CENTRE FOR
CYBER SECURITY
BELGIUM

Recommandations pour les solutions de sécurité de type anti-virus, EDR et XDR

août 2022

Table des matières

Sommaire

Dans le contexte actuel, une stratégie de défense en profondeur est nécessaire et les organisations doivent se préparer de manière adéquate. Cela comprend de nombreux aspects tels que des politiques et procédures appropriées, la formation (sensibilisation) des utilisateurs finaux, des processus de gestion des vulnérabilités, une bonne gestion des configurations, des pares-feux (locaux), des protections des applications Web (WAF), des systèmes de gestion des informations et des événements de sécurité (SIEM), des systèmes de détection des intrusions (IDS), une segmentation adéquate du réseau, la gestion des appareils mobiles, etc.

Le déploiement et la gestion d'un antivirus, d'un **EDR** (*endpoint detection and response*) et même d'un **XDR** (*extended endpoint detection and response*) font partie de la solution requise pour atteindre cet objectif.

Le présent document fournit des lignes directrices pour les critères généraux, pragmatiques et techniques génériques, de même que quelques références pertinentes pour les solutions de sécurité **Antivirus**, EDR et XDR.

Nous avons défini trois niveaux dans cette approche : le **niveau 1** (Basic) fait référence à la protection antivirus, le **niveau 2** (substantial) à l'EDR et le **niveau 3** (advanced) à l'XDR.

Si votre organisation dispose déjà d'une solution de sécurité de base, des licences supplémentaires pourraient vous permettre d'évoluer vers les capacités conseillées d'une solution d'EDR (voir niveau 2).

Quelques définitions

Antivirus (niveau 1, Basic protection) : Applications qui analysent (en temps réel/à l'accès ou programmées à un intervalle) les fichiers, sur la base de signatures ou d'heuristiques. Elles sont idéales pour détecter les logiciels malveillants connus.

EDR - Endpoint Detection and Response (Niveau 2, substantial protection) : Il s'agit d'une solution de nouvelle génération qui intègre généralement des scanners antivirus, mais qui ajoute des fonctionnalités supplémentaires comme une gestion centralisée, de la corrélation, et l'interprétation des événements.

XDR - eXtended Detection and Response (niveau 3, advanced protection) : Elle augmente les capacités d'une ou plusieurs solutions EDR dans un environnement inter-domaines en ajoutant des sources de corrélation supplémentaires mais aussi des fonctionnalités additionnelles.

Niveau 1, Basic Protection : Antivirus (également appelé *Anti-malware*)

Solution apportée :

L'approche traditionnelle a toujours été l'utilisation d'un antivirus comme solution de protection des systèmes. Les scanners étaient les outils les plus efficaces, reposant principalement sur les signatures et l'heuristique. Aujourd'hui, les scanners antivirus restent le contrôle technique le plus utilisé pour l'atténuation des menaces liées aux logiciels malveillants. Voir également l'excellente publication du NIST.gov sur les outils de lutte contre les logiciels malveillants. (1)

Capacités minimales importantes pour un logiciel antivirus (1):

- Analyser les composants critiques de l'hôte tels que les fichiers de démarrage et les registres de démarrage ;
- Effectuer des analyses en temps réel de chaque fichier lorsqu'il est téléchargé, ouvert, ou exécuté (analyse à l'accès);
- Surveiller le comportement des applications courantes, comme les clients de messagerie, les navigateurs web et les logiciels de messagerie instantanée ;
- Les logiciels antivirus sur les hôtes doivent être configurés pour analyser régulièrement tous les disques durs afin d'identifier toute infection du système de fichiers. Il est également recommandé d'analyser les supports amovibles insérés dans l'hôte avant d'autoriser leur utilisation ;
- Les utilisateurs doivent également être en mesure de lancer une analyse manuellement selon les besoins, connue également sous le nom d'analyse à la demande.
- Identifier les types courants de logiciels malveillants ainsi que les outils des attaquants ;
- La désinfection des fichiers, qui consiste à supprimer les logiciels malveillants à l'intérieur d'un fichier, et la mise en quarantaine des fichiers, qui signifie que les fichiers contenant des logiciels malveillants sont stockés dans un espace isolé en vue d'une désinfection ou d'un examen ultérieur.

Les critères importants sont :

- Administratif : Géré de manière centralisée, contrôlé et suivi régulièrement par les administrateurs de l'antivirus ;
    - Protection contre les manipulations : L'utilisateur ne doit pas pouvoir désactiver ou supprimer l'antivirus,
    - Mise à jour régulière des signatures antivirus et des bases de données,
    - Visibilité des infections et de l'état des déploiements (*reporting*).
- Précision : Décrit le taux de réussite relatif de l'outil et les types d'erreurs qu'il peut commettre ;
- Surcharge du système : Impact sur les performances du système.

Stratégie de mise en œuvre :

Les organisations doivent déployer un logiciel antivirus sur tous les hôtes pour lesquels un logiciel antivirus satisfaisant est disponible. Le logiciel antivirus doit être installé le plus tôt possible après l'installation du système d'exploitation, puis mis à jour avec les dernières signatures et les derniers correctifs du logiciel antivirus (pour éliminer toute vulnérabilité connue du logiciel antivirus lui-même). (1).

Évaluation/comparaison des produits Organisations

- **AV-Test** https://www.av-test.org/en/ : Organisation allemande acquise par le groupe suisse IT Security en 2021. Tous les deux mois, les chercheurs publient les résultats de leurs tests, ce qui inclut une liste de produits ayant obtenu une certification (2).

  Méthodologie : AV-Test utilise différents modules pour chaque système d'exploitation, sur la base de 3 critères principaux :
  - La protection reflète les résultats des tests de protection contre les logiciels malveillants et autres attaques,
  - Les performances démontrent l'influence des produits testés sur la vitesse des systèmes d'essai,
  - La facilité d'utilisation indique les influences perturbatrices des produits testés dues aux fausses alarmes et aux limitations dans l'utilisation d'Internet.
- **AV-Comparatives** https://www.av-comparatives.org : Organisation autrichienne indépendante qui teste et évalue les logiciels antivirus, publiant régulièrement des graphiques et des rapports en libre accès. Les financements d'AV-Comparatives sont soutenus par plusieurs universités (3).

  Méthodologie : Les tests sont effectués chaque année.
  - Test de protection dans le monde réel : attaques de logiciels malveillants en ligne qu'un utilisateur professionnel typique pourrait rencontrer en surfant sur Internet (751 cas de test en 2021).
  - Test de protection contre les logiciels malveillants : il s'agit d'un scénario dans lequel le logiciel malveillant préexiste sur le disque ou pénètre dans le système de test via, par exemple, le réseau local ou un dispositif amovible, plutôt que directement depuis l'internet (30 tests en 2021).
  - Tests de performance : Impact sur les performances du système.

Bien que les logiciels antivirus soient devenus une nécessité pour la prévention des incidents liés aux logiciels malveillants, il est impossible pour un logiciel antivirus d'endiguer tous les incidents liés aux logiciels malveillants. Souvent, les logiciels antivirus n'excellent pas dans le blocage des menaces inconnues. Les logiciels antivirus détectent les logiciels malveillants principalement en recherchant certaines caractéristiques des exemples connus de logiciels malveillants, ce qui est très efficace pour identifier les logiciels malveillants connus, mais moins pour détecter les logiciels malveillants hautement personnalisés et adaptés (1).

Niveau 2 : Protection élevée EDR (Substantial protection *Endpoint Detection and Response*) (4) (5)

Solution apportée :

La corrélation et l'interprétation des événements deviennent de plus en plus importantes pour détecter et répondre à des logiciels malveillants plus avancés et personnalisés, par exemple les rançongiciels (ransomwares).

Les logiciels antivirus ne sont pas bien adaptés pour effectuer ce genre de tâche. Il se peut en effet que des événements distincts soient légitimes, mais qu'une surcharge d'événements se produisent sur une courte période, et que cela soit dû à un incident malveillant.

Pour remédier à cette situation, une nouvelle génération d'outils a été développée par différents fournisseurs. Il n'existe pas de définition ou de norme unique en matière d'EDR, ce qui signifie que les capacités des fournisseurs peuvent varier considérablement. Plusieurs fournisseurs ajoutent aux fonctionnalités de l'EDR d'autres fonctionnalités telles que l'antivirus, la sécurité du réseau… Tout cela rend la comparaison difficile.

Capacités minimales importantes pour l'EDR (4):

1) Détecter les incidents de sécurité ;
2) Contenir les incidents au niveau des points d'accès ;
3) Enquêter sur les incidents de sécurité ;
4) Fournir des conseils en matière de remédiation.

Le CCB recommande qu'une solution d'EDR ait au minimum les capacités suivantes :

- Surveillance des points d'accès et enregistrement des événements ;
- Recherche de données, enquête et traque des menaces ;
- Détection d'activités suspectes ;
- Des renseignements exploitables pour soutenir la réponse ;
- Remédiation automatisée ;
- Prise en charge de plusieurs systèmes d'exploitation ;
- Module de gestion centrale.

Le CCB recommande que l'outil sélectionné possède également les capacités supplémentaires suivantes :

- Rapport sur les vulnérabilités ;
- Capacités d'analyse criminalistique (forensic) / collecte de données sur les systèmes ;
- API pour la liaison de systèmes externes.

Détails des capacités :

- Surveillance des points d'accès et enregistrement des événements

  Nous recommandons que l'outil choisi ait la possibilité d'enregistrer des événements, comme les processus en cours d'exécution, les utilisateurs actifs sur la machine, les connexions réseau actives, les services existants sur la machine…

  Nous recommandons également que l'outil puisse transférer les alertes/événements vers un système externe comme un SIEM ou une solution de journalisation/stockage.

- Recherche de données, enquête et traque des menaces

  Nous recommandons que l'outil sélectionné puisse exécuter des requêtes personnalisées. De préférence, il peut également exécuter des scripts personnalisés vers un ensemble spécifié de systèmes.

  Idéalement, l'outil prend en charge l'interaction directe avec le système d'exploitation de la station de travail, afin de permettre à l'équipe de sécurité d'enquêter sur les menaces sur le système concerné et d'exfiltrer des échantillons pour une analyse plus approfondie dans un environnement séparé (*sandbox*).

- Des renseignements exploitables

  Nous recommandons que l'outil choisi ait la possibilité d'ingérer des indicateurs de compromission (IOC). Il peut s'agir d'adresses réseau (IP), de hachages de fichiers, de noms de fichiers, de noms de domaine, d'e-mails… Plus le nombre d'indicateurs pouvant être ingérés de manière automatisée est important, mieux c'est.

- Détection d'activités suspectes

  Nous recommandons que l'outil choisi prenne en charge la création de règles de détection personnalisées par l'organisation elle-même. La détection basée sur les signatures ainsi que la détection basée sur les règles (détection comportementale) sont recommandées.

- Prise en charge de plusieurs systèmes d'exploitation

  Nous recommandons que l'outil choisi dispose d'agents disponibles pour plusieurs systèmes d'exploitation. Les systèmes basés sur Windows, Windows Server, Mac OS, et les distributions Linux basées sur Debian ou Redhat doivent être supportés.

- Remédiation automatisée

  Nous recommandons que l'outil sélectionné ait la possibilité de répondre automatiquement aux incidents détectés et qu'il puisse mettre en quarantaine un point d'accès.

- Composant de gestion centrale

  Nous recommandons que l'outil sélectionné puisse se connecter en permanence à sa plateforme de gestion centrale. Toute connexion réseau (internet) doit être prise en charge (même si cela signifie qu'il n'y a pas de connexion VPN directe vers l'organisation).

  Si une solution dans le cloud est utilisée, nous recommandons que cette solution soit physiquement située dans un centre de données européen et qu'une évaluation de l'impact sur la protection des données (DPIA) soit effectuée.

  Certaines solutions intégrées dans le cloud peuvent offrir des avantages tels que l'automatisation de la configuration et de la maintenance des composants de gestion, l'établissement de rapports intégrés prédéfinis, etc.

Stratégie de mise en œuvre :

Nous recommandons d'embarquer autant d'appareils que possible (sur tous les systèmes d'exploitation pris en charge).
Le logiciel doit être installé le plus tôt possible après l'installation du système d'exploitation, puis mis à jour avec les derniers correctifs logiciels. Les mises à jour ne sont normalement pas aussi fréquentes que pour les logiciels antivirus, mais les organisations devraient être en mesure de déployer des mises à jour dès que possible après la publication d'un correctif.

Évaluation/comparaison des produits Organisations

Nous recommandons de toujours évaluer les capacités minimales de chaque solution avec les recommandations de la base de connaissances MITRE ATT&CK™ (6).

La base de connaissances ATT&CK™ fournit une base commune pour décrire à la fois les critères de test et les résultats. ATT&CK est une base de connaissances développée par MITRE, accessible dans le monde entier, regroupant les tactiques et techniques utilisées par les cybercriminels, basée sur des observations réelles d'attaques de cybercriminels contre des réseaux informatiques (6).

MITRE a effectué un test d'évaluation d'outils EDR spécifiques d'une manière intéressante. Selon certains vendeurs, MITRE est le premier dans l'industrie à évaluer les vendeurs d'EDR. MITRE a choisi 2 acteurs de menaces spécifiques (APT3 & APT29) et a ensuite exécuté les techniques ATT&CK associées lors d'un cyber exercice.

L'évaluation la plus récente a été réalisée sur base des tactiques, techniques et procédures (TTP) de 2 groupes:

- Wizard Spider (7) est un groupe criminel à motivation financière qui mène depuis août 2018 des campagnes de ransomware contre diverses organisations, allant des grandes entreprises aux hôpitaux.
- Sandworm Team (8) est un puissant groupuscule de menaces russe qui a été attribué à l'unité 74455 du GRU russe par le ministère de la Justice des États-Unis et le Centre national de cybersécurité du Royaume-Uni. Les attaques les plus notables du Sandworm Team comprennent le ciblage en 2015 et 2016 de sociétés électriques ukrainiennes et les attaques NotPetya de 2017. Le Sandworm Team est actif depuis au moins 2009.

Les résultats détaillés par fournisseur peuvent être consultés sur le site Att&ck Evaluations (9).

Il est important de noter que MITRE ne classe pas les participants, mais en effectuant quelques recherches sur Internet, vous trouverez des résumés pour vous faire une opinion.

Niveau3 : Protection avancée XDR - *(advanced protection eXtended Endpoint Detection and Response)*

Solution apportée (10) (5)

La plupart des organisations ne disposent pas d'une infrastructure (*endpoint*) unifiée, standard et consolidée. Les équipes de sécurité doivent être en mesure d'obtenir une vue d'ensemble de tous les systèmes et alertes de l'infrastructure complète. XDR rationalise l'ingestion, l'analyse et les flux de données de sécurité sur l'ensemble de la chaîne de sécurité d'une organisation, améliorant ainsi la visibilité des menaces de sécurité cachées et avancées en unifiant la réponse.

XDR est l'évolution de l'EDR (*Endpoint Detection and Response*). Alors que l'EDR collecte et corrèle les activités sur plusieurs points d'accès, la XDR élargit le champ de la détection au-delà des points d'accès pour fournir une détection, une analyse et une réponse sur les points d'accès, les réseaux, les serveurs, les charges de travail dans le cloud, le SIEM et bien plus encore.

Cela permet d'obtenir une vue unifiée, centralisée , de plusieurs outils et vecteurs d'attaque. Cette visibilité améliorée permet de contextualiser ces menaces pour faciliter le triage, l'investigation et les efforts de remédiation rapide.

Stratégie de mise en œuvre :

Nous recommandons l'intégration d'autant de plateformes que possible. Cependant, un déploiement progressif est recommandé. Une plateforme XDR doit disposer de suffisamment de temps pour établir une base de référence du comportement du flux de données afin de détecter avec précision les anomalies de sécurité. (11).

Capacités importantes pour un XDR (12)

- Indépendance

  La solution XDR doit s'intégrer à de multiples technologies et éviter le verrouillage des fournisseurs.

- Capacités de corrélation et de détection basées sur les machines

  Permet une analyse plus rapide d'ensembles de données beaucoup plus importants et réduit le nombre de faux positifs.

- Modèles de données préconstruits

  Intègre les renseignements sur les menaces et automatise la détection et la réponse sans que les ingénieurs logiciels aient à faire toute la programmation ou à créer toutes les règles. Nous recommandons que la solution XDR permette la création de règles supplémentaires personnalisées.

- Intégration avec les SIEM, les SOAR et les outils de gestion des cas.

  Plutôt que d'exiger le remplacement de ces produits, la XDR permet aux entreprises de maximiser la valeur de leurs investissements.

  Remarque : Il est important de quantifier la quantité de données de journal et de télémétrie qui seront collectées et la durée de stockage des données. Cela aidera à déterminer la quantité d'espace de stockage nécessaire à la plateforme XDR, ainsi que la bande passante qui sera

consommée sur les réseaux locaux, WAN, et les connexions vers le cloud pour envoyer les données à un agent de collecte de données XDR.

Évaluation/comparaison de produits Organisations (11)

Le CCB recommande d'évaluer d'abord l'infrastructure et les outils de votre organisation avant de décider de l'achat d'une solution XDR. Il existe quelques différences mineures entre les plateformes XDR.

- Niveau de détection
  Certaines applications XDR s'appuieront davantage sur les données de détection des points d'accès, d'autres sur les données qui traversent le réseau. Le fait de n'avoir aucun ou la plupart des travailleurs à domicile dans votre organisation, un réseau vaste, diversifié, et complexe, ... peut être un facteur clé dans le processus décisionnel.

- Informations sur les menaces (Threat intelligence)
  Il est important d'examiner comment le fournisseur gère le renseignement sur les menaces et la traque à l'aide de données externes sur les menaces et s'il est suffisamment proactif. La plupart des plates-formes XDR d'entreprise utilisent leurs propres équipes internes de détection des menaces pour identifier les menaces nouvelles ou émergentes. Les informations de renseignement sur les menaces recueillies par ces groupes peuvent être utilisées pour créer automatiquement des politiques de sécurité qui sont ensuite déployées vers les outils de sécurité de l'organisation. La capacité de ces équipes à identifier rapidement les menaces et à créer une politique est un facteur critique pour les exploits de type « zero-day ».

Ecosystème Windows

Chaque système d'exploitation Windows récent est livré avec un client Windows Defender (antivirus) gratuit installé, prêt à l'emploi. Les organisations sont, bien entendu, libres d'installer ou non ce produit antivirus. Si vous installez un autre produit antivirus, le composant antivirus du client Defender sera simplement remplacé. Tous les autres composants du client defender continueront à fonctionner (pare-feu Windows Defender, etc.).

D'autre part, le client gratuit Windows Defender peut être configuré et mis à niveau vers un client EDR (13) (14) .

Le « Defender for endpoint » peut également être déployé sur des serveurs Windows (15) ou sur votre infrastructure dans le cloud (16).

En tant que valeur ajoutée pour l'écosystème Defender, « Defender for Identity » pourrait être une fonctionnalité importante. Après l'installation d'un monitoring de tous les contrôleurs de domaine Active Directory (sur site), des options supplémentaires de gestion d'identité sont disponibles dans la plateforme cloud (17).

Comme pour tous les produits intégrés dans le cloud , certaines modifications peuvent être apportées par défaut à votre environnement, modifiant ainsi votre exposition à la sécurité. Cela nécessite un suivi et une évaluation continus des changements mis en place par le fournisseur.

Des conditions de licence particulières peuvent s'appliquer. Veuillez toujours vérifier les conditions de licence auprès de votre fournisseur.

Nous vous recommandons également d'installer Sysmon qui enrichira vos capacités de journalisation et de diagnostic (18).

D’autres systèmes d’exploitation (Linux, Mac OS, ...) ou des périphériques non-Microsoft ne fournissent pas toujours le même niveau de fonctionnalités et de sécurité dans la suite Defender. Examinez vos systèmes non Microsoft, la version et/ou la distribution utilisée et la manière dont elle est prise en charge par le fournisseur. (19)

L’utilisation des règles Yara n’est pas encore prise en charge (juin 2022), mais une « *Advanced query hunting* » est disponible avec une mise en œuvre spécifique au fournisseur.

Références

1. **NIST 800-83.** Guide to Malware Incident Prevention and Handling for Desktops and Laptops. *Nist.gov.* [En ligne] https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final.

2. **Wikipedia AV-test.** ***nl.wikipedia.org.*** **[En ligne] https://nl.wikipedia.org/wiki/AV-test.org.**

3. Wikipedia AV-Comparatives. ***en.wikipedia.org.*** **[En ligne] https://en.wikipedia.org/wiki/AV-Comparatives.**

4. Gartner. endpoint-detection-and-response-solutions. ***gartner.com.*** **[En ligne] https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions.**

5. Crowdstrike. edr vs mdr vs xdr. ***crowdstrike.com.*** **[En ligne] https://www.crowdstrike.com/cybersecurity-101/endpoint-security/edr-vs-mdr-vs-xdr/.**

6. Mittre Attck Product evaluations. attck based product evaluations. ***Mittre.com.*** **[En ligne] https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/attck%E2%84%A2-based-product-evaluations.**

7. Wizard Spider. [En ligne] https://attack.mitre.org/groups/G0102/.

8. Sandworm Team. [En ligne] https://attack.mitre.org/groups/G0034/.

9. mitre-engenuity.org. [En ligne] https://attackevals.mitre-engenuity.org/.

10. sentinelone.com. [En ligne] https://www.sentinelone.com/blog/understanding-the-difference-between-edr-siem-soar-and-xdr/.

11. Evaluate XDR. ***techtarget.com.*** **[En ligne] https://www.techtarget.com/searchsecurity/tip/How-to-evaluate-and-deploy-an-XDR-platform.**

12. ***XDR according Mandiant.*** **[En ligne] mandiant.com. https://www.mandiant.com/resources/what-is-xdr.**

13. What is Defender for Endpoint. ***docs.microsoft.com.*** **[En ligne] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide.**

14. Configure Defender for Endpoint (client). ***docs.microsoft.com.*** **[En ligne] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints?view=o365-worldwide.**

15. Configure Defender for Endpoint (server). ***docs.microsoft.com.*** **[En ligne] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-endpoints?view=o365-worldwide.**

16. Configure Defender for Endpoint (cloud). ***docs.microsoft.com.*** **[En ligne] https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-introduction.**

17. What is Defender for Identity. ***docs.microsoft.com.*** **[En ligne] https://docs.microsoft.com/en-us/defender-for-identity/what-is.**

18. Sysmon, Microsoft. [En ligne] https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.

19. Configure Defender for Endpoint (other). ***docs.microsoft.com.*** **[En ligne] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints-non-windows?view=o365-worldwide.**

Contact

Centre pour la Cybersécurité Belgique
Rue de la Loi, 16/ Wetstraat 16
1000 Bruxelles/ Brussel
info@ccb.belgium.be

Avis de non-responsabilité

Le présent document et ses annexes ont été élaborés par le Centre pour la Cybersécurité Belgique (CCB), une administration fédérale créée par arrêté royal du 10 octobre 2014 et placée sous l'autorité du Premier ministre.

Le CCB décline toute responsabilité quant au contenu de ce document.

Les informations fournies :

- sont exclusivement de nature générale et ne visent pas à prendre en considération toutes les situations particulières ;

- ne sont pas nécessairement exhaustives, précises ou à jour sur tous les points

Rédacteur responsable

Centre pour la Cybersécurité Belgique
Monsieur De Bruycker, Administrateur
Rue de la Loi, 16
1000 Bruxelles