Livre blanc

Au-delà de l'EDR : analyser et corréler en natif les indicateurs de sécurité des Endpoints, du réseau, de l'email et du Cloud.

XDR : un levier pour une détection et une réponse plus efficaces et pertinentes face aux menaces

Par Dave Gruber, ESG Senior Analyst

Août 2019

Ce livre blanc a été commandité par Trend Micro et diffusé sous licence ESG.

Contents

Détecter et répondre aux menaces est devenu un défi majeur

Avec des menaces toujours plus nombreuses, une surface d'attaque en expansion et des attaques de plus en plus sophistiquées, la détection et la réponse aux menaces sont devenues un challenge pour les équipes de sécurité. Alors que les entreprises, pour la plupart d'entre elles, ont déployé de multiples solutions de sécurité, les menaces sophistiquées échappent régulièrement à la détection car les données remontées par ces solutions ne sont pas collectées et analysées de manière transversale.

Les entreprises ont tenté de pallier cette problématique en utilisant le SIEM comme un outil d'agrégation de données. L'étude d'ESG nous révèle que 88% des entreprises sont déjà en cours de déploiement d'un SIEM, ou l'ont planifié.[1] En tout état de cause, les SIEM traditionnels sont onéreux à installer et à maintenir, avec souvent un investissement initial lourd. Les récentes annonces de Google/Chronicle Backstory et de Microsoft Sentinel, offrant des outils de SIEM Cloud-native, encouragent le besoin de consolider et d'analyser des ensembles volumineux de données et d'indicateurs provenant d'une multitude de systèmes de sécurité protégeant les Endpoints, le réseau, l'email et le Cloud.

Même si ces SIEM Cloud font économiser les coûts élevés de stockage d'un SIEM classique, il leur manque les éléments contextuels leur permettant d'accélérer les délais de détection et de réponse. Les systèmes SIEM ne proposent pas de capacités d'analyse ou de corrélation basées sur le ML (Machine Learning) et ces tâches incombent à des analystes SOC déjà débordés.

Pour pallier ces carences, les entreprises se sont tournées vers des systèmes d'Endpoint Detection & Response (EDR). Ces puissants outils agrègent et analysent les données d'activité des Endpoints, puis utilisent ces informations de veille pour détecter les attaques en cours.

Les analystes en sécurité font appel à l'EDR au quotidien pour traquer des menaces présentes mais non identifiées. Cependant, ces outils EDR, seuls, ne sont pas suffisants pour la plupart des équipes de sécurité. Bon nombre d'entreprises tirent déjà parti d'APIs pour exporter les données hors des systèmes EDR et les corréler à d'autres données de sécurité, obtenant ainsi des informations complémentaires sur les causes profondes et l'impact des attaques. Quand les indicateurs sont corrélés sur l'ensemble du parc des outils de sécurité, les détections pertinentes et rapides peuvent être plus facilement automatisées, pour stopper les attaques en cours et aider les analystes à mieux comprendre le comportement des assaillants. L'utilisation conjointe de données associées aux Endpoints, au réseau, au Cloud et à l'email donne une vision claire des stratégies d'attaques sophistiquées.

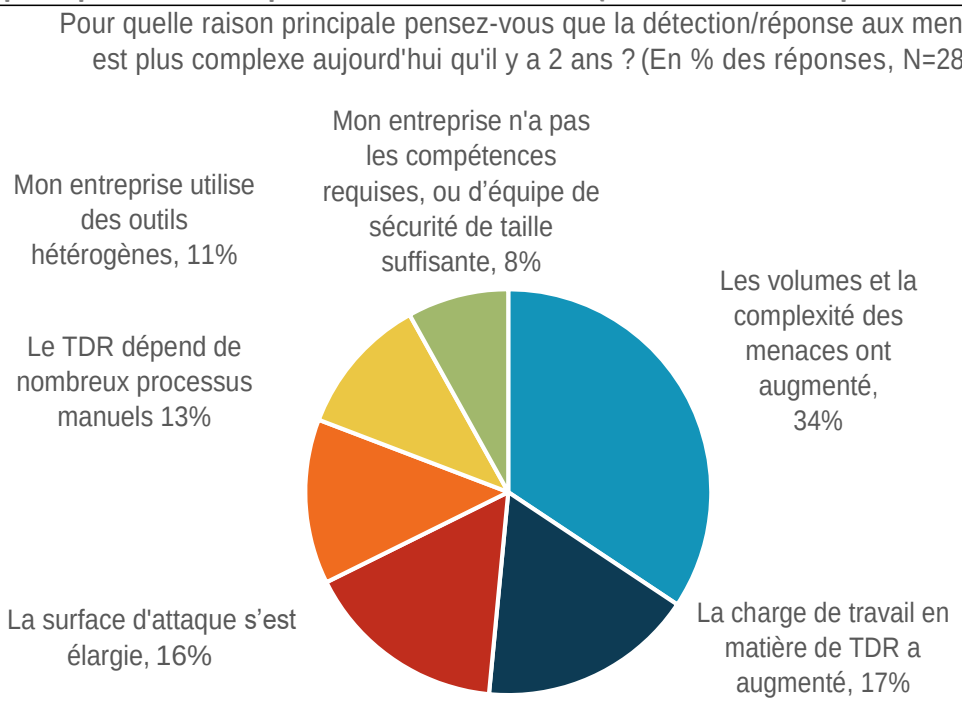
La technologie EDR, à elle seule, ne permet pas aux professionnels de la sécurité de détecter, d'analyser et de répondre aux attaques éclair des assaillants actuels. Une approche plus large s'impose donc.

Un état des lieux de la détection et de la réponse aux menaces

Fin 2018, ESG a mené une étude pour dresser un état des lieux en matière de détection et de réponse aux menaces (TDR - Threat Detection and Response). 45 % des interrogés déclarent que le TDR est bien plus complexe qu'il y a 2 ans, et pour 31 %, qu'il est sensiblement plus complexe. Les personnes interrogées citent le volume croissant et/ou la plus grande sophistication des menaces (34%) et l'élargissement du spectre des attaques (16 %) en tant que causes de cette complexité globale accrue (cf. graphique 1). 82 % des répondants conviennent que l'amélioration de la détection et de la réponse aux menaces constitue une priorité élevée pour leur entreprise.

[1] Source : ESG Master Survey Results, *The Threat Detection and Response Landscape*, Avril 2019. Toutes les références et les graphiques de ce livre blanc sont issus de cette étude.

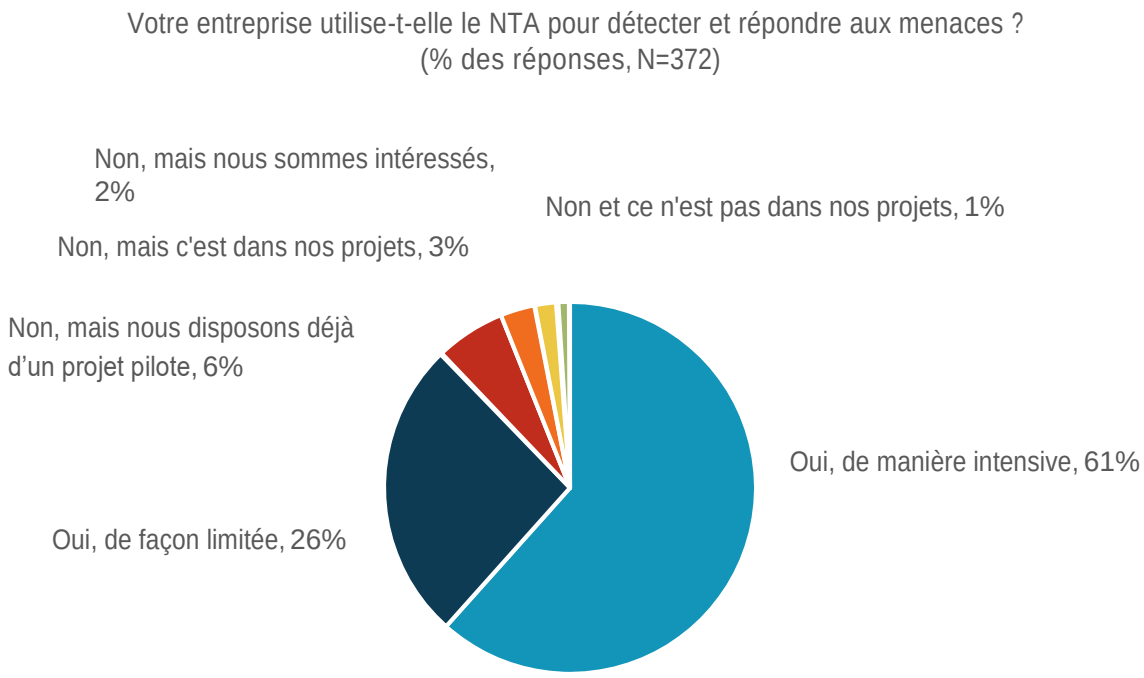
Graphique 1. Raison principale de la complexité des activités TDR (détection et de réponse aux menaces)



Source: Enterprise Strategy Group

Lors d'une attaque, les assaillants progressent latéralement au sein du réseau dans l'optique d'obtenir des privilèges d'accès plus élevés. Connaître leur point d'entrée, le schéma de déplacement et de découverte, et les comportements spécifiques, exige d'agréger les indicateurs provenant de multiples vecteurs de menaces. Les outils d'analyse du trafic réseau (NTA - Network Traffic Analysis) aident les analystes dans la compréhension des mouvements latéraux, mais, sans corrélation avec l'activité des Endpoints, il est difficile d'avoir une vision complète de l'attaque.

Graphique 2. La majorité des entreprises déclare utiliser le NTA pour détecter et répondre aux menaces



Source: Enterprise Strategy Group

De nombreuses entreprises post-traitent les données issues de l'EDR et du NTA pour reconstituer une attaque. Pourtant, même avec des solutions EDR, les équipes de sécurité ont du mal à suivre. Les études d'ESG montrent que 66 % des personnes interrogées estiment que l'efficacité de leur capacité TDR est limitée parce qu'elle repose sur de multiples outils distincts et autonomes. Ainsi, si les équipes disposent d'outils en place, ils ne les exploitent pas encore à leur pleine capacité.

Défi : analyser et agréger les données s'avère coûteux et chronophage

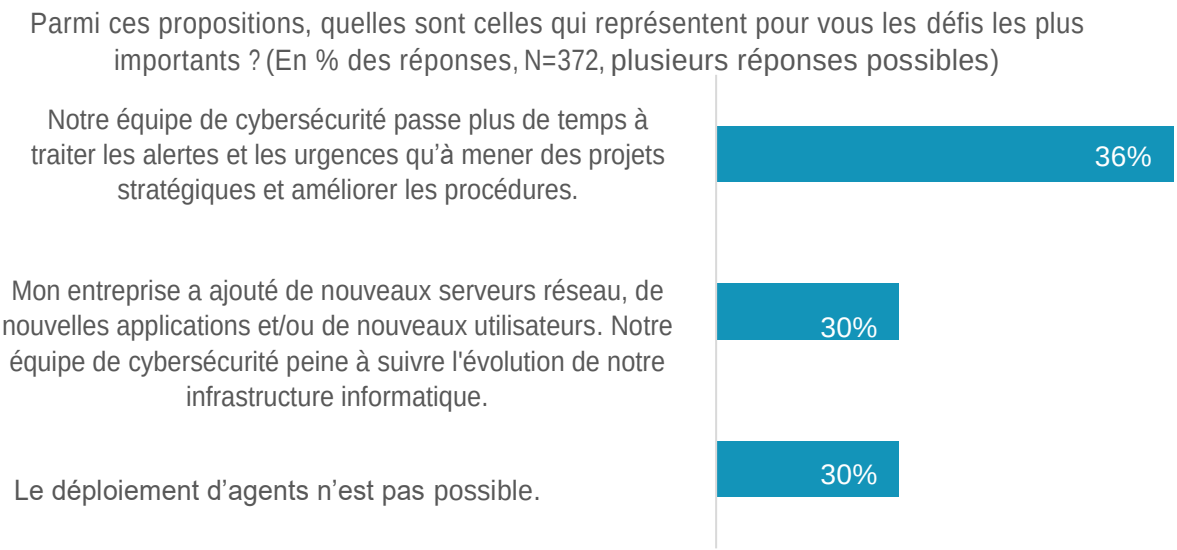
Agréger des indicateurs en provenance de sources hétérogènes n'est pas seulement une gageure, mais tout simplement impossible dans bien des cas. Les multiples outils stockent et indexent les données de manière différente, forçant les équipes locales à faire cavalier seul dans leur effort d'intégration. Constituer et maintenir des bases de données sécuritaires est également onéreux et chronophage. Faute de compétences et de budget, la plupart des entreprises ne sont pas outillées pour appliquer les technologies IA/ML sur des référentiels de données de sécurité conçus sur mesure.

Même lorsque les données sont agrégées, elles sont rarement réintégrées dans le workflow quotidien des analystes en sécurité. La plupart des solutions ne permettent donc pas de tirer parti des enseignements du passé pour détecter les attaques à venir. Les données sont souvent isolées dans des systèmes autonomes et doivent être corrélées manuellement. Une vision globale sur les attaques sophistiquées fait aussi défaut à ces outils, forçant les analystes à rechercher et analyser les données manuellement.

Défi : les équipes de sécurité peinent à suivre

Quand on pose la question aux analystes en sécurité pour savoir quel sont leurs plus grands défis en termes de TDR, l'étude ESG révèle qu'ils sont tellement débordés par le quotidien qu'ils n'ont pas le temps d'être proactifs en termes de stratégie, de processus et de mise en place d'infrastructures éprouvées (Cf. graphique 3). L'étude montre également que les entreprises sont confrontées à un flux continu de nouveaux serveurs, applications et utilisateurs, et qu'elles ne disposent pas des moyens de déployer des agents logiciels de sécurité sur tous les dispositifs.

Graphique 3 : les trois principaux défis du TDR : la prise en charge des incidents, l'expansion de la surface d'attaque et l'absence de visibilité en temps réel.



Source: Enterprise Strategy Group

Face à la pénurie de compétences en cybersécurité, il est prioritaire de se pencher sur le volume des alertes et sur les processus d'investigation et de remédiation, afin de répondre aux défis actuels.

Défi : les solutions EDR ne couvrent pas tout le spectre des indicateurs nécessaires

Si l'EDR a ouvert les yeux à bon nombre d'entreprises, il manque toujours une vision plus globale, plus large, pour agir en temps réel. Les solutions EDR peuvent parfois détecter des mouvements internes, mais l'absence d'indicateurs issus du réseau, du Cloud et de l'email ne permet pas de détecter rapidement les menaces et n'offre aucune visibilité sur le véritable comportement de l'assaillant.

Les solutions EDR offrent de puissantes capacités de détection et de réponse. Notamment la possibilité de comparer en permanence les caractéristiques d'une activité identifiée avec des informations de veille, de visualiser une attaque, de réagir en mettant à l'arrêt ou en interdisant des processus informatiques, de restreindre l'accès à des domaines et adresses IP spécifiques et de disposer de données d'investigation post-incident. Mais si les fonctions des solutions EDR modernes sont précieuses, elles nécessitent souvent une corrélation avec d'autres données de sécurité pour créer une vue complète de l'attaque.

Pour les entreprises ayant déjà déployé des solutions de détection et de réponse pour leurs Endpoints, les indicateurs de ces Endpoints manquent d'exhaustivité et ne démasquent donc potentiellement pas des comportements agressifs.

De quoi avons-nous besoin ?

La détection et la réponse aux menaces forment le cœur du métier de l'analyste en sécurité. La capacité à analyser rapidement et continuellement les événements, les comportements et les alertes permet d'optimiser le TDR. Lorsque les analystes peuvent identifier les incidents sur différents vecteurs d'attaque et qu'ils disposent d'une image complète des Endpoints, du réseau, de la messagerie et du Cloud, ils peuvent neutraliser les menaces plus rapidement, y répondre plus vite et, en fin de compte, déjouer les agresseurs avant tout dommage majeur.

La capacité à analyser rapidement et continuellement les événements, les comportements et les alertes permet d'optimiser le TDR.

Il faut davantage d'indicateurs provenant des réseaux, de l'email et du Cloud, mais aussi procéder à des analyses basées sur l'IA/ML sur ce vaste ensemble de données, pour ainsi détecter et hiérarchiser les menaces les plus importantes. En combinant l'analyse du trafic réseau et les indicateurs des Endpoints, les assaillants tentant de se mouvoir au sein d'un réseau sont repérés en amont. Cet ensemble de données intégrées aide également les analystes à déterminer plus rapidement l'origine d'une attaque.

Avec un recours important au phishing pour détourner les identifiants et 94 % des logiciels malveillants issus de l'email[2], la corrélation des menaces véhiculées par email, l'exécution de logiciels malveillants sur des Endpoints et les mouvements internes sur le réseau, fournissent des données contextuelles pour comprendre les stratégies d'attaque.

Une fois les indicateurs agrégés, corrélés et analysés sur un périmètre large, ce processus continu d'analyse doit être étroitement intégré au workflow de chaque analyste en sécurité.

Trend Micro XDR

Trend Micro XDR, proposé en tant que plate-forme ou fourni en tant que service managé, rassemble et analyse les indicateurs provenant des Endpoints, du réseau, de l'email et du Cloud, en utilisant le Machine Learning et un traitement analytique orienté sécurité pour corréler les événements. Ce niveau renforcé d'automatisation assure un gain de temps majeur pour les analystes devant trier les alertes et mener leurs recherches, tout en automatisant/accélérant les processus de détection et de réponse.

[2] Source : 2019 Verizon Data Breach Report.

Tableau 1. Des indicateurs exhaustifs pour des perspectives pertinentes et des résultats plus rapides.

Endpoint	Réseau	Email	Cloud
Processus	Connexions latérales	Processus appelés via les pièces jointes	Changements de configuration
Connexion réseau	Flux de trafic	Liens externes	Instances nouvelles/modifiées
Accès aux fichiers	Activités de l'utilisateur		Indicateurs serverless
Modification du registre			Accès privilégié

Source : Enterprise Strategy Group

Stockés dans le Data Lake de Trend Micro, situé aux États-Unis et en Europe pour des raisons de conformité, les indicateurs de chaque entreprise sont soigneusement protégés, et dissociés des données provenant d'autres entreprises.

Grâce au Machine Learning, à un traitement analytique expert orienté sécurité (enrichi par la veille mondiale sur les menaces fournie par Trend Micro), et aux règles de détection (mises à jour par les experts sécurité de Trend Micro), l'XDR vise à réduire le "bruit de fond" en corrélant et en hiérarchisant les alertes. En se détournant des faux positifs, les analystes se concentrent alors sur les alertes les plus critiques.

Quand l'analyse par ML des données exploite les capteurs natifs, les analystes disposent généralement d'une meilleure compréhension des signaux d'activité et de détection. Cette approche s'annonce plus efficace que celles utilisant des API pour s'interfacer avec des produits tiers.

Lorsque certains fournisseurs tentent d'enrichir leurs solutions EDR en intégrant des fournisseurs tiers de réseaux et de messagerie, ils échouent souvent, faute d'une approche totalement intégrée et adossée au ML, pour analyser les indicateurs issus des Endpoints, du réseau, de la messagerie et du Cloud.

Pour exemple, les types de données extraites sont hétérogènes. Souvent, seules les données d'alertes sont transmises, sans les données complètes d'activité (indicateurs, métadonnées et données Netflow). Ce sont donc moins d'informations qui alimentent les modèles analytiques de corrélation et de priorisation. Qui plus est, la façon de définir ce que sont la détection et les indicateurs de gravité peut varier d'un fournisseur à l'autre. La disparité des indicateurs rend difficile le rapprochement ou la compréhension des données et donc l'évaluation du risque global.

Par exemple, les signaux d'alertes précoces issus de l'analyse du trafic peuvent être associés à l'activité des Endpoints et du Cloud, permettant ainsi de cibler les comportements spécifiques des assaillants, ce qui aide les analystes à neutraliser les exactions en cours, ainsi que celles à venir.

Trend Micro XDR offre des investigations guidées et coordonne les possibilités de réponse sur plusieurs couches de sécurité, permettant aux analystes de prendre des mesures et de remédier aux attaques sur les nombreux dispositifs ciblés au sein de l'infrastructure.

Les solutions constitutives de Trend Micro étant proposées par l'éditeur, les entreprises peuvent automatiquement activer les mises à jour de sécurité en temps réel sur l'ensemble du périmètre à protéger.

Les API disponibles permettent aux solutions XDR de Trend Micro d'être intégrées aux solutions SIEM et SOAR.

Pour les entreprises qui ne disposent pas de ressources suffisantes ou qui souhaitent une disponibilité en 24/7, Trend Micro propose des services TDR managés pour les Endpoints, les réseaux, l'email et le Cloud. Les clients qui utilisent plusieurs services perçoivent mieux les avantages d'une analyse en profondeur, de la priorisation des incidents et de la prise en charge des menaces.

XDR et SIEM

Les plateformes SIEM (gestion d'informations et d'événements de sécurité) jouent un rôle clé dans la plupart des architectures de sécurité, en fournissant un point d'agrégation pour les logs, les événements et les alertes de sécurité. Les solutions XDR ne remplaceront pas le SIEM, mais fourniront un niveau supplémentaire d'automatisation et d'analyse qui alimente le SIEM, réduisant ainsi les efforts des analystes en sécurité. Le SIEM reste le lieu d'agrégation historique des informations qui seront utilisées par les entreprises dans le cadre d'analyses post-incident ou d'audits de conformité. Alors que de nombreuses organisations en font un mécanisme d'agrégation d'indicateurs, le SIEM ne propose ni analyses pointues basées sur le Machine Learning, ni éléments contextuels et portant sur les événements et les alertes. Les solutions XDR visent à devancer le SIEM en corrélant les événements de manière à accélérer la détection et la réponse aux menaces. Avec l'évolution des solutions XDR, il est fort possible qu'elles remplacent un grand nombre de fonctions assurées aujourd'hui par le SIEM.

Perspectives

76% des entreprises affirment que la détection et la réponse aux menaces sont devenues plus complexes aujourd'hui qu'il y a deux ans et que les outils actuels ne suffisent plus. Si les solutions de détection et de réponse au niveau des Endpoints ont aidé de nombreuses entreprises à identifier et à réagir à des attaques qui, selon elles, n'auraient pas été détectées, ces entreprises avouent néanmoins prendre du retard, en n'étant pas capables de suivre le volume actuel des attaques. Une nouvelle approche s'impose donc.

La grande majorité des entreprises prévoit d'augmenter les dépenses en matière de TDR au cours des 18 prochains mois (46% de façon significative, 42% de façon progressive) mettant ainsi en évidence la criticité de cette approche. Avec l'apparition de nouvelles solutions TDR et de services managés rendus possible grâce à l'XDR, les utilisateurs peuvent s'attendre à renforcer leur visibilité et leur niveau d'automatisation, réduisant ainsi le délai moyen de détection et de réponse aux menaces. Les analystes en sécurité consacreront ainsi plus de temps aux attaques sophistiquées, affineront leurs stratégies et amélioreront leurs processus.

Des fournisseurs de solutions XDR tels que Trend Micro offrent une nouvelle promesse, en aidant les équipes de sécurité à garder la main sur les risques associés à une cybercriminalité en constante évolution.