Veille sur les EDR

Qu’est-ce qu’un EDR ? Endpoint Detection and Response C’est une catégorie de solutions qui se met en place sur des terminaux d’une organisation par les administrateurs réseau et qui va détecter les activités suspectes de façon poussée.

Comment cela fonctionne ? On peut comparer l’edr a une boite noire d’un avion, il va récupérer des informations sur les journaux d’évènements, les applications lancées et les tentatives de connexion par exemple. Puis avec les données collectées il va apprendre comment le poste est utilisé puis réagir en cas de comportement inhabituel. En cas de relevé anormal, l’activité va être analysée par la plateforme de l’EDR ou alors par un système automatisé qui va être capable de réagir avec force face à une menace, en mettant le poste en quarantaine afin qu’il ne contamine pas le réseau de l’organisation comme avec un ransomware pour lesquelles ils sont réputés efficace.

Malgré tout il réside quelques points d’amélioration comme certaines attaques qui passe entre les mailles du filet qui peuvent être dissimulées sous des logiciels ou comportement invisible aux yeux des EDR. Un autre axe d’amélioration intervient aussi dans les faux positifs, comme la solution est aussi basée sur de l’IA il y a des risques d’erreur ce qui peut donc être contreproductif pour les équipes de sécurités.

Dans l’avenir cette solution va continuer d’évoluer ce qui va la rendre encore plus efficace en prévenant des attaques avant qu’elles ne se produisent, mais il ne faut pas oublier qu'en contrepartie les logiciels malveillants ont de nouvelles perspectives d’évolution.

Pour conclure, les EDR deviennent des outils de plus en plus indispensables pour les organisations, en restant à jour et avec les dernières avancées, ils permettent de détecter les attaques mais aussi de réagir avant qu’une attaque cause des dégâts majeurs dans une organisation. Cependant, comme pour beaucoup de technologie son efficacité dépend de sa configuration et de l’intégration dans un parc qui possède potentiellement un système de sécurité.

Blogorama

Varonis

Itrnews

Einpresswire

Cybersécurité / Périmètre : EDR (Endpoint Detection and Response)