Livre blanc du SANS Institute

Pourquoi les EDR traditionnels sont inefficaces, et les solutions à ce problème

Rédigé par **Jake Williams**

Juin 2019

Commandité par

McAfee

Introduction

Quiconque travaille dans le domaine de la sécurité informatique, et ne vit pas dans une grotte, a certainement entendu parler de l'EDR (Endpoint Detection and Response). Censée révolutionner la manière dont les analystes en sécurité neutralisent les attaques informatiques, cette technologie n'a hélas pas tenu les promesses de son battage médiatique. Il en va d'ailleurs de même pour bon nombre d'autres solutions de sécurité.

L'argumentaire de vente d'un système EDR ressemble généralement à ceci : « Bien sûr, vous pouvez consulter les alertes dans votre solution SIEM, ouvrir un ticket de remontée des problèmes dans votre suite de logiciels de productivité et demander à un administrateur système d'intervenir. Mais le temps que vous exécutiez toutes ces opérations, l'auteur de l'attaque aura sans doute déjà exfiltré vos données. Ce n'est pas tant que vos fonctions de détection sont insuffisantes, mais plutôt qu'elles sont éparpillées. Et ensuite, comment allez-vous riposter ? Le temps, c'est de l'argent. Et le temps joue en faveur du pirate. C'est pourquoi vous avez besoin de l'EDR. Il consolide les fonctions de détection et de réponse en une seule plate-forme. »

Malheureusement, comme vous l'avez probablement deviné, l'EDR n'a pas vraiment répondu aux attentes.

L'un des défauts majeurs des déploiements EDR est que ces systèmes ne s'intègrent pas aux autres outils (SIEM, IDS, DLP, etc.) utilisés par les analystes en sécurité. Autre problème récurrent dans ces déploiements : la séparation des tâches habituelle entre équipe informatique et équipe de cybersécurité. La plate-forme EDR occupe l'intersection entre ces deux domaines : l'équipe de cybersécurité assure généralement la fonction de détection, tandis que l'équipe informatique se charge de la fonction de réponse. Chaque réponse entraîne un risque de panne système. Et puisque c'est le département informatique qui assume la responsabilité de toute indisponibilité

système, il est parfaitement logique qu'il ait coutume de gérer toutes les fonctions de réponse. Cependant, comme l'EDR couvre à la fois les fonctions de détection et de réponse traditionnelles, il rompt avec ce modèle et ouvre potentiellement la voie à des problèmes de processus et de workflow.

En outre, de nombreuses plates-formes EDR sont intrinsèquement incapables de fonctionner comme la véritable solution tout-en-un promise par le fournisseur. La plupart ne s'intègrent pas aux solutions SIEM. D'autres sont totalement focalisées sur le terminal, négligeant le rôle que joue le trafic réseau à la fois pour l'élimination des faux positifs et pour l'apport du contexte nécessaire à la génération d'alertes légitimes.

Dans les sections qui suivent, nous allons examiner d'autres lacunes des plates-formes EDR classiques et les solutions à mettre en œuvre pour une implémentation EDR efficace. Nous présenterons également une liste des éléments à contrôler lors de la sélection et du déploiement d'une telle plate-forme.

Causes des défauts de l'EDR

À l'instar de nombreux systèmes de sécurité informatique, les plates-formes EDR ne se montrent généralement pas à la hauteur des résultats annoncés. Or, comme c'est le cas des déploiements SIEM décevants, ces mauvais résultats semblent paradoxaux. Ces technologies étant relativement matures, certaines caractéristiques communes devraient permettre d'expliquer les lacunes constatées. Dans cette section, et à la figure 1, nous allons examiner plusieurs raisons expliquant pourquoi les systèmes EDR ne parviennent pas à tenir leurs promesses une fois déployés.

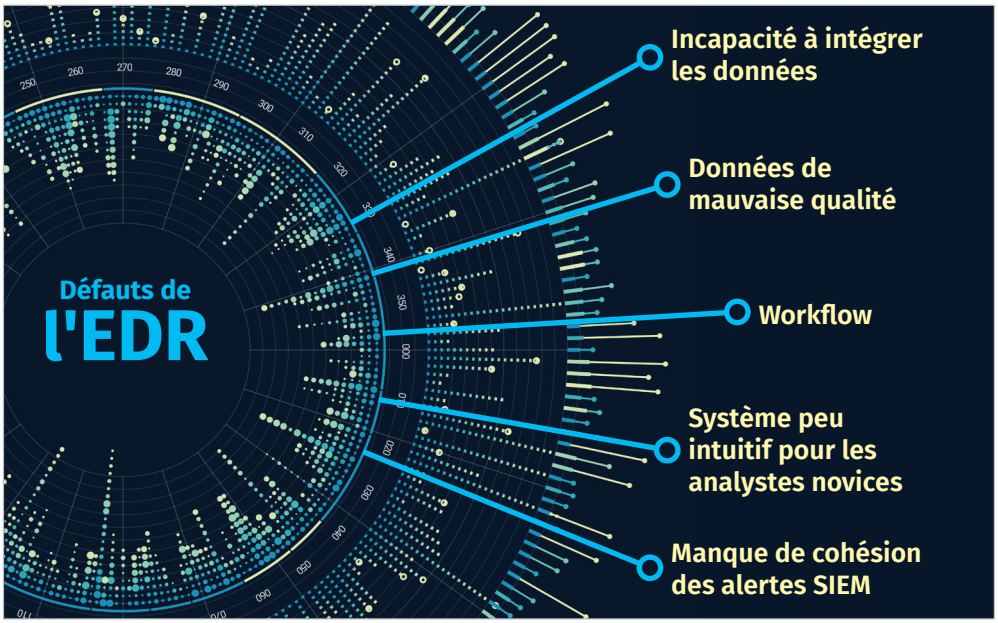

Figure 1. Défauts des systèmes EDR.

Incapacité à intégrer les données issues d'autres sources

Le manque d'intégration de ces plates-formes avec d'autres sources de données est la cause majeure, et sans doute la plus courante, des échecs des déploiements EDR. Bien que l'intégration au SIEM soit la plus demandée, de nombreuses autres sources de données peuvent contribuer à enrichir les alertes EDR tout en éliminant les faux positifs. Idéalement, les outils EDR devraient s'intégrer aux sources de données suivantes :

- Journaux DNS
- Journaux des flux de trafic réseau ou NetFlow
- Journaux des proxys web
- Données d'inventaire informatique
- Résultats d'analyse des vulnérabilités
- Journaux DHCP
- Informations de connexion Active Directory
- Journaux de fournisseurs d'authentification multifacteur (MFA)

Bien que la liste ci-dessus ne soit certainement pas exhaustive, la plupart des plates-formes EDR actuelles ne s'intègrent pas avec ces sources de données. Certains fournisseurs EDR feront remarquer que leur système permet à la solution SIEM d'absorber la plupart de ces types de données et qu'il s'intègre avec elle.

C'est peut-être vrai, mais pourquoi utiliser la solution SIEM par l'intermédiaire du système EDR si c'est la seule intégration possible ? Pourquoi ne pas simplement transmettre les données EDR à la solution SIEM pour qu'elle les analyse ? C'est une option, mais qui cantonne l'EDR à la détection, sans fonction de réponse. Après avoir établi un plan d'action, il faut passer du contexte du système SIEM à celui de la plate-forme EDR pour exécuter l'action de réponse. Ce processus lourd trahit les promesses d'efficacité qui avaient motivé l'adoption d'une solution EDR. Qui plus est, il subordonne cette dernière au système SIEM.

Données d'investigation de mauvaise qualité

C'est là un autre défaut courant des solutions EDR. Quasiment toutes celles qui sont disponibles sur le marché actuellement sont en mesure d'examiner les données des terminaux, telles que les listes de processus, les clés et valeurs de registre, ainsi que les connexions réseau actives. Ces données sont très utiles pour identifier une intrusion, mais ne suffisent pas à elles seules. En effet, elles n'offrent pas le contexte permettant à d'autres outils tels qu'un SIEM d'éliminer les faux positifs et mettre en évidence les vraies alertes.

À titre d'exemple, des données EDR médiocres ne déclencheront aucune alerte en cas d'attaque par utilisation généralisée de mot de passe (password spraying). Lors de ce type d'attaque, le pirate tente d'utiliser un même mot de passe sur plusieurs comptes, voire tous les comptes du domaine. S'il n'intègre pas les journaux stockés dans la solution SIEM, l'EDR risque de passer à côté de l'attaque.

Les données de mauvaise qualité ne sont pas imputables à un système EDR particulier (ni même aux systèmes EDR en général). Il s'agit plutôt d'un problème de visibilité. Généralement, les systèmes EDR analysent des données provenant d'un seul terminal à la fois, alors que les solutions SIEM mettent en corrélation des données de plus haut niveau sur plusieurs terminaux (notamment des données réseau). De nombreuses entreprises pensent qu'un EDR remplacera le système SIEM pour les détections sur le terminal, mais elles constatent malheureusement que le premier ne leur offre qu'une vision incomplète de la situation.

Complexité d'exécution des analyses de qualité

Dans bien des cas où les investigations réalisées demeurent incomplètes, toutes les données nécessaires pour les finaliser sont en réalité accessibles à l'analyste. Le hic, c'est qu'il ne s'en rend pas compte parce qu'il cherche au mauvais endroit. Le manque d'intégration entre EDR et SIEM y est pour beaucoup. En effet, après avoir reçu une alerte dans le système EDR, l'analyste doit basculer vers la solution SIEM pour obtenir des données complémentaires. Or, ces données n'y sont pas toujours stockées de façon à simplifier l'investigation.

DHCP est souvent à l'origine du problème. De nombreux journaux figurant dans le SIEM contiennent uniquement des informations d'adresse IP. D'autres journaux ne comportent que des informations de nom d'hôte. Bien sûr, certains contiennent les deux. La plupart des systèmes EDR ont recours à un agent installé sur le terminal, de sorte que l'ID d'installation constitue l'identificateur unique le plus approprié pour le

terminal. Néanmoins, il est peu probable que la solution SIEM capture ces informations, ce qui signifie que leur mise en corrélation et l'émission d'alertes exigent de nombreux allers-retours entre les systèmes SIEM et EDR.

La situation se complique encore si toutes les données requises ne sont pas disponibles dans le SIEM. Par exemple, il arrive souvent que les journaux DHCP (essentiels pour corréler d'autres données utiles) ne soient pas du tout alimentés en données dans le SIEM. Ou parfois, ils sont transférés au SIEM, mais conservés moins longtemps que d'autres données qui ont besoin de ces journaux DHCP pour obtenir le contexte. Chaque basculement obligatoire entre systèmes pour offrir à l'analyste un tableau complet de l'incident réduit la probabilité de voir l'investigation menée à bien de façon approfondie.

Difficulté pour les analystes novices à être rapidement opérationnels

Nombre de systèmes EDR manquent à leurs promesses en situation réelle car ils offrent trop d'options à l'analyste. Face aux innombrables possibilités de configuration, les analystes peu expérimentés peuvent se sentir submergés, et ils le sont souvent.

Depuis que l'EDR a trouvé sa place au sein de l'écosystème de la sécurité informatique, il joue un rôle actif dans l'interrogation des terminaux. La solution SIEM tient quant à elle un rôle passif (elle assimile et met en corrélation les données des journaux). Le rôle actif de l'EDR a toutefois un prix. Tirer pleinement parti de cette plate-forme exige de savoir quelles questions poser, ce qui est excessivement compliqué pour les analystes sans grande expérience.

Il est possible de poser des questions à la solution SIEM, mais les possibilités sont limitées aux données déjà stockées. Cette contrainte se traduit par la nécessité pour les ingénieurs de répondre à certaines questions difficiles avant un incident, comme illustré à la figure 2.

Même si l'on peut s'appuyer sur les meilleures pratiques pour répondre à certaines de ces questions, il est impossible d'apporter une réponse précise à la totalité d'entre elles pour un incident spécifique survenant dans une entreprise donnée.

Le système EDR comble ce vide. La solution SIEM stocke et met en corrélation les journaux les plus susceptibles d'être utiles au cours d'une investigation, mais le système EDR procure à l'analyste une flexibilité optimale pour poser les questions dont il ignorait au départ qu'il devrait y répondre. La capacité de l'EDR à remédier aux lacunes est particulièrement remarquable lors de l'apparition de nouvelles classes d'attaques. Comme les cybercriminels adaptent constamment leurs techniques, les entreprises doivent être à même de revoir rapidement leurs méthodes d'investigation. C'est là où les systèmes EDR font mieux que d'autres technologies disponibles sur le marché aujourd'hui : ils offrent la souplesse nécessaire pour interroger activement les terminaux protégés.

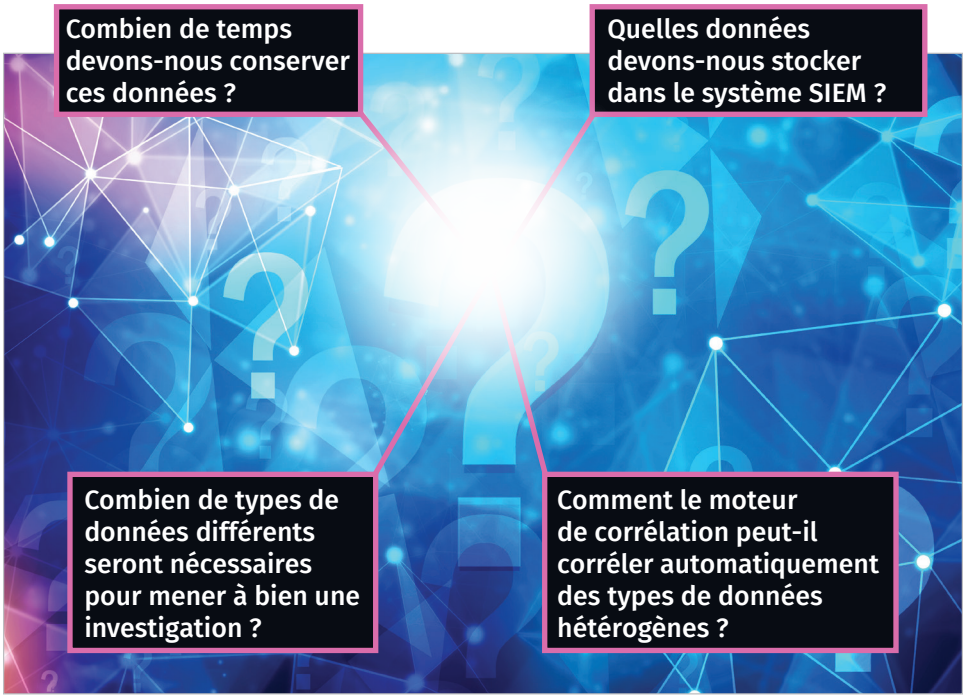

Figure 2. Considérations en matière d'architecture de journalisation.

Les EDR peuvent contribuer à résoudre le problème d'accumulation de données que posent également d'autres solutions. Comme l'EDR permet à l'analyste d'interroger en temps réel les données des terminaux, il n'est plus nécessaire de tout consigner « au cas où ». L'analyste peut lancer la collecte des données de terminal voulues au moment où elles deviennent nécessaires.

Supposons que l'on découvre un nouveau pirate qui exploite une nouvelle attaque par transfert local direct de DLL dans l'environnement d'entreprise. Pour mener l'enquête, l'analyste doit identifier les DLL chargées sur chacun des terminaux de l'entreprise. Bien que, techniquement, ces données puissent être journalisées à chaque lancement d'un nouveau processus et transmises au SIEM, leur volume rend cette approche difficile à mettre en pratique. Il est nettement préférable d'interroger ces données à la demande à l'aide du système EDR afin de rechercher tous les processus ciblés dans lesquels la DLL malveillante a été injectée. Cette méthode a l'avantage de nécessiter moins de stockage, mais également de permettre une exécution plus rapide de la requête, sur des données en temps réel issues du système EDR et non sur des données historiques provenant du SIEM (lesquelles risquent d'ailleurs de ne plus être applicables).

Traiter une alerte émise par le SIEM est une chose, mais répondre à des questions non structurées de la plate-forme EDR exige un niveau de compétences totalement différent. Les analystes novices ont déjà du mal à savoir quelles questions poser. C'est pourquoi ils attachent souvent moins de valeur à la plate-forme EDR. La situation est pire dans les entreprises dépourvues d'une solide équipe d'analystes en sécurité informatique expérimentés. Les solutions EDR offrant des interfaces intuitives et des outils de création de scénarios d'investigation aident à pallier le manque d'expérience des analystes novices, accélérant ainsi leur prise en main.

Même les analystes rompus à l'utilisation d'un SIEM peuvent estimer que la nature active d'un système EDR le rend moins intuitif. Les plates-formes EDR prenant en charge les workflows pouvant être définis par l'utilisateur sont plus intéressantes pour les entreprises qui emploient des analystes novices.

Manque de cohésion entre les alertes des systèmes SIEM et EDR

Dans la plupart des déploiements EDR que nous avons observés sur le terrain, les alertes générées par le SIEM ne sont pas en phase avec celles provenant du système EDR. Ce problème est parfois dû à un manque d'intégration. Mais la présence de processus mis en place avant le déploiement EDR peut également en être à l'origine.

Cela dit, une plate-forme EDR capable d'assimiler aisément les données SIEM et de les utiliser pour soit générer des alertes, soit ajouter du contexte aux alertes EDR existantes, peut très bien compenser cet inconvénient. C'est simple : les systèmes EDR incapables d'absorber les données d'autres sources créent une nouvelle solution cloisonnée. Face à la mutation rapide des attaques actuelles, les entreprises ne peuvent pas se permettre de déployer des solutions qui ne s'intègrent pas facilement avec d'autres.

Une multitude de produits SIEM intègrent un système de gestion des tickets au sein du logiciel même. De nombreuses entreprises utilisent la solution de gestion des tickets intégrée au système SIEM en tant qu'outil de gestion des cas et de suivi des alertes. Reste que la plupart des systèmes EDR ne peuvent pas s'intégrer simplement avec ces outils de gestion des cas propriétaires.

Mettre en place une architecture des opérations de sécurité à l'épreuve du temps permet d'éviter ce problème. Si possible, n'optez pas pour des solutions propriétaires dépourvues d'interfaces externes. Bien que l'utilisation d'un système de gestion des tickets externe s'accompagne d'autres exigences en matière de licences et d'heures de configuration supplémentaires, l'investissement initial en vaut probablement la peine pour faciliter les changements futurs au niveau de l'architecture.

Lorsqu'un système centralisé de gestion des tickets est utilisé, les solutions SIEM et EDR alimentent le même système. L'environnement dispose alors d'un emplacement unique dans lequel l'analyste peut identifier toutes les alertes pertinentes, quel que soit le système les ayant générées. Le problème est que, bien trop souvent, l'analyste reçoit

les alertes à partir du SIEM immédiatement, dans le cadre du workflow établi, tandis qu'il doit régulièrement interroger le système EDR pour vérifier la présence de nouvelles alertes. Une solution provisoire serait d'envoyer les alertes EDR au SIEM et d'y configurer ensuite des règles de corrélation de façon à générer automatiquement des tickets relatifs aux alertes EDR. Cette solution est toutefois loin d'être idéale, car elle fait de l'EDR un produit de second rang par rapport au SIEM.

L'EDR : plus que la détection

Jusqu'ici, ce livre blanc s'est concentré sur les workflows et les capacités de détection du système EDR. Or l'EDR ne se résume pas à la détection. Les fonctionnalités de réponse aux incidents sont clairement tout aussi importantes. Pourtant, lors de l'évaluation de ces systèmes, les utilisateurs se rendent souvent compte que les fonctions de correction et de réponse ont été greffées a posteriori à celles dédiées à la détection. De même, lorsque nous examinons les cycles de vie des produits, nous constatons fréquemment que la détection bénéficie de bien plus d'améliorations que la réponse.

Nous avons déjà évoqué une raison de ce déséquilibre : un système EDR offre des fonctionnalités qui relèvent communément des rôles de l'équipe de cybersécurité et de l'équipe informatique. Malgré le chevauchement de compétences entre les deux, c'est le département de cybersécurité seul qui assume le plus souvent la charge budgétaire des systèmes EDR.

Il semble que les fournisseurs de solutions EDR obéissent pour la plupart aux forces du marché. Ils partent du principe que les décideurs des équipes de cybersécurité sont bien plus susceptibles d'accorder de la valeur aux fonctionnalités de détection qu'aux fonctionnalités de réponse. Nous pensons qu'ils ont tort. De nombreuses fonctions de requête pouvant être exécutées par un système EDR peuvent également l'être par un système de gestion des actifs informatiques, tel que SCCM. L'avantage majeur offert par le déploiement d'une solution EDR ne se constate que lorsque ses capacités de réponse sont prises en compte. Dans cette section, nous allons passer en revue certaines des fonctionnalités de réponse que doit idéalement proposer un système EDR.

Fonctionnalités de réponse idéales pour les systèmes EDR

- Arrêter les processus en cours d'exécution
- Empêcher l'exécution de processus en fonction de critères (nom, chemin, arguments, parent, éditeur ou valeur de hachage)
- Bloquer la communication de processus spécifiques sur le réseau
- Bloquer la communication de processus avec des noms d'hôte ou adresses IP spécifiques
- Désinstaller des services
- Modifier les clés et valeurs de registre
- Arrêter ou redémarrer un terminal
- Déconnecter des utilisateurs d'un terminal
- Supprimer des fichiers et répertoires du système d'exploitation, même s'ils sont activement en cours d'utilisation (un redémarrage peut être nécessaire)

La plupart des systèmes EDR offrent un sous-ensemble de ces fonctionnalités. Le redémarrage des terminaux compte parmi celles qui sont le plus souvent absentes. Il arrive fréquemment que les cyberattaques installent des rootkits en mode utilisateur qui détournent l'exécution de code système (hooking). L'objectif est d'empêcher la suppression des clés et valeurs de registre servant à assurer la persistance du malware entre les redémarrages. Tout au long de son exécution, le logiciel malveillant dissimule au moyen de processus les fichiers et répertoires dont il se sert. Bien souvent, il recourt à un service régulé par le Gestionnaire de contrôle des services pour rester actif de manière durable.

Faute de pouvoir exécuter le redémarrage à distance d'un système, il est fort possible qu'une solution EDR ne permette pas d'éradiquer un logiciel malveillant qui tire parti des techniques mentionnées précédemment. En cas d'incident, les analystes doivent pouvoir réagir et endiguer le problème rapidement. Restaurer l'image d'un système à chaque alerte antivirus ne suffit plus ; cette approche a fait son temps face aux menaces actuelles.

La plupart des systèmes EDR d'aujourd'hui permettent aux analystes de mettre fin à des processus particuliers. Or, ils sont souvent incapables d'empêcher un processus identique de redémarrer immédiatement. L'analyste se trouve ainsi embarqué dans un jeu futile où les efforts incessants qu'il déploie pour mettre en échec le cyberpirate sont vains : celui-ci aura toujours l'avantage. Lors de l'évaluation d'un système EDR, examinez attentivement la façon dont il permet aux analystes de bloquer de façon proactive une technique d'attaque connue, au lieu de simplement y riposter.

Enfin, l'emploi d'interpréteurs de scripts comme PowerShell ou cscript pose souvent problème dans les systèmes EDR. Tous deux sont utilisés régulièrement pour exécuter des opérations système normales, mais souvent aussi à de mauvaises fins par les logiciels malveillants. Le système EDR doit offrir à l'analyste des fonctions lui permettant de faire la différence entre l'utilisation légitime et illégitime des interpréteurs de scripts.

Liste de contrôle pour l'évaluation des solutions EDR

Au cours des dernières années, le marché des solutions EDR est devenu relativement encombré. Les entreprises doivent évaluer correctement un EDR si elles veulent maximiser les chances que son implémentation réponde aux attentes définies. Cette section propose une liste de contrôle décrivant les fonctionnalités qui contribueront à la réussite du déploiement EDR au sein d'une entreprise. Même si toutes les fonctionnalités répertoriées ne sont pas toujours nécessaires pour garantir cette réussite, nous les avons incluses ici car leur importance est attestée.

Fonctionnalité	Niveau de priorité	Justification
Capacité à interroger tous les terminaux, des groupes préconfigurés de terminaux ou des groupes ad hoc créés à l'aide d'autres données de requête	ÉLEVÉ	Au cours d'une investigation, les analystes doivent configurer des groupes ad hoc impossibles à prévoir au moment de l'installation du système EDR. Les groupes sont souvent créés sur la base d'une autre requête soumise à l'EDR (par exemple, pour rechercher tous les hôtes sur lesquels utilisateurX s'est connecté au cours des sept derniers jours).
Fonctionnalité de réponse qui répond aux besoins prévus de l'entreprise	ÉLEVÉ	L'entreprise doit analyser les incidents traités par le passé et examiner les mesures de réponse prises manuellement pour déterminer si l'EDR peut prendre la relève. Lors de l'évaluation, un système EDR n'offrant pas les options de réponse adaptées au workflow de l'entreprise doit être moins bien noté.
Intégration avec la solution SIEM	ÉLEVÉ	L'intégration du système EDR avec la solution SIEM est vivement recommandée. Idéalement, l'intégration devrait être bidirectionnelle. Quoi qu'il en soit, l'EDR doit être en mesure de transmettre des données au SIEM.
Prise en charge des workflows adaptée aux analystes novices	ÉLEVÉ	Tout en fournissant un maximum de flexibilité aux analystes chevronnés, la solution EDR doit prendre en charge des workflows prédéfinis (et configurables) adaptés au personnel moins expérimenté, qui a besoin d'être guidé davantage lors des investigations.
Intégration du système de gestion des tickets	MOYEN	Le système EDR doit être capable d'alimenter en données un système de gestion des tickets tiers (tel que JIRA).
Groupes séparés de privilèges pour les requêtes et les réponses	MOYEN	La séparation des privilèges nécessaires à la création des requêtes et à la mise en œuvre des réponses est indispensable à l'adoption réussie de la plate-forme EDR. De nombreux utilisateurs chargés d'interroger les données (comme dans le cadre de la traque des menaces) ne doivent pas avoir la possibilité d'arrêter des processus, par exemple pour la suppression de fichiers.
Traitement des indicateurs de compromission	MOYEN	L'EDR doit idéalement être capable de traiter les indicateurs de compromission de différents formats, tels que Yara et OpenIOC, mais il doit prendre en charge au moins un format.
Intégration des hyperviseurs pour les groupes d'analyse	MOYEN	Dans les environnements informatiques modernes, les serveurs opèrent une migration transparente entre hyperviseurs physiques. Le système EDR analyse les ressources consommateur sur les serveurs invités, ce qui peut entraîner une surallocation des ressources de l'hyperviseur. Si la solution EDR prend en charge l'intégration des hyperviseurs, les groupes d'analyse peuvent être dynamiques.
Intégration des journaux syslog	FAIBLE	Le système EDR doit être capable d'envoyer des alertes via syslog pour un maximum de flexibilité d'intégration avec les autres systèmes.
Limitation de l'impact des analyses	FAIBLE	Le système EDR doit proposer des options de configuration permettant de limiter l'impact des analyses exécutées. Les utilisateurs citent l'interruption de service comme étant l'un des problèmes qui limitent l'adoption de l'EDR par les entreprises.
Plusieurs emplacements d'exportation de données	FAIBLE	Certains de ces produits ne peuvent s'intégrer qu'avec un unique système de suivi (syslog n'a qu'une seule destination, par exemple), ce qui limite la flexibilité lors de la mise au point d'une architecture système complète.
Intégration d'API	FAIBLE	L'intégration d'API permet à l'entreprise de personnaliser l'enrichissement des données et les activités de réponse. Les entreprises qui automatisent les interactions entre systèmes peuvent modifier la priorité de cette fonctionnalité.

Cas d'utilisation d'un système EDR

L'application la plus évidente d'un système EDR est la détection des intrusions et l'automatisation de la réponse. Dans cette section, nous passerons en revue divers cas d'utilisation illustrant l'opérationnalisation d'une solution EDR en environnement réel. Nous pourrions certainement aborder d'autres scénarios, mais ces exemples conviennent parfaitement pour illustrer les types de workflows que prend en charge une solution EDR.

Le système EDR détecte un processus nommé lsass.exe exécuté en tant qu'utilisateur normal

Les faits

Le processus **`lsass.exe`** doit toujours s'exécuter dans un contexte système, jamais dans celui d'un utilisateur normal. Comme un analyste débutant pourrait ignorer qu'il ne peut y avoir qu'une seule instance du processus **`lsass.exe`** en cours d'exécution sur un hôte Windows, le système EDR attire l'attention sur ce fait et déclenche une alerte, ce qui lance une investigation. Au cours du traitement de l'alerte, l'analyste interroge l'EDR pour identifier les processus en cours d'exécution sur le terminal et découvre qu'un processus **`lsass.exe`** non autorisé s'exécute en tant qu'enfant de **`cmd.exe`**. Le processus **`cmd.exe`** s'exécute lui-même en tant qu'enfant de **`winword.exe`**. L'analyste soupçonne alors le processus non autorisé d'être le résultat d'une attaque par phishing menée à l'aide d'un document Word malveillant. Les date et heure de début des processus l'amènent à conclure que l'e-mail de phishing vient d'être ouvert. C'est donc l'occasion idéale pour que le système EDR traite l'incident en quelques minutes à peine, de l'intrusion à la détection jusqu'à la correction.

Rôle du système EDR

Reconnaissant le caractère certainement malveillant du processus **`lsass.exe`** non autorisé, l'analyste recherche les connexions réseau impliquant un des processus non autorisés. Il s'aperçoit que **`lsass.exe`** communique avec une adresse IP située en Europe de l'Est. Il utilise le système EDR pour arrêter immédiatement les processus non autorisés (**`lsass.exe`**, **`cmd.exe`** et **`winword.exe`**). Il s'en sert également pour exécuter des requêtes afin d'identifier les terminaux qui communiqueraient avec l'adresse IP suspecte. L'analyste détecte deux autres terminaux, dont il demande ensuite des informations système (processus en cours et informations de configuration des services, par exemple). Contrairement au premier système, ceux-ci n'utilisent pas un processus **`lsass.exe`** non autorisé ; quoi qu'il en soit, l'EDR facilite l'identification des processus malveillants.

Les systèmes traditionnels de surveillance du réseau (comme NetFlow et la capture de paquets complète) n'offrent pas le niveau de granularité des plates-formes EDR. Certes, ils sont capables d'orienter la personne chargée de l'investigation vers un terminal qui communique avec une adresse IP suspecte, mais pas d'identifier les processus réellement en cause. Cela signifie que l'analyste doit faire intervenir encore un autre système pour poursuivre son travail. En revanche, l'EDR permet au responsable de l'investigation d'identifier les processus spécifiques impliqués dans la communication (et d'y mettre fin).

Bien que la compromission du premier système vienne de se produire et soit facile à régler, le moment où les machines nouvellement identifiées ont été compromises n'est pas encore connu. L'analyste examine scrupuleusement les informations renvoyées par le système EDR et découvre que le mécanisme de persistance utilisé est un fichier LNK situé dans le répertoire de démarrage de l'utilisateur. Ce fichier est supprimé à l'aide de l'EDR.

L'analyste utilise l'EDR pour collecter d'autres éléments d'investigation numérique sur le système, notamment des descripteurs de fichiers ouverts provenant des processus malveillants identifiés. Cette opération permet de mettre au jour un fichier auparavant inconnu que le logiciel malveillant utilise, fichier qui passe ensuite dans les mains des experts en rétroconception de l'entreprise. Ceux-ci sont en mesure de décoder le fichier, qui contient une liste des domaines de rappel utilisés par le logiciel malveillant. Il est important de souligner que ce fichier (et les indicateurs de compromission récemment découverts) n'aurait pas été identifié sans l'aide de l'EDR.

Même si le malware utilise des noms de processus et des valeurs de hachage de fichier différents, la solution EDR a détecté la présence du même numéro de version de fichier, à savoir **`1.0.29.5.`**, sur les trois systèmes compromis. L'analyste recourt à l'EDR pour rechercher les systèmes exécutant des processus dotés de ces métadonnées exécutables. Ce type de détection est tout à fait impossible sans la technologie EDR, car un tel niveau de détail de journalisation ne serait jamais atteint avec un SIEM traditionnel.

Pour clore la phase de réponse, l'EDR est utilisé pour arrêter le reste des processus en cours d'exécution, confirmer la suppression du fichier **`.LNK`** employé comme mécanisme de persistance et bloquer la communication réseau avec les adresses IP et domaines identifiés.

Cette étude de cas démontre les avantages offerts par une solution EDR à plusieurs niveaux. Tout d'abord, sur la première machine identifiée comme étant compromise, l'incident est détecté et corrigé à partir d'une console unique en l'espace de quelques minutes. Ensuite, l'analyste est en mesure d'identifier immédiatement, en temps réel, les processus qui communiquent avec les adresses IP malveillantes (sans avoir à passer d'un système à l'autre). Enfin, il peut exécuter des requêtes pour rechercher des informations qui ne seraient jamais consignées dans un SIEM (le numéro de version du fichier, par exemple) et ainsi s'assurer qu'il ne reste aucune variante non détectée du logiciel malveillant dans l'environnement.

La solution EDR détecte les comportements suspects

Les faits

L'entreprise reçoit de nouvelles données de cyberveille indiquant qu'une menace APT connue pour la cibler utilise le répertoire **`%USERPROFILE%\AppData\Roaming\SharePoints`** pour y rassembler provisoirement des données en vue de leur exfiltration. Elle n'a observé récemment aucune activité émanant de ce groupe APT au sein de son réseau, mais craint que les nouveaux indicateurs publiés y soient détectés. Si c'est le cas, elle souhaite pouvoir réagir rapidement et refouler le pirate.

Rôle de l'EDR

Le système EDR est chargé d'interroger chaque machine du réseau pour détecter la présence du répertoire **`%USERPROFILE%\AppData\Roaming\SharePoints`**, identifié par la cyberveille comme un indicateur de compromission. Ce répertoire est découvert sur quatre machines, deux au siège de l'entreprise et deux dans différents sites distants ne disposant pas d'équipe informatique ou de sécurité informatique sur place. Il est toujours regrettable de détecter une intrusion, mais si aucun support n'est présent sur le site touché, la situation se complique.

Au moyen de requêtes lancées via le système EDR, l'analyste recherche immédiatement des informations sur les processus, notamment les DLL chargées et les données sur les connexions réseau des quatre machines concernées. Dans un premier temps, il ne voit pas de processus semblant malveillant, mais constate qu'une DLL qu'il ne connaît pas, **`kernel64.dll`**, est chargée dans l'espace d'adressage d'**`explorer.exe`** (processus du Bureau de l'utilisateur). Détecter la DLL chargée dans **`explorer.exe`** revient à identifier l'indicateur de compromission diffusé, lequel est également lié à l'utilisateur (et non à la machine).

En examinant les données de connexion réseau, l'analyste constate que sur trois des machines infectées, le processus **`explorer.exe`** a établi une connexion à une adresse IP externe via le port TCP 33389. Après avoir envisagé d'utiliser le système EDR pour bloquer d'emblée la communication avec cette adresse IP, il change d'avis et décide de lui soumettre d'abord d'autres requêtes.

S'appuyant sur les connaissances acquises grâce aux précédentes requêtes, il interroge alors toutes les machines qui communiquent avec le port TCP 33389 ou l'adresse IP suspecte. Il recherche également tous les processus qui chargent une DLL nommée **`kernel64.dll`**. Il découvre ainsi qu'elle est chargée par cinq autres machines. Toutefois, comme celles-ci ne contiennent pas le répertoire relais destiné à l'exfiltration, elles n'auraient pu être identifiées à l'aide des données de cyberveille fournies au départ. L'analyste repère également une autre adresse IP suspecte.

À l'aide de l'EDR, il lance une requête sur les paramètres du registre des ordinateurs identifiés de tous les utilisateurs connectés afin de déterminer le mécanisme de persistance utilisé par le logiciel malveillant. Toutes les machines infectées possèdent une entrée AutoRun servant à démarrer une application de profilage système tierce légitime. Cette dernière étant dotée d'une signature numérique, elle a été autorisée par les listes blanches d'applications ; en fait, elle sert au transfert local direct d'une DLL à partir du disque et à son injection dans **`explorer.exe`**, après quoi elle se ferme. D'autres requêtes EDR sont exécutées pour rechercher les autres machines sur lesquelles l'application de profilage système aurait éventuellement été installée. Aucune n'est toutefois détectée.

La phase de détection étant terminée, l'analyste passe à la réponse. Il utilise l'EDR pour supprimer à distance les clés de registre AutoRun utilisées à des fins de persistance ainsi que l'application de profilage système tierce (et les DLL malveillantes injectées). Toujours à l'aide de l'EDR, il bloque toutes les communications avec les adresses IP identifiées. Bien que la communication doive également être bloquée au niveau du pare-feu, cette tâche incombe généralement à une autre équipe. La coordination entre différentes équipes durant la réponse entraîne des retards. Certes, il n'aurait probablement pas été approprié de bloquer la communication avec les adresses IP au cours des phases d'identification et d'évaluation de l'incident. Mais dès lors que l'équipe de réponse passe à l'action, le blocage doit s'effectuer immédiatement et de façon transparente. D'après notre expérience, cette intervention coordonnée avec l'équipe réseau n'est ni immédiate ni transparente, ce qui confirme tout l'intérêt de la solution EDR.

L'analyste recourt également à l'EDR pour, dans un premier temps, collecter les fichiers contenus dans les répertoires relais des machines infectées afin d'évaluer l'impact de l'incident, puis pour supprimer ces répertoires (et tous les fichiers recueillis par le pirate). Enfin, les ordinateurs sont redémarrés à distance à l'aide de la solution EDR — le redémarrage étant la meilleure pratique recommandée dans ce cas, au vu de la technique d'injection de code utilisée. Après leur connexion, ils sont soumis à une nouvelle analyse pour vérifier qu'ils sont sains.

Dans cet exemple d'incident, l'EDR s'avère particulièrement utile là où il n'existe pas d'équipe informatique ou d'équipe de sécurité informatique dédiée. Sans lui, l'entreprise n'aurait pas pu neutraliser la menace simultanément sur toutes les machines détectées dans les différents sites. À l'heure où les cybercriminels sont de plus en plus sophistiqués, les entreprises doivent être certaines d'agir rapidement pour les empêcher de contrer la riposte en déployant de nouveaux logiciels malveillants inconnus.

Conclusion

Le marché des solutions EDR, simple niche autrefois, a explosé ces dernières années. Néanmoins, ce n'est pas parce qu'ils sont qualifiés d'EDR que tous les produits se valent en termes de fonctionnalités ou que leur efficacité a été démontrée. Dans ce livre blanc, nous nous sommes penchés sur les fonctionnalités que devrait idéalement proposer un système EDR, sur divers cas d'utilisation de l'EDR et sur les lacunes de certains déploiements. Nous proposons également une liste de contrôle destinée à l'évaluation des produits EDR. Lors de l'évaluation des déploiements EDR, les divers conseils de ce livre blanc seront précieux, tels que :

- Utiliser la liste de contrôle des fonctionnalités EDR
- Tirer parti de l'analyse des divers problèmes courants des déploiements EDR
- S'assurer que la solution EDR choisie applique les fonctionnalités de réponse adéquates
- Déterminer dès le départ l'incidence de l'intégration au SIEM et à d'autres outils sur le déploiement EDR
- Vérifier que la solution EDR prend en charge des workflows adaptés aux analystes novices

L'auteur

Jake Williams est analyste et formateur en chef auprès du SANS Institute. Il est également auteur de cours et responsable de la conception de plusieurs défis NetWars destinés à la suite prestigieuse de formations sur la cybersécurité développées par le SANS Institute. Pendant plus de dix ans, Jake Williams a exercé diverses fonctions dans le domaine de la sécurité informatique au sein de plusieurs organismes publics, se spécialisant dans les matières de l'investigation numérique côté offensive, du développement de logiciels malveillants et du contre-espionnage numérique. Il est le fondateur de Rendition InfoSec, entreprise proposant des tests d'intrusion, des services d'investigation numérique et de réponse aux incidents, une expertise en exfiltration de données cloud, ainsi que des outils et conseils pour protéger les données client contre les attaques persistantes sophistiquées à la fois sur site et dans le cloud.

Commanditaire

SANS voudrait remercier le commanditaire de cette étude :

McAfee™