

Etat de l’art et intelligence économique du marché des EDR

**Membres du groupe**

Mesmin NGOULO BEMBE

Corentin VIEILLESCAZES

**Responsable**

Nicolas BLOUMINE

Table des matières

[Introduction 4](#_Toc126926995)

[Les EDR : la genèse 4](#_Toc126926996)

[La problématique qu’adressent les EDR 4](#_Toc126926997)

[Détection lors d’une attaque : framework d’attaques vs EDR 4](#_Toc126926998)

[Les fonctionnalités fondamentales d’un EDR 4](#_Toc126926999)

[Le marché des EDR 4](#_Toc126927000)

[Comparatif des solutions EDR 4](#_Toc126927001)

[Quel EDR pour quelle entreprise ? 4](#_Toc126927002)

[La géopolitique des EDR 4](#_Toc126927003)

[Les EDR au centre de la sécurité opérationnelle 4](#_Toc126927004)

[La sécurité opérationnelle 4](#_Toc126927005)

[EDR et SOC 4](#_Toc126927006)

[Les limites des EDR 4](#_Toc126927007)

[Vers un futur en XDR ? 4](#_Toc126927008)

[Qu’est-ce qu’un XDR 4](#_Toc126927009)

[XDR vs EDR 4](#_Toc126927010)

[L’XDR est-il vraiment le futur ? 4](#_Toc126927011)

[Conclusion 4](#_Toc126927012)

[Annexes 4](#_Toc126927013)

[Bibliographie 4](#_Toc126927014)

[Liens des ressources 4](#_Toc126927015)

# 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 leur 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]](#footnote-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.

Les EDR vont plus loin dans la protection et fournissent une surveillance continue et répond 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 développé 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 com 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 rendus compte que les outils classiques ne suffisaient plus d’où l’entrée sur le marché des EDR.

## Les fonctionnalités fondamentales d’un EDR

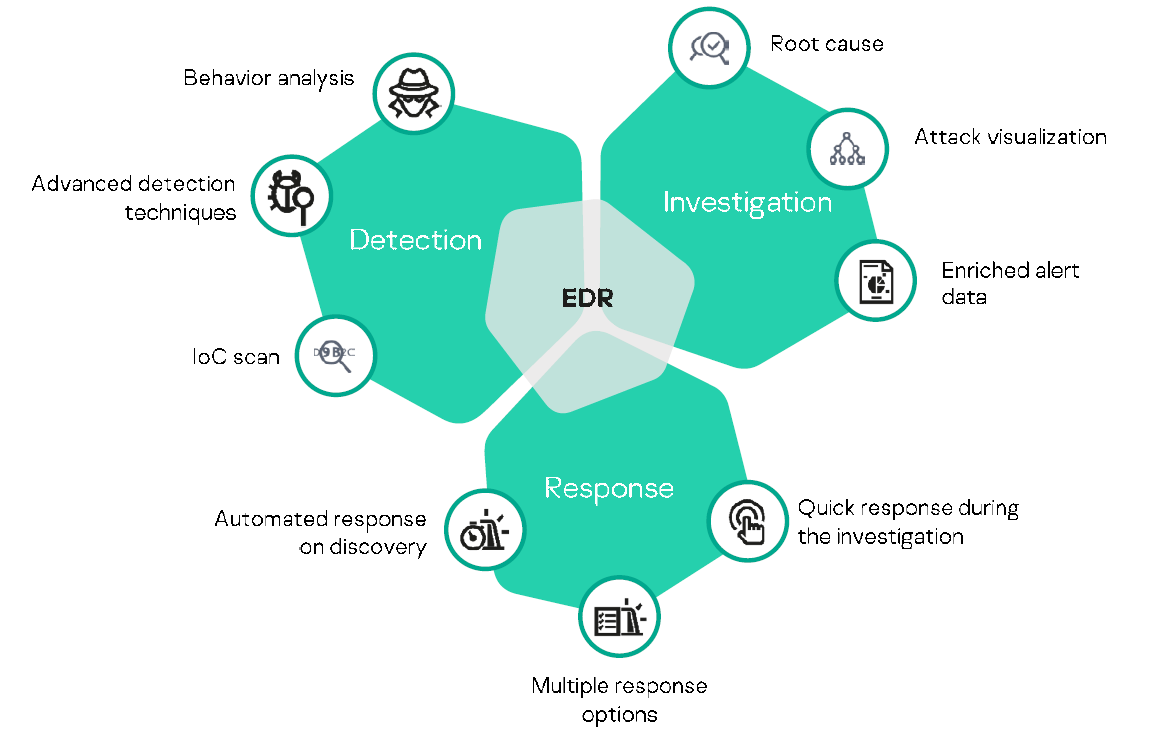
Avant les années 2010s, les entreprises embauchaient des équipes de réponse à incidents pour investiguer les failles de sécurité. En 2013, le plus fiable était Mandiant qui fournissaient des professionnels en sécurité en cas d’incident et cela n’était pas gratuit.

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 malvaillants.
* 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

# Le marché des EDR

## Comparatif des solutions EDR

## Quel EDR pour quelle entreprise ?

## La géopolitique des EDR

# Les EDR au centre de la sécurité opérationnelle

## La sécurité opérationnelle

La sécurité opérationnelle, également appelé SecOps est un composant clé de la cybersécurité qui concerne les entreprises sur ces pratiques (procédure, formation, sensibilisation), ces politiques de sécurité et les systèmes mis en place pour protéger le SI (Système d’information) contre d’éventuelle 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[[2]](#footnote-2) (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 mises en œuvre pour fournir une protection en temps réel contre les menaces.

Dans la SecOps nous y retrouvons plusieurs objectifs, tel 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.

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 travaillent 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 remonté. 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 également 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 également 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 a 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 peut également offrir 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 également 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 relevé en rapport aux EDR comme on peut le lire dans l’étude « Tactical Provenance Analysis for Endpoint Detection and Response Systems »[[3]](#footnote-3)

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.[[4]](#footnote-4)
* 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 »[[5]](#footnote-5), pour eux les limites de l’EDR ne réside pas dans les défis précèdent relever. Ils 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 point :

* 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 remonté avec l’EDR, 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 ?

## Qu’est-ce qu’un XDR

## XDR vs EDR

## L’XDR est-il vraiment le futur ?

# Conclusion

# Annexes

# Bibliographie

# Liens des ressources

Repositories Github des codes source :

Scrapper:

Lien drive d’une vidéo démo du scrapper:

1. Evaluation Criteria for Endpoint Protection Platforms”, Gartner, Inc. Mario de Boer. March 24, 2015 [↑](#footnote-ref-1)
2. livre d’Alexandre Fernandez-Toro « Sécurité opérationnelle conseil et pratiques pour sécuriser le SI ». [↑](#footnote-ref-2)
3. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9152771> [↑](#footnote-ref-3)
4. <https://pages.siemplify.co/rs/182-SXA-457/images/ESG-Research-Report.pdf> [↑](#footnote-ref-4)
5. [https://www.silicon.fr/avis-expert/pourquoi-ledr-nest-pas-suffisant#](https://www.silicon.fr/avis-expert/pourquoi-ledr-nest-pas-suffisant) [↑](#footnote-ref-5)