

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

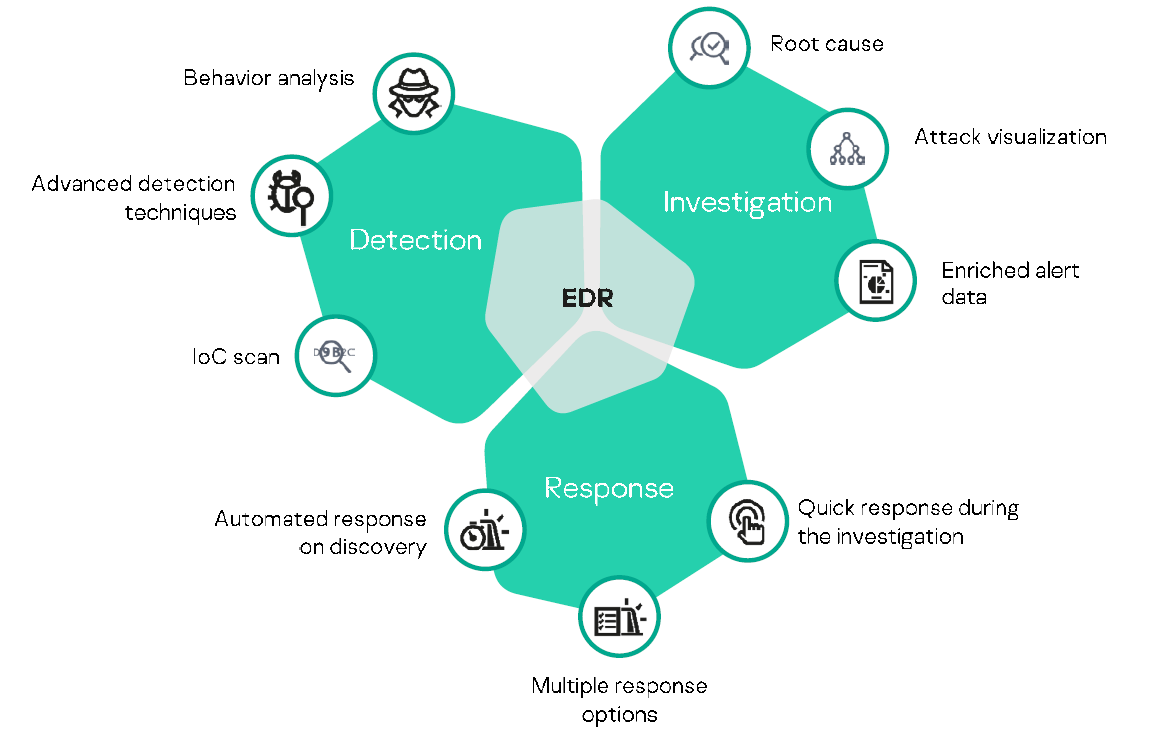
Avant les années 2010s, les entreprises embauchaient des équipes de réponse à incidents pour investiguer les failles de sécurité. En 2013, le plus fiable était Mandiant qui fournissaient des professionnels en sécurité en cas d’incident et cela n’était pas gratuit.

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

## EDR et SOC

## Les limites des EDR

# 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)