Du bon usage d'un EDR

EDR est l'acronyme de "Endpoint Detection and Response", qui peut être traduit en français par "Détection et Réponse aux Menaces sur les Terminaux".

Il s'agit d'une technologie de cybersécurité qui permet de surveiller les terminaux (ordinateurs, serveurs, téléphones mobiles, etc.) afin de détecter et bloquer des activités suspectes ou malveillantes telles que l'exécution de logiciels malveillants, des exfiltrations de données, des tentatives d'exploitation de vulnérabilités, etc. L'EDR agit comme un complément (et non en remplacement) de l'antivirus. Là où l'antivirus va détecter des fichiers connus comme malveillants, l'EDR va se concentrer sur les comportements suspects. Il fournit des alertes et des rapports détaillés pour permettre aux équipes de sécurité de prendre des mesures de réponse rapides et efficaces.

Fonctionnement d'un EDR

Le fonctionnement technique de l'EDR peut être résumé en plusieurs étapes clés :

- Collecte de données : L'EDR collecte des données à partir des terminaux surveillés, telles que les fichiers créés ou modifiés, les processus en cours d'exécution, les connexions réseau, les journaux d'événements, etc.
- Analyse des données : Les données collectées sont analysées en temps réel à l'aide d'algorithmes avancés pour détecter les comportements suspects et les menaces potentielles. Cette analyse peut être effectuée sur les terminaux eux-mêmes ou sur un serveur centralisé.
- Détection des menaces : En fonction des règles de détection et des algorithmes utilisés, l'EDR peut détecter une variété de menaces, telles que les attaques de logiciels malveillants, les exfiltrations de données, les tentatives d'exploitation de vulnérabilités, etc. Il peut également servir à rechercher des indicateurs de compromission à la demande.
- Alertes et rapports : Lorsqu'une activité malveillante est détectée, l'EDR peut fournir des alertes et des rapports détaillés aux équipes de sécurité pour leur permettre de prendre des mesures correctives immédiates.
- Réponse automatisée : En cas d'événement relatif à la sécurité, l'EDR peut automatiser certaines actions de réponse, telles que la mise en quarantaine des fichiers infectés ou la désactivation des processus malveillants. Dans certains cas, il va même jusqu'au confinement réseau du poste.

Dépendances et limites d'un EDR

- Dépendance des données : l'EDR repose sur la collecte et l'analyse de données provenant de terminaux surveillés. Si ces données ne sont pas fiables, si les terminaux ne sont pas correctement configurés ou si la connexion entre les terminaux et le serveur de collecte est interrompue, l'EDR ne sera pas en mesure de détecter l'ensemble des activités malveillantes les concernant.
- Faux positifs : l'EDR peut générer des alertes pour des activités qui s'avèrent être légitimes et entraîner une charge de travail supplémentaire pour les équipes de sécurité, qui doivent examiner chaque alerte pour déterminer si elle représente une réelle menace. **Une première période d'apprentissage et « de réglage » est donc indispensable** après le déploiement et **nécessite une grande interaction** entre les équipes en charge de la surveillance et la DSI de l'établissement pour légitimer les actions courantes. **Cette période peut durer de 2 à 6 mois** et doit être évalué avant le lancement du projet.

Point de vigilance : en installant un EDR, l'établissement de santé augmente sa surface d'attaque. Il introduit un outil ayant des droits SI hautement privilégiés qui pourraient permettre à un attaquant de prendre le contrôle du SI dans le cas où il disposerait d'un accès administrateur à la console suite à la compromission du service (vulnérabilité, vols d'identifiants, etc.).

Coût et complexité : Une solution EDR peut être coûteuse et complexe à déployer et à gérer. Elle nécessite des compétences techniques spécialisées et peut être difficile à intégrer (voir impossible en raison d'incompatibilités techniques par exemple) avec des technologies existantes.

Du bon usage d'un EDR

Quand installer un EDR ?

- La sécurité du SI doit faire l'objet d'une attention particulière avant toute installation d'un EDR (application des mesures d'hygiène informatique) ; sa mise en œuvre doit être intégrée dans un plan global de renforcement de la sécurité, mais ne doit pas remplacer les mesures de durcissement concernant les dimensions les plus critiques du SI (sécurité des sauvegardes, des systèmes socles (hyperviseurs, Active Directory), administration, etc.). Ces mesures sont complémentaires et permettent d'accroître l'efficacité des alertes remontées par l'EDR.
- Dans un environnement Microsoft Active Directory, il est recommandé d'installer un EDR lorsque cet environnement a atteint un niveau de sécurité acceptable, c'est-à-dire en ayant obtenu idéalement un score minimal de 3 suite à un audit ORADAD ou suite à un audit Pingcastle montrant un niveau de sécurité « satisfaisant ». Les dépenses et efforts humains seront plus efficients dans des travaux d'amélioration de la sécurité de l'AD, en suivant les recommandations énoncées dans le rapport délivré par l'un de ces services plutôt que dans l'installation d'un nouvel outil.
- L'EDR n'est vraiment efficace que s'il y a une intervention humaine rapide en cas de détection. Il est donc important de mettre en place une capacité humaine d'analyse et d'action sur les alertes.

L'EDR ne doit pas être déployé dans le cadre d'une réponse à un incident comme un outil de supervision de circonstance et d'aide au retour de l'activité à la normale ; en effet il faut une période de réglages (levée des faux-positifs), souvent assez longue, pour qu'il soit réellement efficace.

Lorsqu'un prestataire souhaite déployer un EDR dans le cadre de sa prestation, le contrat doit prévoir une clause détaillant une procédure ou l'assistance en vue de son retrait éventuel du SI. Cette procédure doit être écrite, et mise en place par le prestataire de sécurité dès l'installation de la solution.

Conseils pour une mise en œuvre sécurisée d'un EDR

- **Ne pas exposer l'interface de la console** à tout Internet et mettre en place un filtrage restrictif
- Gérer la granularité des droits :
  - Les **analystes** doivent avoir des **droits de consultation** étendus (pas d'actions) ;
  - **Seul des superviseurs** doivent pouvoir réaliser des actions sur le parc de leurs clients
  - N'utiliser le compte admin racine que dans **certains cas précis** (création d'utilisateurs, modification des règles d'actions automatisées, création de groupes de droits, etc.)
- Obliger tous les acteurs à utiliser le MFA **par défaut**
- **Superviser régulièrement la console** afin de s'assurer de la qualification des alertes remontées
- **Former les agents** qui vont participer au traitement des alertes
- **Réaliser un déploiement couvrant le plus grand nombre possible de machines** sur le SI
- **Adopter une démarche itérative et régulière de levée des faux positifs** (à mettre en place avant le lancement du projet)