MASTERE SPECIALISE CYBERSECURITE ET CYBERDEFENSE 2022-2023

OSINT : Etat de l'art et intelligence économique du marché des EDR

Responsable :

Nicolas BLOUMINE

Membres du groupe :

Mesmin NGOULO BEMBE

Corentin VIEILLESCAZES

Table des matières

Introduction

Les dix (10) dernières années, nous avons assisté à l'émergence d'une gamme d'outils de détection des incidents de sécurité sur un système d'information précisément au niveau de l'infrastructure qu'on appelle les EDR pour Endpoint Detection and Response. En effet, cela est une réponse à l'escalade du nombre et de la complexité plus en plus grandissantes des cyberattaques.

Mais jusque-là, rien de nouveau sous le soleil, car les éditeurs de solutions développent des contremesures, les cybercriminels développent des manières de les contourner et les éditeurs contrent les nouvelles manières ainsi de suite, c'est ainsi que cela a toujours fonctionné.

Alors pourquoi donc ces outils de détection et de réponse ? A quelle problématique cela répond-il ? Pour quels types d'entreprises et pourquoi ?

Nous allons réponse à l'ensemble de ces questions dans ce document et par la même occasion expliquer pourquoi ces outils ne sont plus que des outils accessoires, mais nécessaires, voire indispensables lorsqu'on veut lutter efficacement contre la menace croissante.

Nous allons donc commencer par définir ce qu'est un EDR, la problématique que ça résout et comment ça la résout.

Puis nous allons évoquer le marché des EDR avec une liste non exhaustive de solutions que nous allons comparer, expliquer leurs différents points forts et faibles et expliquer, mais aussi de leur provenance dans un contexte géopolitique.

Ensuite, nous aborderons la sécurité opérationnelle et expliquer en quoi l'EDR est essentiel pour une gestion optimale de la sécurité opérationnelle tout en spécifiant ces limites et comment cela s'intègre dans un tout.

Enfin, nous essayerons de nous tourner vers le futur en effleurant l'XDR (eXtended Destion and Response), ses liens et différences avec l'EDR et nous nous demanderons si c'est le futur de la détection et réponse aux incidents.

Les EDR : la genèse

Avant les EDR, nous avions déjà des outils de détection d'activités malveillantes sur les terminaux d'une infrastructure tels que les antivirus par exemple. Mais plus globalement, on parlait de Endpoint Protection Platform (EPP). Gartner définit l'EPP[1] comme un ensemble d'outils de protection des terminaux d'une entreprise constitué de fonctionnalités telles que : scan de malware utilisant une méthode statique basée sur les signatures des codes malveillants, firewall intégré, contrôle de ports. C'est donc un outil principalement utilisé pour la protection.

[1] Evaluation Criteria for Endpoint Protection Platforms", Gartner, Inc. Mario de Boer. March 24, 2015

Les EDR vont plus loin dans la protection et fournissent une surveillance continue et répondent aux menaces avancées sur les terminaux. Mais alors quelles sont ces menaces ?

La problématique qu'adressent les EDR

Les EDR (Endpoint Detection and Response) ont été développés pour compenser les manques des EPP et anciens antivirus à contrer toutes les cyber-attaques.

Au début des années 2010, se démocratisaient le fait de pouvoir exécuter un code malveillant sans installer de logiciel, mais juste en utilisant un exécutable pour échapper aux antivirus. Et il existe plusieurs façons d'introduire des fichiers et documents qui ne seront pas scannés.

Prenons deux exemples de menaces qui ont emmené au besoin des EDR.

Documents malveillants : phishing

Beaucoup d'utilisateurs comprennent la différence entre une application et un document Word, Excel, PowerPoint ou PDF. En effet, un programme peut exécuter du code tandis qu'un document ne peut juste qu'être lu ou écrit. Justement, c'est parce que cela n'est pas totalement vrai que des compagnes de phishing bien structurées arrivent à convaincre les utilisateurs d'ouvrir des documents qui semblent sans danger. En effet, avec un email personnalisé, on peut convaincre un recruteur d'ouvrir un CV piégé par exemple et donc contourner les outils de protection classiques.

Mouvement latéral

Le mouvement latéral est une technique où un attaquant peut à l'aide d'une commande propager sur le réseau. Il se trouve que quelques protocoles systèmes permettent facilement de faire un mouvement latéral. Un exemple notoire est celui connu sous le nom de « EternalBlue » qui a exploité le protocole SMB utilisé pour partager des fichiers sur un réseau. Des ransomwares connus tels que WannaCry ou encore NotPeya ont exploité cette vulnérabilité en 2017 pour se propager sur les réseaux et ainsi infecter le maximum de terminaux.

D'autres méthodes comme encore les « fileless malware » sont juste d'autres manières de contourner les antivirus classiques. Ainsi, au début des années 2010, les professionnels de la sécurité opérationnelle se sont rendu compte que les outils classiques ne suffisaient plus d'où l'entrée sur le marché des EDR.

Les fonctionnalités fondamentales d'un EDR

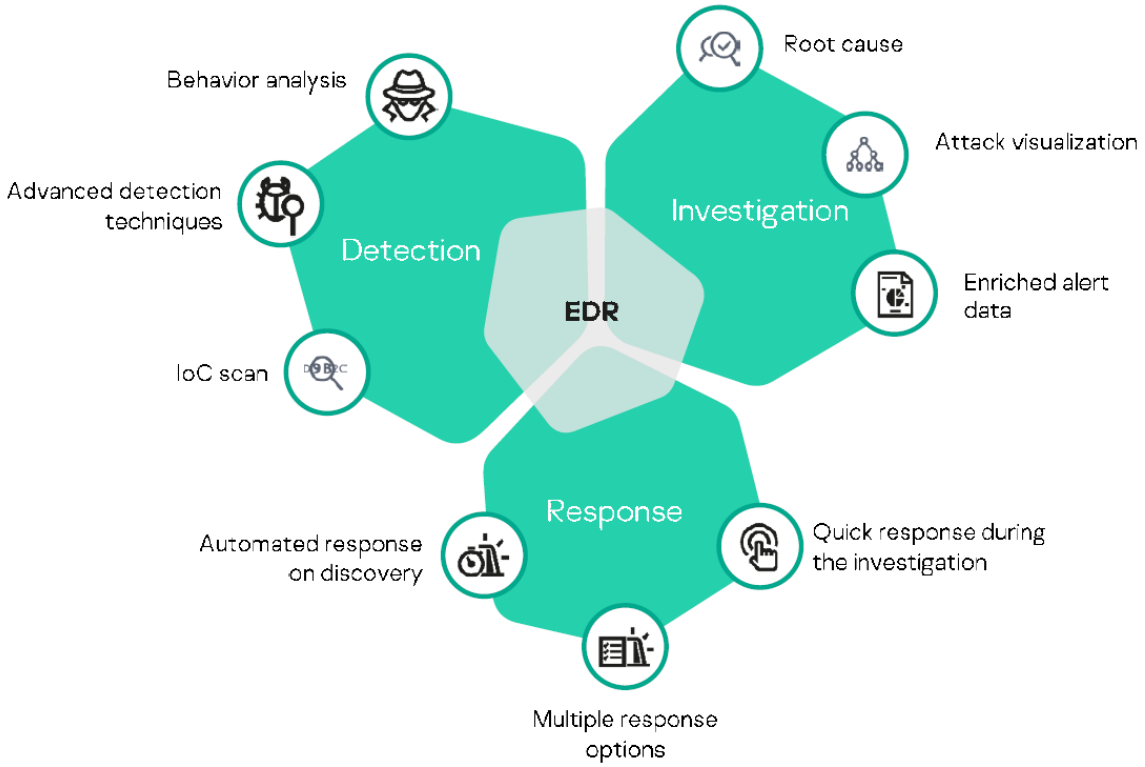
Avant les années 2010s, les entreprises embauchaient des équipes de réponse à incidents pour investiguer les failles de sécurité. En 2013, le plus fiable était Mandiant qui fournissaient des professionnels en sécurité en cas d'incident et cela n'était pas gratuit.

En même temps, des entreprises ont commencé à investir dans des outils permettant d'avoir une visibilité des réseaux et des activités sur les terminaux en temps réel. On peut prendre l'exemple de Facbook osquery. C'est un 2013 que **Anton Chuvakin** a pour la première fois sorti le terme ETDR (Endpoint Threat Detection and Response) qui deviendra juste EDR pour Endpoint Detection and Response.

Toutes les solutions EDR ont les mêmes objectifs : **identifier, investiguer et répondre aux menaces complexes.** Et pour accomplir cela, elles doivent avoir un ensemble de fonctionnalités qui sont :

- Fonctionnalité de détection : utilisant des techniques telles que l'analyse basée sur du machine learning et du sandboxing pour détecter et prévenir les codes malveillants.
- Une fonction d'analyse temps réel, de surveillance de la mémoire, recherche de modèle de comportement pour faciliter à la détection et répondre de manière rapide
- La Threat Intelligence appliquée
- La visibilité sur les terminaux qui est sinéquanone pour détecter des activités malveillantes
- Surveillance en temps réel des flux de données : récolte de ces données pour analyse à postériori
- Fonctionnalité de forensic pour investiguer les anciennes failles et celles non découvertes
- Fonctionnalité de réponse à incident à travers des alertes et des réponses aux activités malveillantes
- Fonctionnalité de filtrage afin de prévenir les « faux positifs »

Notons que les menaces d'origine cyber sont souvent traitées par une approche par couche en utilisant une série de filtres. Ainsi, même si toutes les solutions EDRs n'ont pas exactement toutes ces fonctionnalités, certaines sont indispensables notamment celles de la **visibilité**, d'**investigation** et de **réponse rapide et préférablement automatisée**.



Détection lors d'une attaque : framework d'attaques vs EDR

MITRE ATT&CK est une base de connaissances sur les tactiques et techniques des cyberattaques basée sur des observations réelles d'attaques. Les tactiques expliquent les objectifs de l'attaquant tandis que les techniques représentent comment ils sont atteints. La matrice MITRE ATT&CK organise visuellement ces tactiques et techniques pour faciliter la compréhension. Une séquence d'attaque complète peut être construite en passant par les colonnes de tactiques de gauche à droite et en utilisant les techniques appropriées. Certaines techniques peuvent être utilisées pour plusieurs tactiques et certaines techniques peuvent être utilisées pour atteindre différents objectifs.

Les outils EDR utilisent les tactiques et techniques de MITRE ATT&CK pour détecter les comportements malveillants en utilisant des règles de correspondance pour identifier les événements qui génèrent des alertes. Les événements sont enregistrés localement sur les hôtes et les événements pertinents peuvent être envoyés à une base de données centrale pour l'analyse. Les principaux fournisseurs d'EDR, déjà fournissent des règles de correspondance pour détecter les TTP (Tactics Techniques Procedures) de MITRE ATT&CK, mais les analystes peuvent également ajouter de nouvelles règles pour détecter des TTP supplémentaires dans une entreprise où l'outil EDR est déployé.

Les outils EDR ont principalement 4 fonctions : **détection d'incidents de sécurité potentiels**, **gestion de l'ingestion de journaux à grande échelle**, **enquête sur les incidents de sécurité** et **fourniture de conseils de remédiation**. Ils enregistrent des événements détaillés et bas niveau sur chaque hôte et les stockent localement. Les événements pertinents peuvent être envoyés à une base de données centrale pour l'alerte et l'analyse, pendant laquelle des événements supplémentaires peuvent être tirés de l'extrémité pour fournir un contexte forensique. Les outils EDR utilisent un système de correspondance de règles pour traiter le flux d'événements et identifier les événements qui doivent générer des alertes. Les principaux fournisseurs d'EDR déjà fournissent des règles de correspondance pour détecter les TTP de MITRE ATT&CK, mais les analystes peuvent également ajouter de nouvelles règles pour détecter des TTP supplémentaires dans une entreprise où l'outil EDR est déployé.

Le marché des EDR

Le marché des EDR est constitué de solutions de plusieurs types. Dans cette partie, nous allons nous baser sur le quadrant de marché Radicati afin de réaliser notre analyse.[2]

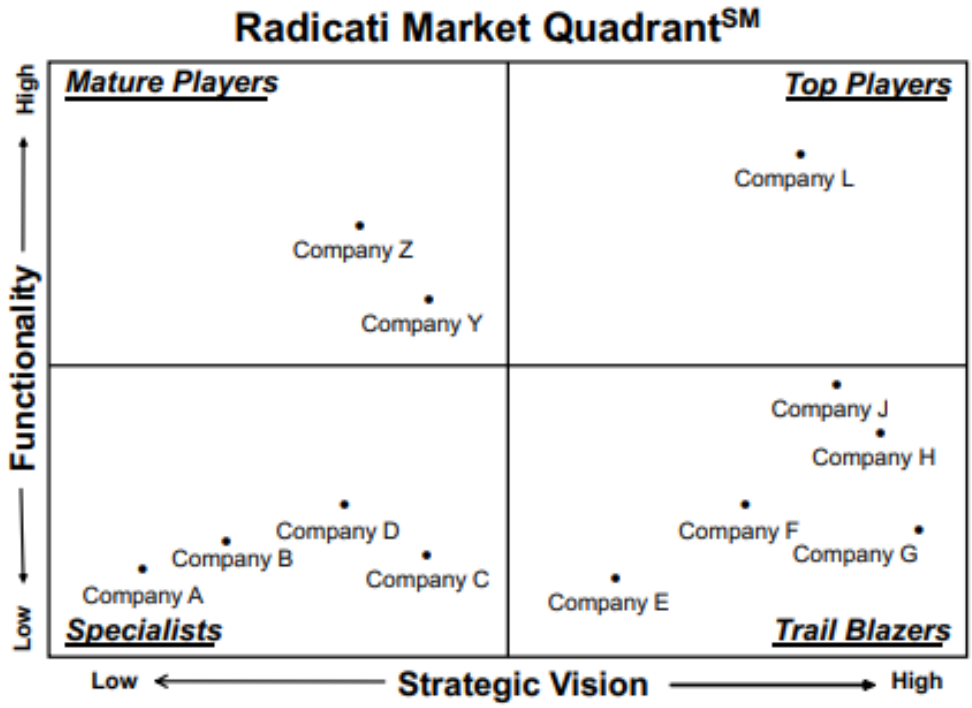
Comparatif des solutions EDR

Les quadrants de marché Radicati permettent de visualiser comment les différents fournisseurs s'inscrivent dans des marchés technologiques spécifiques à un moment donné. Il y a quatre catégories dans ces quadrants:

[2] https://dl.acronis.com/u/rc/White-Paper-Acronis-Cyber-Protect-Endpoint%20Security-Market%20Quadrant-2021-EN-US.pdf

1. Les principaux acteurs qui sont les leaders actuels avec des produits offrant une profondeur et une ampleur de fonctionnalité.
2. Les pionniers qui offrent des technologies avancées mais qui ne sont pas encore considérés comme des principaux acteurs.
3. Les spécialistes qui peuvent être des entreprises émergentes ou établies offrant des solutions très bonnes pour leur clientèle.
4. Les joueurs matures qui sont des entreprises établies qui ont ralenti leur innovation et ne sont plus considérés comme des acteurs importants sur le marché.

Les fournisseurs peuvent se déplacer dans les quadrants au fur et à mesure de l'évolution de leurs produits et des besoins du marché.

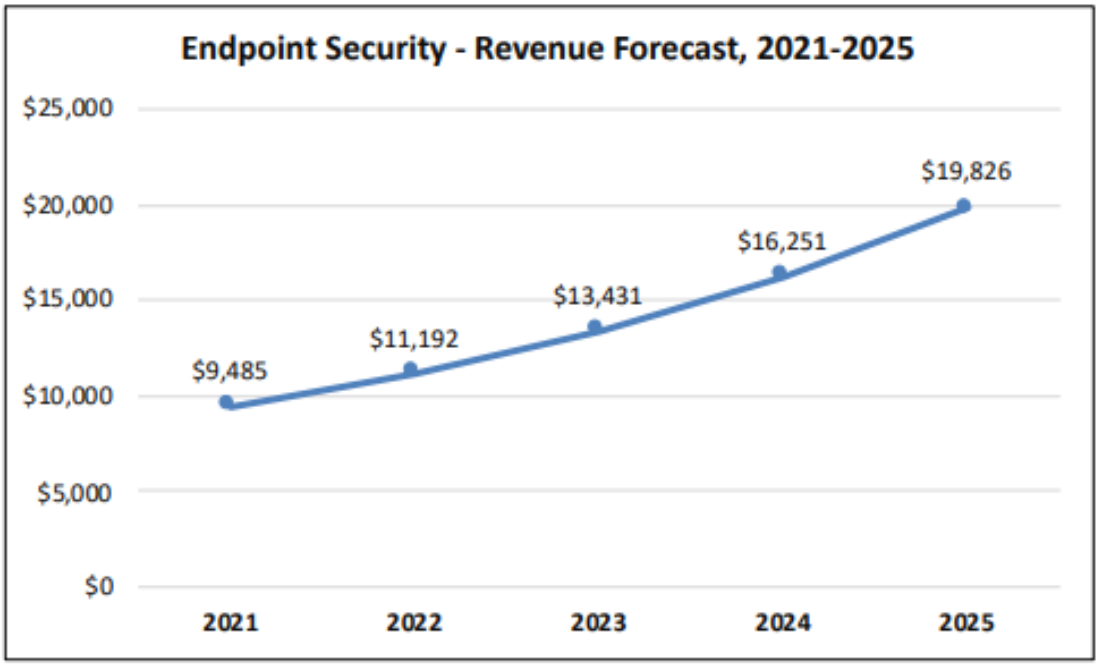


Les principaux acteurs sur ce marché incluent Acronis, Bitdefender, BlackBerry, Cisco, CrowdStrike, Cybereason, ESET, F-Secure, Kaspersky, McAfee, Microsoft, OpenText, SentinelOne, Sophos, Symantec, Trend Micro, VMware et WatchGuard.

Le marché de la sécurité des terminaux continue de connaître une forte croissance car les entreprises de toutes tailles déploient des solutions de plus en plus sophistiquées pour protéger contre toutes les menaces et les attaques malveillantes. Les solutions de sécurité des terminaux sont de plus en plus intégrées dans la stratégie globale de sécurité des entreprises et partagent des informations sur les menaces et les contrôles de politique avec d'autres composants de sécurité tels que les pare-feux, les passerelles web sécurisées, les passerelles de messagerie sécurisées, la prévention de la perte de données ou Data Leak Prevention (DLP) et d'autres.

Le marché de la sécurité des terminaux avait dépassé 9,4 milliards de dollars en 2021 et atteindre plus de 19,8 milliards de dollars en 2025, en raison de la forte croissance prévue dans ce marché.

Nous remarquons également que la distinction entre les solutions traditionnelles et les solutions des endpoints de nouvelle génération existe de moins en moins car presque tous les fournisseurs proposent des solutions comportementales incluant les EDR, MDR, XDR etc …



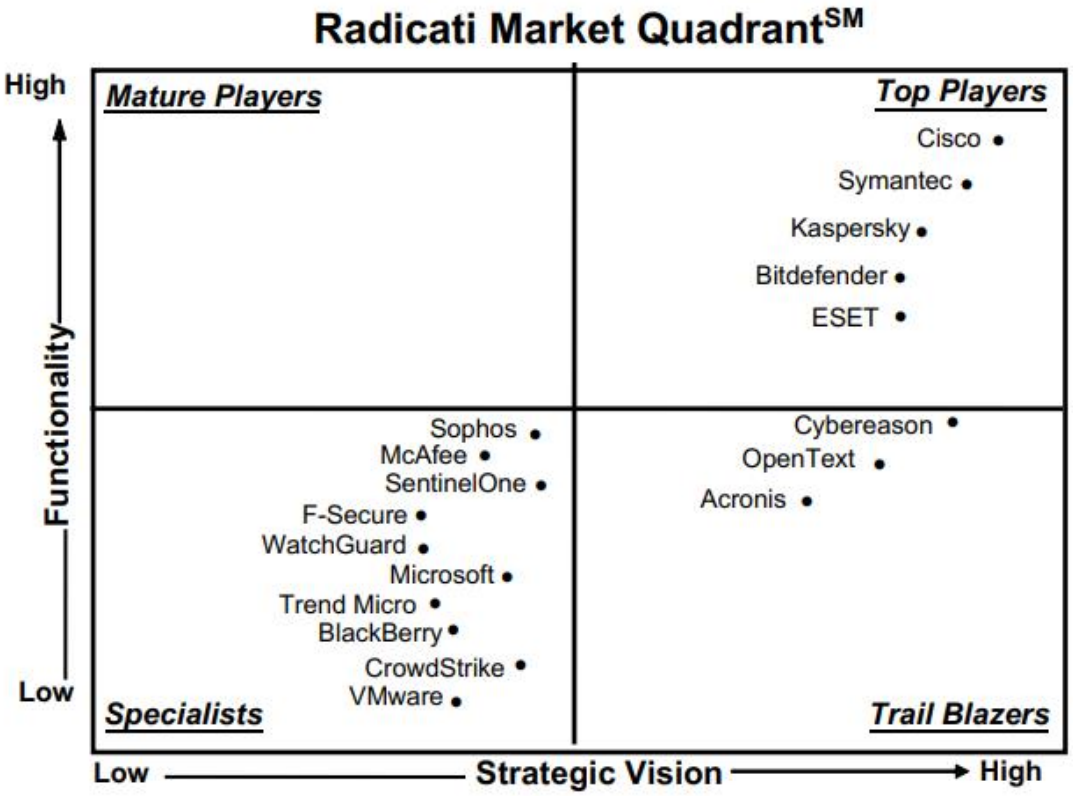
Les fournisseurs sont positionnés dans les quadrants en fonction de deux critères : la **fonctionnalité** et la **vision stratégique**.

- La fonctionnalité est évaluée en fonction de l'étendue et de la profondeur des fonctionnalités de chaque solution de chaque fournisseur. Toutes les fonctionnalités et fonctionnalités ne doivent pas nécessairement être la technologie originale du fournisseur, mais elles doivent être intégrées et disponibles pour le déploiement lors de l'achat de la solution.
- La vision stratégique se réfère à la direction stratégique du fournisseur, qui comprend : une compréhension approfondie des besoins des clients, la capacité à livrer à travers des modèles de prix et de canal attrayants, un support client solide et une innovation continue forte.

Les fournisseurs dans l'espace de sécurité des points finaux sont évalués selon les caractéristiques et les fonctionnalités clés suivantes: les **options de déploiement**, la **prise en charge des plates-formes**, la **détection de logiciels malveillants**, **les outils de suppression d'antivirus**, **l'intégration de répertoire**, **le pare-feu**, **le filtrage d'URL**, **l'évaluation des**

correctifs tiers, **la récupération des correctifs tiers**, **les rapports**, **la sécurité web et email**, **le contrôle des périphériques**, et plus encore.

En outre, pour tous les fournisseurs, ils ont pris en compte les aspects suivants : le prix, le support client, les services professionnels. Le prix, est-il facile à comprendre et permet-il aux clients de budgétiser correctement pour la solution, est-il en adéquation avec le niveau de fonctionnalité proposé et représente-t-il une « bonne valeur » ? Le support client est-il adéquat et en adéquation avec les besoins et les exigences de réponse des clients ? Les services professionnels, le fournisseur fournit-il le bon niveau de services professionnels pour la planification, la conception et le déploiement, soit par le biais de leurs propres équipes internes, soit par le biais de partenaire.



Quel EDR pour quelle entreprise ?

Le choix d'un outil EDR dépend de plusieurs facteurs clés pour une entreprise, notamment la taille de l'entreprise, le niveau de sécurité nécessaire, le coût, la complexité et les fonctionnalités.

Pour les petites entreprises, un EDR abordable et facile à utiliser avec des fonctionnalités de base telles que la détection de menaces, la réponse automatisée pourrait suffire sachant qu'il existe des EDR open source tel que OpenEDR.

Pour les entreprises moyennes à grandes, un EDR plus avancé avec des fonctionnalités supplémentaires telles que les rapports, la sécurité mails, la détection des attaques ciblées et la prévention des attaques en autres peuvent être nécessaires.

Il est également important de considérer le coût de l'EDR et le coût total de possession, y compris les coûts de déploiement, de formation et de maintenance.

Il est recommandé de faire une évaluation approfondie des besoins en matière de sécurité de l'entreprise et de consulter un expert en sécurité pour choisir le bon EDR pour répondre à ces besoins.

En somme, il est très difficile de donner des prix car ces prix varies suivant les types d'entreprises, le service fourni avec le logiciel, les modules activés du logiciel etc….

La géopolitique des EDR

A l'échelle du globe, nous remarquons que les leaders (top players) des solutions EDR sont concentrés aux Etats-Unis et les autres sont ensuite éparpillées ci et là.

Nous avons voulu établir ce constat car géopolitiquement, nous remarquons que l'Europe mais plus précisément la France est loin d'être parmi les pays précurseurs. Cela ne veut pas dire qu'il n'existe pas de service managé en France ou que des solutions n'existent pas.

En effet, nous avons des entreprises telles que CybelAngel ou Vicarius qui offrent des fonctionnalités que l'on pourrait retrouver dans les EDR. Cependant, la plupart des entreprises françaises se concentrent plus sur les services managés et utilisent des solutions classiques telles que Symmantec, Cyberreason pour assurer les fonctions EDR.

Les EDR au centre de la sécurité opérationnelle

La sécurité opérationnelle

La sécurité opérationnelle, également appelée SecOps est un composant clé de la cybersécurité qui concerne les entreprises sur les pratiques (procédure, formation, sensibilisation), les politiques de sécurité et les systèmes mis en place pour protéger le SI (Système d'information) contre d'éventuelles menace. Il s'agit d'un processus continu de gestion de la sécurité, qui vise à minimiser les risques pour les actifs de l'entreprise et à réduire les impacts potentiels des incidents de sécurité afin de renforcer la résilience de l'entreprise face aux menaces.

La sécurité opérationnelle va entrer dans les fonctions du RSSI[3] (responsable de la sécurité des systèmes d'information) de l'entreprise étant chargé de mettre en place des processus de sécurité opérationnelle, comme exprimé dans le livre d'Alexandre Fernandez-Toro « Sécurité opérationnelle conseil et pratiques pour sécuriser le SI ». Des entreprises ont pris le parti pris de faire une équipe SecOps qui travaille étroitement avec l'équipe du RSSI tel que l'entreprise ICDC.

Pour mettre en œuvre une stratégie de sécurité opérationnelle efficace, il est important de travailler en étroite collaboration entre les différentes entités de l'entreprise, les équipes informatiques, les responsables et les employés de l'entreprise. Les politiques de sécurité doivent être claires et bien comprises par tous les employés, tandis que les outils de sécurité doivent être correctement mis en œuvre pour fournir une protection en temps réel contre les menaces.

Dans la SecOps, nous y retrouvons plusieurs objectifs, tels que la surveillance de nouvelles menaces, le contrôle du réseau, la réactivité face aux incidents et l'analyse des incidents.

L'un des aspects les plus importants de la sécurité opérationnelle est la détection et la réponse aux incidents de sécurité. Les équipes de sécurité doivent être en mesure de détecter rapidement les incidents de sécurité et de les gérer efficacement afin de minimiser leur impact. Cela peut inclure la mise en œuvre de système de détection d'intrusion, la création de processus de gestion des incidents et la formation du personnel sur les techniques de réponse aux incidents de sécurité.

La gestion des vulnérabilités est également un élément clé de la sécurité opérationnelle. Les équipes de sécurité doivent être en mesure de détecter les vulnérabilités potentielles dans les systèmes informatiques et les réseaux afin de les corriger rapidement pour minimiser les risques pour l'entreprise. Pour cela, il est possible de mettre en œuvre différent moyen tel que la mise en œuvre de scan de vulnérabilités, la création d'une procédure de gestion de vulnérabilités ainsi que la formation du personnel sur les meilleures pratiques en matière de gestion des vulnérabilités.

[3] Livre d'Alexandre Fernandez-Toro « Sécurité opérationnelle conseil et pratiques pour sécuriser le SI ».

En outre, la sécurité opérationnelle nécessite également la formation du personnel sur les meilleures pratiques en matière de sécurité. Les employés doivent comprendre les politiques de sécurité et les technologies de sécurité mises en place et savoir comment les utiliser de manière sécurisée pour minimiser les risques.

La SecOps en informatique est un élément clé pour la mise en place d'une stratégie de cybersécurité efficace. Cependant, pour garantir une protection complète contre les menaces, il est important de travailler en collaboration avec une équipe de sécurité opérationnelle (SOC, Security Operations Center).

Un SOC est composé d'une équipe qui travaille en collaboration avec les équipes informatiques et les responsables de la sécurité pour surveiller en continu le système d'information de l'entreprise.

Les membres d'un SOC sont chargés de surveiller les menaces en temps réel, de détecter les incidents de sécurité et de coordonner les réponses appropriées. Ils travaillent également en étroite collaboration avec les différentes équipes informatique de l'entreprise pour identifier et corriger les vulnérabilités du système d'information.

Avoir un SOC permet d'offrir une protection en temps réel contre les menaces en ligne, de réduire les risques pour les actifs de l'entreprise et de renforcer la résilience de l'entreprise face aux menaces. De plus, un SOC peut également aider à améliorer les processus de sécurité opérationnelle en identifiant les opportunités d'amélioration et en travaillant en collaboration avec les équipes informatiques et les responsables de la sécurité pour les mettre en œuvre.

La sécurité opérationnelle en informatique est un élément clé pour la mise en place d'une stratégie de cybersécurité efficace. En travaillant en étroite collaboration avec leur SOC, les entreprises peuvent offrir une protection en temps réel contre les menaces et ainsi réduire les risques et renforcer la résilience de leur entreprise face aux menaces.

EDR et SOC

L'Endpoint Detection and Response (EDR) est une solution de cybersécurité essentielle pour les entreprises modernes. Cette solution va s'appliquer à tous les terminaux du système d'information, afin de surveiller en continu les activités pour y détecter les menaces potentielles.

Grâce à l'utilisation d'algorithmes avancés qui va permettre de détecter les comportement et activités suspectes au sein de l'entreprise tels que des logiciels malveillants, des attaques DoS (déni de service), des attaques par phishing et bien d'autres attaque.

Pour pouvoir être exploité à son maximum, l'EDR doit être utilisé par des personnes étant qualifié en cybersécurité pour comprendre et analysé les alertes remontées. C'est donc naturellement que l'on le retrouve au sein d'un SOC pour offrir une protection supplémentaire.

L'intégration de l'EDR dans un SOC peut apporter une valeur significative pour les équipes. En fournissant une visibilité en temps réel sur les activités sur les terminaux, ainsi il peut aider le SOC à détecter les incidents de sécurité plus rapidement et à coordonner des réponses plus efficaces.

De plus, il peut fournir des informations détaillées sur les menaces, telles que la source de la menace, les étapes de propagation et les données compromises, pour aider les SOC à comprendre les menaces et à élaborer des plans de réponse plus efficaces.

Permet de renforcer la capacité du SOC à bloquer les menaces en temps réel grâce à ses techniques de détection et de réponse avancées. En travaillant en collaboration avec les équipes de sécurité informatique, il va permettre d'aider la mise en place de procédure de réponse à incidents afin d'être plus efficaces face aux menaces.

En somme, l'intégration de l'EDR dans un SOC peut renforcer significativement la capacité des équipes à protéger les systèmes informatiques d'une entreprise contre les menaces. L'EDR apporte une visibilité en temps réel sur les activités sur les terminaux, des informations détaillées sur les menaces et une capacité renforcée à bloquer les menaces.

Il offre aussi une plus grande flexibilité et une meilleure collaboration entre les différentes équipes de sécurité informatique. Par exemple, les équipes de sécurité peuvent configurer l'EDR pour collecter des données sur les menaces à partir de différents systèmes et sources, ce qui peut aider à fournir une image plus complète de la menace. Les différents services informatiques de l'entreprise peuvent utiliser les fonctionnalités de collaboration intégrées de l'EDR pour travailler ensemble pour résoudre les incidents de sécurité plus rapidement et efficacement.

Il est important de noter que l'EDR peut aider à améliorer la conformité aux réglementations de sécurité, telles que les lois sur la protection des données personnelles, en fournissant des enregistrements détaillés des activités sur les points de terminaison. Cela peut aider les entreprises à démontrer qu'elles ont mis en place des mesures de sécurité appropriées pour protéger les données sensibles et répondre aux exigences réglementaires.

L'EDR est un élément clé de la stratégie de cybersécurité d'une entreprise. En intégrant l'EDR à un SOC, les entreprises peuvent bénéficier de nouvelles capacités de détection et de réponse aux menaces. Avec une collaboration renforcée entre les différents services. Les entreprises peuvent ainsi renforcer la sécurité de leurs systèmes informatiques et améliorer leur conformité réglementaire en matière de protection des données.

Les limites des EDR

Plusieurs points ont été relevés en rapport aux EDR comme on peut le lire dans l'étude « Tactical Provenance Analysis for Endpoint Detection and Response Systems »[4]

[4] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9152771

Les chercheurs, on définit trois grands défis au sein des EDR :

- Leur premier défié est celui de la « **qualité des données** » qui sont utilisées. Enormément de données son remonté dans les bases de données qui sont optimisées pour rappeler un grand nombre d'événements qui peuvent être liés à une menace, même si ces événements sont couramment utilisés pour des activités inoffensives. Cela peut entraîner de nombreux faux positifs, et donc une "fatigue des alertes" pour les équipes de sécurité qui sont inondées de notifications. Cela peut également rendre difficile la détection des vraies menaces parmi les nombreux faux positifs. Une étude récente a montré que 35% des équipes de sécurité ont du mal à suivre le volume d'alertes, ce qui met les attaques réelles en danger d'être perdues entre les vraies et les faux positifs.[5]
- Le second défi en matière de détection de menaces est « **l'analyse des alertes** ». Les alertes générées peuvent être difficiles à vérifier pour les analystes de cybersécurité, car ils doivent examiner manuellement les journaux système et reconstituer la chaîne d'événements. Cela peut être fastidieux et nécessite de l'expertise. Les systèmes d'informations pour la sécurité (SIEM) peuvent aider les analystes, mais cela reste difficile et requiert toujours de l'expertise.
- Le dernier défi des outils EDR est la « **conservation à long terme des journaux d'événements** ». Les outils actuels ont tendance à supprimer rapidement les journaux ce qui rend difficile pour les analystes de sécurité de mener des enquêtes sur les attaques à long terme. Cette limitation peut être problématique pour les grandes entreprises qui ont besoin d'un contexte à long terme pour comprendre les interdépendances entre les alertes de menace. Cela peut entraver l'analyse causale des menaces, posant ainsi un défi pour les organisations qui cherchent à se protéger contre les attaques à long terme.

Afin de répondre au problème de validation et l'investigation des alertes, les chercheurs sont déjà parvenus à une solution l'analyse sur la provenance des données.

L'analyse de la provenance des données est une technique qui peut être utilisée pour analyser les événements système en utilisant des graphiques pour décrire l'exécution du système et faciliter l'analyse causale des activités. Les progrès récents dans cette technique ont augmenté sa fiabilité et son efficacité pour améliorer le triage des alertes, détecter les intrusions et dériver des corrélations d'alertes. De plus, ces outils d'analyse causale sont souvent basés sur les mêmes flux d'informations utilisés par les outils EDR existants. Au besoin d'approfondir cette piste, je vous invite à vous référer à ce document.

Dans un article de silicon.fr, ils sont posés la question suivante « Pourquoi l'EDR n'est pas suffisant »[6], pour eux les limites de l'EDR ne réside pas dans les défis précèdent relever. Ils

[5] https://pages.siemplify.co/rs/182-SXA-457/images/ESG-Research-Report.pdf
[6] https://www.silicon.fr/avis-expert/pourquoi-ledr-nest-pas-suffisant#

définissent les EDR comme des incontournable pour détecter et remédier à la plupart des menaces de la cybersécurité. « *Les solutions EDR sont devenues incontournables pour détecter et remédier à la plupart des menaces cybersécurité auxquelles les organisations sont confrontées quotidiennement. Véritable outil d'investigation, ce dernier est devenu un pilier des dispositifs de sécurité modernes. Cependant les attaques ont explosé en fréquence et en gravité mettant à mal l'efficacité et les capacités de protection des EDR.* »

Ils vont reprocher aux EDR plusieurs points :

- Ils soulignent que pour pouvoir utiliser pleinement son EDR qu'il est nécessaire avoir un SOC dédié ou bien managé.
- Que les EDR soient basées sur une mentalité de "présomption de violation" et reproche aux outils de « détection et réponse » telles que les EDR, MDR, NDR et XDR d'être basée sur la remédiation post-exécution.

Pour conclure, les EDR vont être un outil incontournable pour répondre à un besoin de détection et de remédiation. L'obtention d'un EDR va impliquer d'avoir un SOC ayant les connaissant et le niveau d'expertise suffisant afin d'exploité les alertes et données remontées, ainsi qu'un système de type SIEM afin d'améliorer l'analyse et la conservation des journaux d'événement sur le long terme. On peut reprocher aux solutions dites « détection et réponse » d'être basé sur la remédiation post-exécution.

Vers un futur en XDR ?

Nous avons remarqué lors de nos recherches que sur les EDRs plusieurs autres termes remonte tels que MDR, XDR.

MDR correspond à Managed Detection and Response, c'est une solution managée du service de détection et réponse aux incidents. Les opérations sont supervisées par un Centre de Sécurité des Opérations, qui peut être interne ou externalisé.

XDR tant qu'à lui correspond à Extended Dection and Response, ont facilement trouver dans de différents articles que cela est évolution des EDR, dans une première partie nous allons se poser la question de qu'est-ce qu'un XDR ? En second temps de ce qu'elles sont les différences d'un XDR vs un EDR ? Puis nous finirions par se poser la question suivant l'XDR est-il vraiment le futur ?

Qu'est-ce qu'un XDR

Mais qu'est-ce que bien être un XDR (Extended Dection and Response XDR), après quelques recherches, on peut y trouver plusieurs définition.

Microsoft défini l'EDR de la manière suivante :

« *Le terme 'détection et réponse étendues' (XDR), quant à lui, désigne un outil SaaS qui offre une sécurité globale et optimisée en intégrant des produits et des données de sécurité dans*

des solutions simplifiées. Alors que les entreprises sont confrontées à des menaces en constante évolution et à des défis complexes en matière de sécurité, avec des effectifs dans des environnements multiclouds hybrides, la sécurité XDR constitue une solution plus efficace et proactive. Contrairement à des systèmes tels que la protection évolutive des points de terminaison (PEPT), XDR élargit le champ de la sécurité d'une organisation, en intégrant la protection à un plus grand nombre de ses produits, comme les points de terminaison, les serveurs, les applications cloud, le courrier et autres. À partir de là, XDR combine prévention, détection, enquête et réponse, en fournissant une visibilité, des analyses, des alertes corrélées sur les incidents et des réponses automatisées pour améliorer la sécurité des données et combattre les menaces. » [7]

Orange CyberDéfense le définie de la façon suivante :

« *Les solutions XDR permettent de démocratiser les outils de détection. En SaaS, elles permettent de regrouper des données provenant de différentes sources du système d'information et de les relier entre elles, afin de se protéger et de répondre au mieux lors de cyberattaques. Le XDR ne surveille pas seulement les Endpoints, mais aussi les emails, serveurs et le Cloud. En augmentant les capacités de détection, le XDR permet une réaction rapide aux menaces, en amont de la kill chain, limitant nettement les dégâts. Le XDR surveille en continu et de manière proactive pour alerter rapidement en cas de suspicion d'attaque.* »[8]

D'après c'est deux définitions, nous pouvons définir un XDR de la manière suivante :

« *Un XDR est une solution détection et de réponse étendue proposé sous le format SaaS (software as a service) est une solution plus performante et proactive, elle intègre la protection de nombreux points en collectant et en mettant en corrélations les données des terminaux, des réseaux, des applications cloud, messagerie et bien d'autres afin d'être le plus efficient pour détecter les menaces.* »

En somme, les XDR sont des systèmes de détection et de réponse à la sécurité qui collectent les alertes en provenance de sources multiples et les mettent en corrélation pour offrir une image complète d'un incident ou d'une attaque de sécurité.

Les analyses robustes de ces systèmes aident les analystes à comprendre l'activité des menaces et à les détecter plus facilement. Les systèmes XDR procèdent automatiquement et en temps réel à l'identification, à l'évaluation et à la correction des menaces connues, réduisant ainsi la charge de travail des organisations.

L'IA et le Machine Learning sont utilisés pour accroître la scalabilité et l'efficacité. En cas de ressources affectées, le système XDR peut automatiquement appliquer des mesures correctives pour arrêter les processus malveillants, supprimer les règles de transfert malveillantes et identifier les utilisateurs compromis.

[7] https://www.microsoft.com/fr-fr/security/business/security-101/what-is-xdr

[8] https://www.orangecyberdefense.com/fr/insights/blog/detection/soc-siem-xdr-mdr-edr-quelles-differences

XDR vs EDR

Les EDR et les XDR sont deux concepts importants en matière de cybersécurité qui ont émergé récemment. Bien qu'ils semblent similaires, il existe des différences importantes entre les deux et il est important de comprendre chacun d'entre eux pour choisir la bonne solution pour votre entreprise.

L'EDR est une solution de cybersécurité qui vise à détecter et à répondre aux menaces sur les terminaux, tels que les ordinateurs de bureau, les ordinateurs portables et les appareils mobiles. Il utilise la télémétrie provenant des agents installés sur ces appareils pour fournir une visibilité sur les activités suspectes et pour prendre des mesures pour éliminer les menaces.

L'XDR est une évolution de l'EDR qui vise à étendre la couverture de la détection et de la réponse aux menaces pour inclure d'autres points d'entrée dans l'infrastructure de l'entreprise, tels que le réseau, la messagerie, le cloud et bien d'autre. Cette vue complète permet aux solutions XDR de détecter les menaces plus rapidement et de manière plus précise que les solutions EDR seules. De plus, les solutions XDR peuvent également automatiser la réponse aux menaces, de sorte que les actions correctives soient entreprises plus rapidement et de manière plus efficace.

En d'autres termes, l'XDR est conçu pour fournir une protection plus complète et plus intégrée contre les menaces de sécurité en unifiant les données provenant de différents outils de sécurité et en utilisant une infrastructure Big Data pour améliorer la flexibilité, l'évolutivité et les opportunités d'automatisation.

En comparant EDR et XDR, il est important de noter que l'EDR est encore un composant important de la stratégie de sécurité de l'entreprise, mais l'XDR offre une couverture plus complète et une réponse plus coordonnée aux menaces. De plus, en utilisant une plateforme cloud native, l'XDR peut également offrir des avantages supplémentaires en termes de coûts, de scalabilité et d'efficacité opérationnelle.

L'XDR est-il vraiment le futur ?

L'EDR et l'XDR ont tous les deux leur place dans les stratégies de sécurité des entreprises. Si vous avez déjà une stratégie de sécurité bien établie et que vous voulez simplement améliorer la détection et la réponse aux menaces sur les terminaux, une solution EDR peut être suffisante.

Cependant, si vous cherchez à améliorer la sécurité de l'entreprise dans son ensemble, une solution XDR peut être une meilleure option. Les solutions XDR permettent une vue complète de la sécurité de l'entreprise, ce qui signifie que les menaces peuvent être détectées plus

rapidement et de manière plus précise, et que les réponses peuvent être plus rapides et plus efficaces.

En conclusion, EDR et XDR sont tous deux des solutions importantes pour la sécurité informatique qui aident les entreprises à se protéger contre les menaces complexes. EDR est une solution axée sur l'analyse des comportements pour détecter les attaques, tandis que XDR utilise une approche plus large en combinant plusieurs technologies de sécurité pour une protection complète. Les deux technologies ont leurs avantages et inconvénients et peuvent être utilisées conjointement pour une protection optimale.

Outil : Scraper EDR

Dans le cadre de notre étude de l'art, il nous a été demandé de réaliser un scraper après réflexion, nous avons décidé de partir sur un scraper permettant d'obtenir les CVE afin d'établir plusieurs graphiques ainsi qu'un ranking.

Lors du scraping, nous collectons les données suivantes :

- Nom solution
- Numéro CVE
- CVE ID
- Type de vulnérabilité
- Date de publication
- Date de patch
- Score

A partir ces données, notre solution permet d'afficher plusieurs graphes qui représentent :

- La gravité moyenne des CVE par solution,
- Le délai avant la sortie du patch en moyenne par solution,
- Nombre de CVE par solution,
- Et le ranking des solutions.

Indicateurs Ranking

Pour établir notre ranking, nous avons dû se baser sur trois indicateurs en rapport aux CVE des solutions qui sont les suivants :

- La gravité moyenne des CVE,
- Le délai moyen avant la sortie du patch,
- Et le nombre de CVE.

Système d'évaluation du ranking

Notre ranking vas attribuer une note allant de 0 à 10 pour chaque solution sélectionnée en se basant sur les indicateurs cités plus haut.

Les différents indicateurs n'ont pas la même pondération pour la note attribuée :

- L'indicateur de la gravité moyenne des CVE va compter pour 4 points. Pour qu'une solution ait la note maximale, elle devra avoir une moyenne à 0 de gravité.
- L'indicateur de délai moyen avant la sortie du patch va compter pour 5 points. Afin d'obtenir 5 points, la solution devra avoir patcher en moyenne la CVE dans la journée qui suit. Une solution obtiendra 0 point dès lors qu'elle dépassera 21 jours de moyenne de patch. Nous avons établi la limite de 21 jours en se basant sur la médiane du dwell time. Le dwell time représente la durée pendant laquelle un cyberattaquant a le champ libre, depuis le moment où il est entré au moment où il est éradiqué.
- Et pour finir, l'indicateur du nombre de CVE moyen va permettre d'attribuer le dernier point manquant. Afin d'attribué ce dernier point nous allons ce basé sur l'EDR ayant le plus de CVE et celui ayant le moins. Puis avec un produit en crois nous attribuons les points aux autres solutions.

Le total des points obtenu établira l'ordre des solutions de notre ranking.

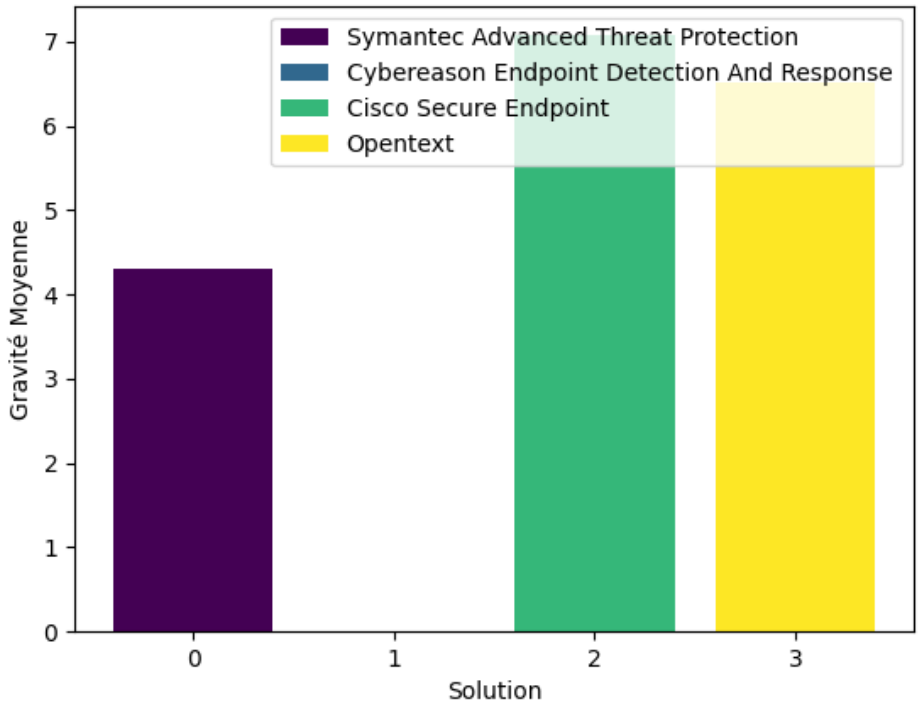
Résultat du ranking

Dans l'exemple qui suit, nous avons considéré 4 solutions EDR

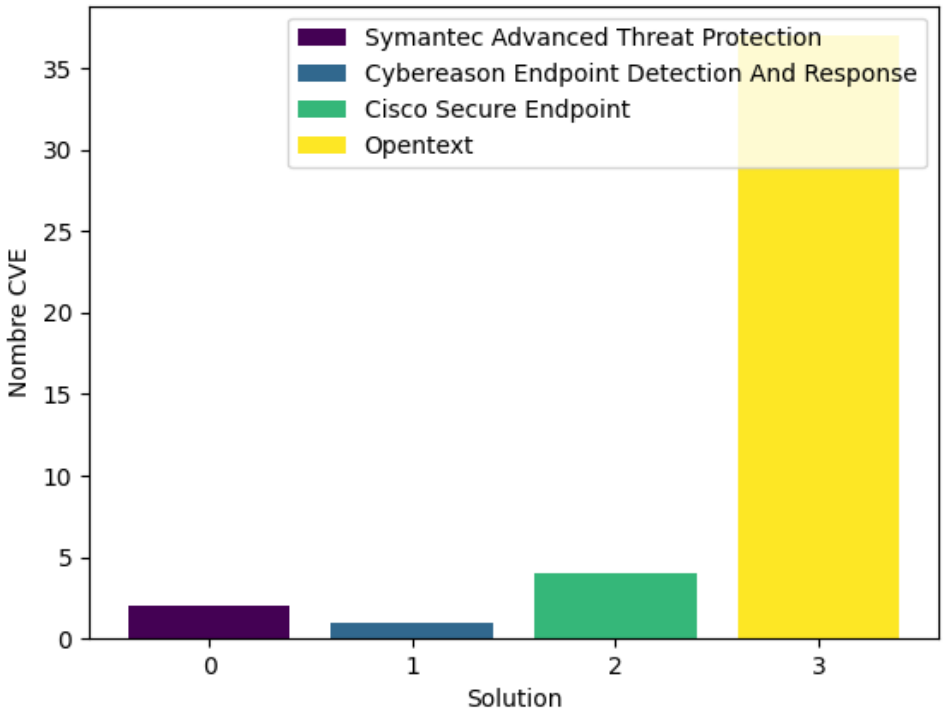
- Symmantec,
- Cybereason,
- Cisco,
- Opentext.

Chaque solution a les caractéristiques suivantes :

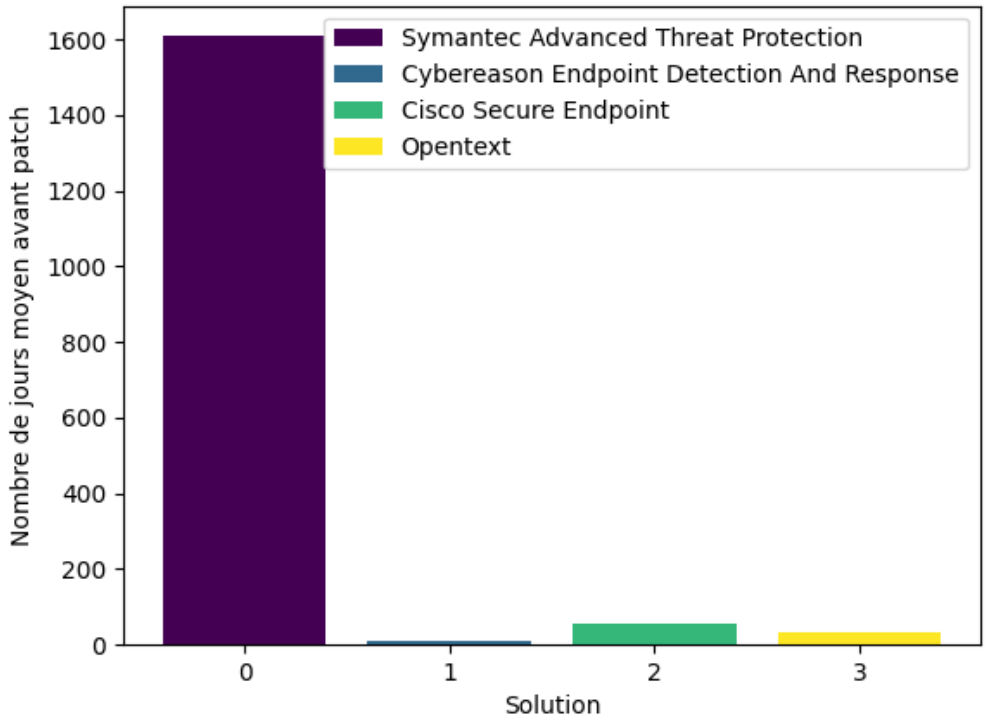
- Gravité moyenne



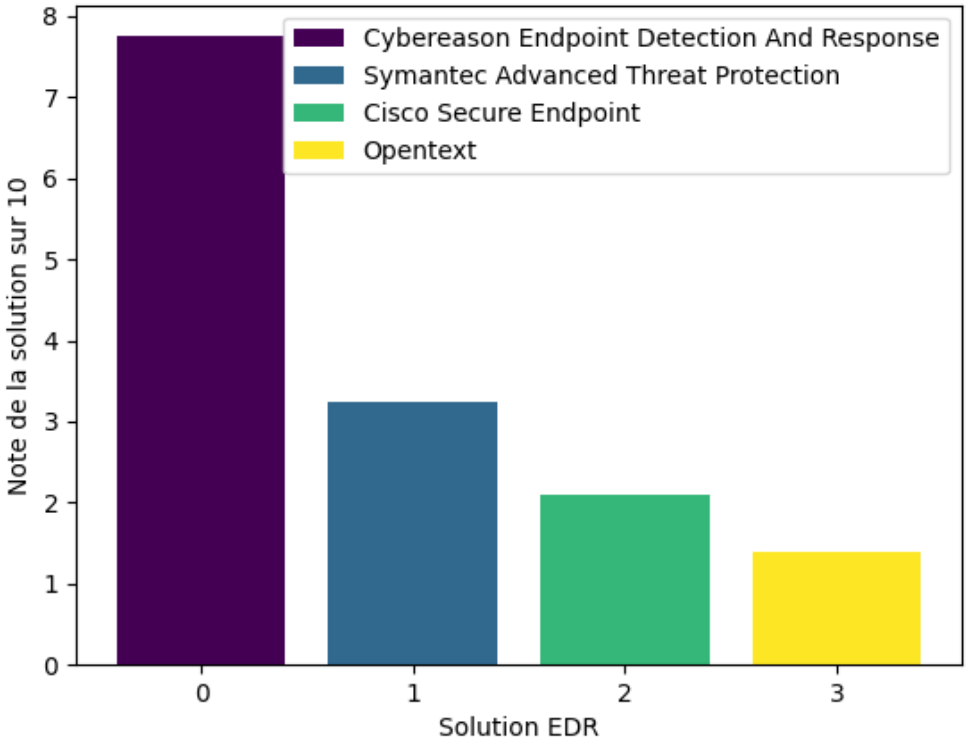
- Nombre de CVEs



- Délai moyen avant patch



En prenant tout cela en compte, nous obetenu le résultat suivant :



En effet, Cyberreason est très bien noté, car cette solution n'a qu'un seul CVE de gravité nulle tandis qu'Opentext est une solution sur laquelle il y a 37 CVEs répertoriés de gravité moyenne à 6.5.

Notre outil est à prendre avec précaution car en réalité, les solutions sans CVE ne sont pas systématiquement les meilleures mais on peut l'utiliser comme critère supplémentaire à la prise de décision entre plusieurs solutions envisagées d'autant plus que cela prend en compte le temps de patch en cas de vulnérabilité détectée.

Conclusion

Les EDR (Endpoint Detection and Response) sont des outils de sécurité opérationnelle de plus en plus populaires pour les entreprises de toutes tailles. Ils permettent de surveiller les activités sur les terminaux, détecter les menaces et répondre rapidement pour minimiser les dommages potentiels. Les EDR peuvent être utilisés conjointement avec d'autres solutions de sécurité pour renforcer la sécurité globale d'une entreprise. Cependant, il est important de choisir un EDR adapté à la taille et aux besoins de l'entreprise, ainsi que de le maintenir à jour pour garantir une protection maximale. Il faut noter qu'il est indispensable d'avoir une équipe sécurité qui aura le temps d'analyser les alertes et de s'occuper de la solution afin d'optimiser son efficacité, en cas contraire, il ne sera d'aucune utilité. En fin de compte, les EDR peuvent être un investissement rentable pour les entreprises soucieuses de leur sécurité numérique en aidant les entreprises à minimiser les impacts financiers, réputationnels et opérationnels causés par les incidents de sécurité. Enfin, les entreprises doivent s'assurer qu'elles disposent d'une solution de sécurité EDR appropriée pour garantir leur protection.

Liens des ressources

Repositories Github des codes [2] :

https://github.com/MesminN/Endpoint_Detection_Response

Lien drive d'une vidéo démo du scrapper:

https://drive.google.com/file/d/1jiVyEZT02mLYWgWImqG_GSm86ohm6A7J/view?usp=share_link