évidemment, le niveau de sécurité s'est déjà considérablement amélioré.

Il restera pourtant encore à intégrer tout le spécifique, toutes ces applications susceptibles de générer de l'information capable d'éclairer sur l'activité ou le contexte local. Bien sûr, il s'agit là du volet « détection » plutôt que « réponse » (celle-ci se concentrant sur les capacités de blocage ou d'isolation des EDR/NDR/CDR). Mais ces sources « maison » sont essentielles pour apporter au projet de XDR une coloration locale, une connaissance fine des « patterns » métiers. Cette télémétrie issue des systèmes internes est souvent l'une des meilleures sources de détection, mais aussi la plus souvent ignorée (les journaux d'erreurs des applications propriétaires, par exemple…).

Et enfin, il y a aussi les sources externes. Tous ces flux de Threat Intelligence certes pas contextualisées, mais indispensables pour évaluer la réputation d'une adresse IP ou d'un nom de domaine observé par un élément de sécurité interne.

## Et maintenant, on fait quoi de tout ça ?

On y est presque. Il manque toutefois l'ingrédient final, qui permettra de libérer le potentiel de cet assortiment de solutions. Une plateforme centrale, dont l'objectif est non seulement l'intégration des éléments remontés par ces sources multiples, mais aussi de faciliter leur exploitation par

l'équipe sécurité afin de modéliser les menaces et identifier celles en cours d'exécution avant qu'il ne soit trop tard.

Aucune console propriétaire ne saura relier les points entre la signature d'un code malveillant identifié sur un poste de travail, le trafic réseau de ce dernier, ses tentatives d'accès bloquées à une application propriétaire et son historique de connexion à une plateforme à Outlook 365. Aucune plateforme propriétaire ne permettra à un analyste sécurité interne d'investiguer des alertes prioritaires selon le contexte propre de l'entreprise, en s'appuyant sur un passif de connaissances capitalisées depuis plusieurs années.

En définitive, la capacité d'intégration est au cœur d'un projet de XDR. Et même si la recherche de « quick wins » fait qu'il est souvent préférable de démarrer par un projet EDR, il sera important de garder à l'esprit tout au long du projet que l'objectif final est bien de créer du lien à travers une capacité de renseignement cyber intégrée et l'usage de standards reconnus tels Stix ou Taxii par exemple pour l'échange d'information et MITRE ATT&CK® pour la classification. Avec pour objectif de permettre aux analystes de l'équipe sécurité de pivoter dans toutes les directions (d'une détection locale à un évènement réseau à un incident Cloud et inversement), et capitaliser au fil des années d'existence du programme.

Ainsi, dans une vision d'un XDR de plus en plus dominée par l'intégration d'outils « best of breed » et internes, il n'y a aucune raison pour que ce dernier élément, cette plateforme centrale qui sera au cœur des investigations de l'équipe sécurité, ne le soit pas également.