Évaluation MITRE ATT&CK, phase 3 : le guide indispensable

Cet eBook offre un aperçu des performances des fournisseurs sur les différents critères d'évaluation, avant de vous livrer quelques conseils utiles pour approfondir votre analyse. Également au sommaire : une description de la méthodologie de test MITRE, les outils fournis par MITRE pour visualiser et comparer les résultats, ainsi que diverses pistes d'analyse pour déterminer par vous-même le fournisseur le plus à même de répondre aux besoins de sécurité de vos terminaux.

paloalto® NETWORKS | CORTEX® XDR BY PALO ALTO NETWORKS

Introduction

Face à des cybermenaces de plus en plus sophistiquées, une prévention et une protection efficaces impliquent une parfaite compréhension des schémas d'attaque. Aussi, pour lutter contre l'évolution constante des menaces persistantes avancées (APT), les fournisseurs de solutions de sécurité doivent s'appuyer sur un modèle objectif afin de tester leurs produits contre les différentes tactiques, techniques et procédures (TTP) des cyberattaquants.

C'est précisément le rôle des évaluations MITRE ATT&CK®, qui offrent une analyse concrète des principaux outils de détection et de réponse sur les terminaux (EDR) ainsi que des solutions étendues de détection et de réponse (XDR) afin de déterminer leur faculté à détecter et repousser les attaques réelles.

Or, pour la troisième année consécutive, Palo Alto Networks s'impose aux tests MITRE ATT&CK comme l'un des fournisseurs les plus performants, avec 100 % de protection contre les menaces et plus de 97 % de visibilité sur les techniques d'attaque (sans aucun changement de configuration)[1].

Voici, globalement, les résultats obtenus par Cortex XDR face aux TTP des groupes Carbanak et FIN7 :

- 100 % d'attaques bloquées lors des tests de protection sur les terminaux Windows® et Linux.
- 97 % de visibilité sur les techniques d'attaque.
- Meilleurs taux de détection parmi l'ensemble des solutions de sécurité ayant obtenu un score de protection parfait.
- 86 % de détection analytique (au sens de MITRE : des détections qui enrichissent le contexte des techniques d'attaque au-delà des données télémétriques).
- 80 % de détections recoupées avec une technique (soit la forme de détection la plus élevée dans le cadre de cette évaluation).
- Meilleur résultat de détection et de protection combinées.

Cortex XDR a bloqué

100 %

des attaques lors des tests de protection sur les terminaux Windows et Linux

CORTEX XDR BY PALO ALTO NETWORKS

Présentation de l'évaluation

De nouveaux fournisseurs ont rejoint le panel de la phase 3 des évaluations MITRE ATT&CK, ce qui prouve l'importance que revêtent les tests externes et objectifs dans le choix d'une solution de sécurité.

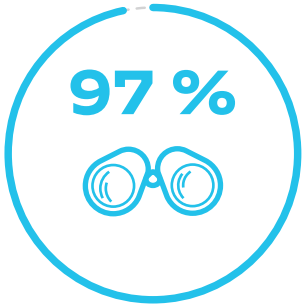
En se prêtant au jeu de l'évaluation, les fournisseurs peuvent identifier certains domaines d'amélioration afin notamment de mettre à jour les règles de prévention, de détection et de réponse sur lesquelles se fondent leurs politiques de sécurité. Cet exercice ne fournit certes pas de score de comparaison ou de classement général, mais il permet de dresser un résumé « techno-agnostique » des différentes méthodologies dont font usage les professionnels de la sécurité pour identifier et prévenir les campagnes d'attaques sophistiquées.

La phase 3 a testé les performances de 29 fournisseurs face aux TTP des groupes Carbanak et FIN7. Chaque participant a fait l'objet de 20 étapes de test distinctes et de 174 sous-tests réalisés sur des systèmes d'exploitation Windows et Linux.

Nouveautés de la troisième édition

Cette année, près de la moitié des fournisseurs se sont livrés à une évaluation de protection distincte sur Windows et Linux. Les produits ont été soumis à dix étapes de test visant à déterminer leur faculté à bloquer activement les attaques. Étant donné nos excellents résultats en matière de prévention des menaces et nos outils complets pour terminaux Linux, nous avons naturellement accepté de participer à ces tests de protection.

Les résultats de l'évaluation sont sans appel : Cortex® XDR™ **a bloqué toutes les attaques ciblant les systèmes Linux et Windows, tout en obtenant le plus fort taux** et la meilleure qualité de détection (voir figure 3). D'autre part, en consacrant un test indépendant à la protection des terminaux, MITRE souligne qu'il est important de dépasser les fonctions de détection traditionnelles, en combinant par exemple une plateforme de protection des terminaux (EPP) avec une solution EDR pour renforcer la sécurité.



Cortex XDR offre 97 % de visibilité
sur les techniques d'attaque, soit les meilleurs taux de détection parmi les solutions ayant obtenu un score de protection parfait

CORTEX XDR BY PALO ALTO NETWORKS

L'approche de MITRE

Plutôt que d'attribuer un score aux différentes solutions de sécurité testées, MITRE en étudie les mécanismes de détection : les occurrences sont chacune rattachées à une catégorie[2], avec les données de capture qui leur sont associées, puis organisées en fonction des techniques d'attaque. Une même technique pouvant être liée à plusieurs types de détection selon les mécanismes employés, les différentes détections observées sont incluses dans les résultats.

Malgré les efforts déployés afin de capturer la totalité des détections générées, certaines occurrences peuvent échapper au modèle de MITRE. En effet, pour qu'une détection soit rattachée à une technique donnée, elle doit s'appliquer de façon spécifique à cette technique. Par exemple, le fait qu'une détection s'applique à une technique employée au cours d'une étape ou d'une sous-étape ne signifie pas pour autant qu'elle s'appliquera à toutes les techniques utilisées au cours de cette étape. Enfin, les fournisseurs de solutions de sécurité doivent envoyer à MITRE une preuve de détection dans chaque catégorie. Pour autant, tous les détails de la détection n'apparaissent pas nécessairement dans les résultats publics de l'évaluation, surtout lorsqu'ils sont de nature sensible.

Pour déterminer la catégorie adéquate, MITRE examine ainsi les captures d'écran, les notes prises au cours de l'évaluation, les réponses aux questions posées au fournisseur, ainsi que les commentaires de ce dernier suite aux résultats préliminaires. MITRE teste également les procédures dans un environnement de laboratoire séparé et s'appuie sur des outils de détection et des artefacts forensiques open source. Les résultats de ces tests permettent alors d'établir ce qui peut être considéré comme une détection pour chaque technique.

Enfin, MITRE procède au calibrage des différentes catégories afin de rechercher les potentielles incohérences et garantir une application homogène entre tous les fournisseurs. Le choix de telle ou telle catégorie repose au final sur une analyse humaine, avec le jugement et les biais qu'elle implique. Il est toutefois possible de s'en écarter en structurant son analyse à la manière du présent guide.

Le saviez-vous ?

MITRE ATT&CK a été créé en 2013 suite au projet Fort Meade Experiment (FMX) de MITRE, au titre duquel des chercheurs ont émulé des techniques et tactiques de cybercriminels

Évaluation des solutions EDR à l'aide du framework MITRE

Les tests MITRE permettent aux entreprises de comparer les résultats de différentes solutions EDR disponibles sur le marché. L'évaluation présente en effet les niveaux d'efficacité des fournisseurs participants, articulés autour d'un référentiel commun garantissant parité et homogénéité tout au long des tests.

Mais quel est donc l'intérêt stratégique pour les fournisseurs participants ? Chez Palo Alto Networks, les évaluations MITRE ATT&CK sont une bonne occasion de faire tester nos produits par un tiers neutre et objectif face aux attaques les plus sophistiquées du moment. Nous récoltons en retour des informations constructives qui nous permettent de renforcer nos solutions de détection et de prévention.

En employant les TTP modernes de groupes cybercriminels comme Carbanak et en émulant les scénarios d'attaque dans un environnement contrôlé (MITRE Engenuity), MITRE permet aux fournisseurs de produits de sécurité d'évaluer leurs performances et de déterminer quelles sont leurs lacunes. Les résultats révèlent ainsi des pistes d'amélioration et fournissent des conseils afin d'optimiser les domaines dans lesquels ils sont moins performants.

Profil de l'attaquant

Le groupe Carbanak est l'auteur d'attaques APT particulièrement efficaces à l'encontre du secteur financier. Ces cyberbraqueurs ont ainsi extorqué près de 1 milliard de dollars à une centaine de banques du monde entier entre 2013 et 2018. L'attaquant est parfois assimilé à FIN7, car les deux groupes utilisent le même malware (Carbanak). Cependant, ces deux entités semblent être différentes et sont donc surveillées séparément.

Le malware Carbanak a dérobé

1 milliard de dollars

à des banques via des attaques menées depuis la Russie, l'Ukraine, l'Europe et la Chine

Carbanak utilise principalement l'envoi d'e-mails de spear-phishing contenant des pièces jointes malveillantes. C'est ainsi que les cybercriminels infectent les systèmes d'établissements bancaires, dérobent les identifiants, collectent des informations (notamment en interceptant l'écran consulté par les employés de banque) et se font passer pour des membres du personnel afin de voler des fonds au moyen de diverses techniques :

- Transfert d'argent sur le compte des cyberfraudeurs via des opérations bancaires en ligne.
- Paiements électroniques et virements effectués sur des comptes aux États-Unis et en Chine.
- Manipulation des soldes en vue de transférer l'excédent via des transactions frauduleuses.
- Détournement de DAB (des complices viennent récupérer l'argent aux heures convenues).

Zoom sur l'émulation de Carbanak/FIN7 par MITRE

- 2 scénarios complets (un par attaquant)
- 20 phases d'attaque
- 174 sous-étapes avec 70 techniques uniques
- Évaluation de la protection (10 étapes)

Pour afficher les techniques prises en compte dans l'ATT&CK Navigator, utilisez le modèle d'évaluation fourni par MITRE (disponible ici).

Credential Access	Discovery	Lateral Movement	Collection
Account Manipulation	Account Discovery	AppleScript	Audio Capture
Bash History	Application Window Discovery	Application Deployment Software	Automated Collection
Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data
Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories
Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System
Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive
Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media
Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged
Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection
Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture
Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser
Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture

Carbanak FIN7 Carbanak+FIN7

Méthodologie de la phase 3

L'environnement

Les évaluations ont été réalisées dans le cloud Microsoft Azure. Chaque fournisseur a reçu deux environnements identiques (le premier réservé au test de détection, le second au test de protection) composés de huit hôtes chacun sur lesquels installer leur logiciel client. Tous avaient également la liberté d'installer un logiciel serveur soit sur une machine virtuelle (VM) déjà déployée dans l'environnement, soit sur une VM importée par leurs soins. Les VM Azure fournies par défaut, de type Standard B4MS, étaient dotées chacune de quatre vCPU et 16 Go de mémoire. Les fournisseurs disposaient d'un accès administratif complet aux hôtes instanciés.

La connexion à l'écosystème de test était assurée par l'intermédiaire d'un serveur VPN (un par environnement) et les mots de passe étaient partagés via des méthodes hors bande. Les fournisseurs pouvaient ensuite utiliser des services RDP ou SSH au sein de l'environnement. Les hôtes n'étaient accessibles qu'au sein du VPN. Si aucune adresse IP publique ne leur était assignée via Azure, ils pouvaient toutefois accéder à Internet.

Suite >

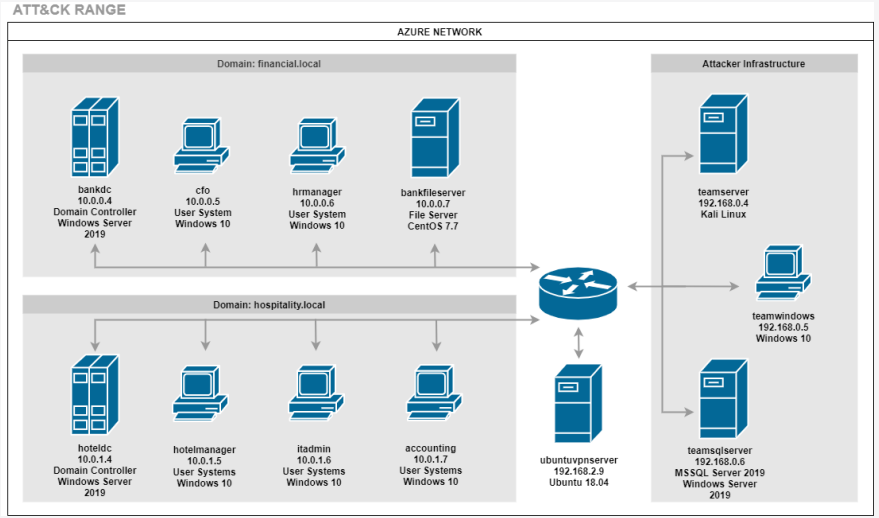


Figure 1 : Configuration de l'environnement ATT&CK – réseau Azure

Environnement d'évaluation Carbanak/FIN7

Hôtes cibles :

- Windows Server 2019
- Windows 10
- CentOS 7.7

Bien que chaque fournisseur utilise sa propre terminologie et son approche spécifique pour détecter les attaques et s'en prémunir, MITRE n'établit que deux catégories (« principale » et « nuance ») afin de pouvoir comparer les produits dans des termes similaires.

Chaque détection ou protection est classée dans une catégorie principale en fonction du contexte fourni, bien qu'une ou plusieurs « nuances » puissent venir se greffer afin de mieux décrire l'évènement en question.

L'évaluation Carbanak+FIN7 comprend ***six catégories de détection principales*** qui reflètent le volume d'informations contextuelles fournies à l'analyste, ainsi que ***trois grandes catégories de protection***.

Suite >

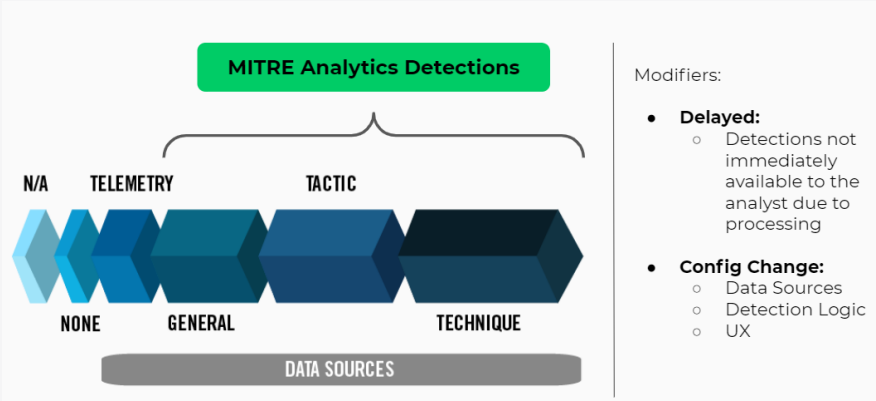


Figure 2 : Catégories de détection Carbanak/FIN7

Catégories de détection

Sans objet (S.O.) : le fournisseur n'avait aucune visibilité sur le système testé. Avant l'évaluation, chaque participant doit déclarer les composants sur lesquels il ne déploie aucun capteur afin de pouvoir prendre correctement en compte la catégorie Sans objet lors des étapes pertinentes.

Aucune : la solution de sécurité n'a collecté aucune donnée sur le comportement testé qui corresponde aux critères de détection concernés. La catégorie Aucune exclut toute nuance, remarque ou capture d'écran.

Télémétrie : données faiblement traitées recueillies par la solution de sécurité indiquant la survenue d'un ou plusieurs évènements spécifiques au comportement testé, correspondant aux critères de détection assignés. Les preuves doivent clairement montrer l'occurrence de l'évènement et être liées au mécanisme d'exécution (afin de distinguer la certitude de la vraisemblance). Ces données doivent être visibles nativement dans l'outil du fournisseur et peuvent inclure les données récupérées à partir du terminal.

Générale : données traitées prouvant qu'un ou plusieurs évènements malveillants/anormaux ont eu lieu en lien avec le comportement testé. Quasiment aucun détail n'est fourni quant au motif (tactique) ou aux modalités (technique) de l'action en question.

Tactique : données traitées spécifiant la tactique ATT&CK ou enrichissement équivalent des données collectées par la solution de sécurité. Celles-ci renseignent l'analyste sur l'intention ou le motif potentiels de l'activité observée. Pour que l'évènement soit qualifié de détection, plusieurs étiquettes doivent identifier la tactique ATT&CK et un lien clair doit être établi entre la description de la tactique observée et la tactique testée.

Suite >

Technique : données traitées spécifiant la technique, la sous-technique ATT&CK ou enrichissement équivalent des données collectées par la solution de sécurité. Celles-ci renseignent l'analyste sur le mode opératoire ou les conséquences de l'action (p. ex. fonctionnalités d'accessibilité ou extraction d'identifiants). Pour que l'évènement soit qualifié de détection, plusieurs étiquettes doivent identifier l'ID de technique ATT&CK (TID) et un lien clair doit être établi entre la description de la technique observée et la technique testée.

Catégories de protection

Ces catégories permettent de déterminer si la solution de sécurité a bien fourni une protection contre l'attaque simulée et si une intervention de l'utilisateur est nécessaire afin de bloquer l'activité. Les catégories de protection peuvent faire l'objet de modifications en fonction des leçons tirées de l'évaluation.

Sans objet (S.O.) : le fournisseur n'a pas déployé de solution de protection sur le système testé. Avant l'évaluation, chaque participant doit déclarer les composants sur lesquels il n'installe aucun capteur afin de pouvoir prendre correctement en compte la catégorie Sans objet lors des étapes pertinentes.

Aucune : la technique testée n'a pas été bloquée et/ou la technique a échoué et aucune donnée ne prouve à l'utilisateur que la solution a bloqué l'activité.

Bloquée : la technique testée a été bloquée et l'utilisateur est informé – explicitement – que la solution de sécurité a bloqué l'activité.

Suite >

Nuances de détection

MITRE fait la distinction entre plusieurs types de détection afin d'enrichir le contexte autour des différentes solutions de sécurité. L'utilisateur final peut ainsi comparer, évaluer ou classer les résultats pour déterminer quel outil de sécurité est le plus avantageux selon ses besoins.

Changement de configuration : le fournisseur a modifié la configuration de son outil de sécurité au cours de l'évaluation, par exemple pour montrer que des données supplémentaires peuvent être collectées ou traitées. La nuance « changement de configuration » peut être associée à d'autres critères décrivant la nature de la modification :

- **Sources de données** – changements apportés pour que le capteur collecte de nouvelles informations.
- **Logique de détection** – modification de la logique de traitement des données.
- **UX** – changements concernant l'affichage de certaines données déjà collectées, mais qui étaient invisibles pour l'utilisateur.

Retard : ce type de détection entraîne un retard de présentation des données pertinentes à l'analyste. C'est par exemple le cas lorsque la détection est générée après un traitement consécutif ou additionnel. Cette nuance ne s'applique pas à l'ingestion automatisée des données, au traitement de routine nécessitant un délai avant d'afficher les données, ni aux problèmes de connectivité qui ne sont pas liés directement à la solution de sécurité. Cette nuance est toujours associée à d'autres critères décrivant plus en détail la nature du retard.

Cortex XDR vs Carbanak+FIN7 : nos résultats

Plutôt que d'attribuer un score aux différentes solutions de sécurité testées, MITRE en étudie les mécanismes de détection : les occurrences sont chacune rattachées à une catégorie, avec les données de capture qui leur sont associées, puis organisées en fonction des techniques d'attaque. Une même technique pouvant être liée à plusieurs types de détection selon les mécanismes employés, les différentes détections observées sont toutes incluses dans les résultats d'évaluation.

MITRE a combiné les techniques d'attaque détectées par télémétrie (nécessitant peu de traitement) et celles ayant fait l'objet d'un traitement analytique (afin de déterminer la « visibilité ») pour arriver au taux de détection global des 174 techniques d'attaques testées.

La différence Cortex XDR : la preuve par les données

Première plateforme XDR du marché, Cortex XDR intègre les données issues des terminaux, des réseaux, du cloud et de sources tierces pour bloquer les attaques sophistiquées. Les résultats que nous avons obtenus à la dernière évaluation MITRE ATT&CK sont, comme depuis trois ans, excellents. Cortex XDR a en effet enregistré des performances supérieures en matière de protection, de détection et de visibilité, soit les trois piliers d'une sécurité des terminaux efficace et globale.

Cortex XDR offre une fiabilité de détection accrue en s'appuyant sur des analyses comportementales et le machine learning. Ainsi, notre solution collecte et rassemble un vaste ensemble de données : journaux de terminaux Cortex XDR, pare-feu nouvelle génération (NGFW), Prisma® Access, fournisseurs de service d'identification, etc. Elle dresse un profil de comportements attendus afin de mettre en évidence les activités inhabituelles susceptibles d'indiquer une attaque. L'analytique comportementale s'appuie sur le traitement des données enrichies via le machine learning et l'analyse statistique. Objectif : mettre à jour les tactiques et les techniques des attaquants, tout en réduisant le nombre de faux positifs par rapport aux règles de détection traditionnelles.

Cortex XDR : des résultats au sommet depuis trois ans

- **2018 :** plus vaste couverture contre les techniques d'attaque
- **2019 :** couverture inégalée des techniques d'attaque
- **2020 :** meilleures détection et prévention combinées

En associant protection, détection analytique et visibilité, Cortex XDR est capable d'identifier avec précision les comportements anormaux. Cela permet à la fois d'accélérer le tri des alertes et de réduire la durée de présence et la latéralisation au sein du réseau.

La protection est le premier rempart

En plus de bloquer toutes les attaques menées à l'occasion des tests de protection MITRE ATT&CK (une nouveauté de la phase 3), Cortex XDR a également intégré les données de journaux des pare-feu nouvelle génération Palo Alto Networks afin d'augmenter la fiabilité de détection. Qui dit protection dit aussi prévention : l'attaquant n'ayant pu exécuter son offensive, sa durée de présence est ainsi nulle. De plus, le blocage de la menace permet de réduire l'accoutumance aux alertes puisque, le cycle d'attaque étant interrompu, aucune suite n'est donnée.

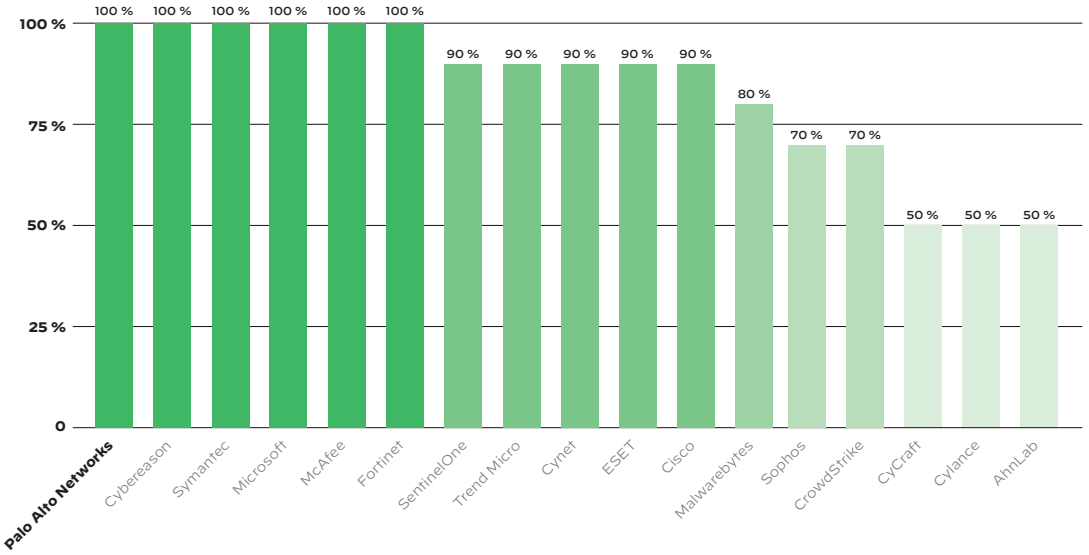


Figure 3 : Cortex XDR a bloqué 100 % des attaques lors des tests de protection sur Linux et Windows

CORTEX XDR BY PALO ALTO NETWORKS

Cortex XDR : meilleures performances générales

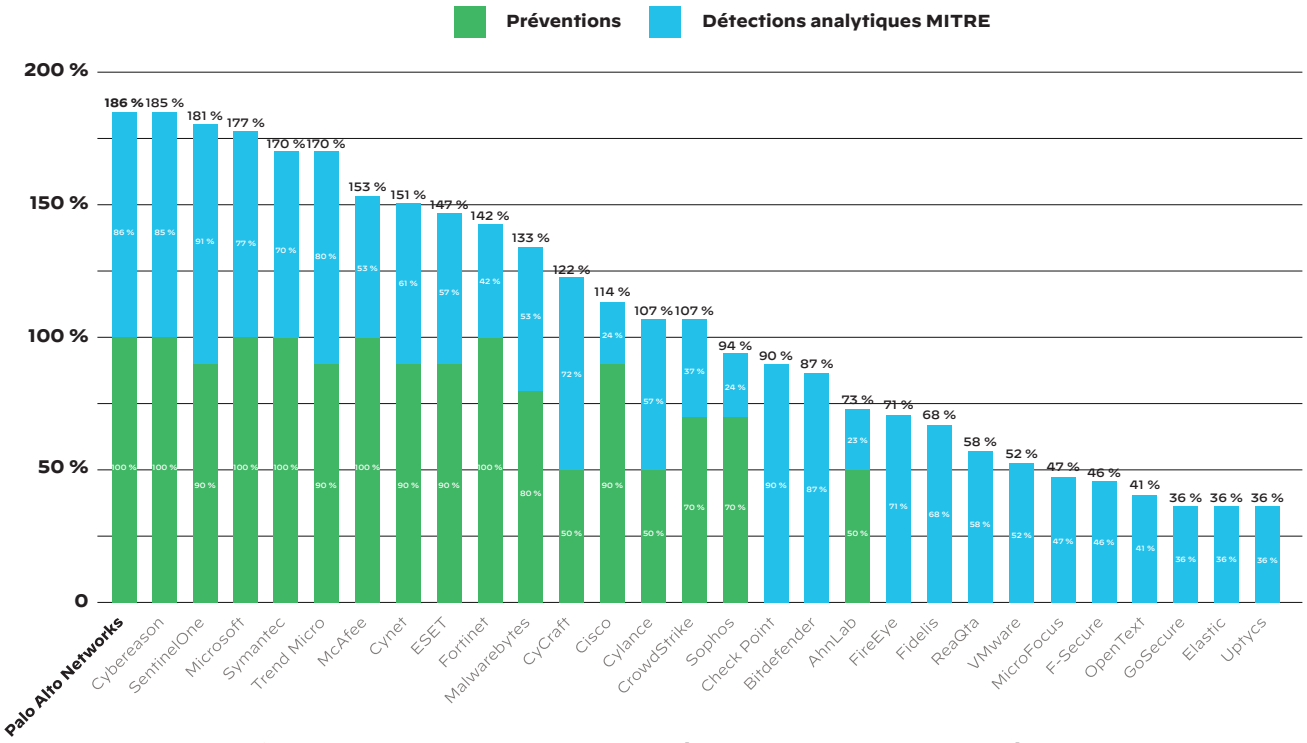


Figure 4 : Meilleures protection et détection analytique combinées

CORTEX XDR BY PALO ALTO NETWORKS

La protection, ou prévention, est un composant essentiel d'une solution EDR efficace. Elle permet aux analystes de sécurité de consacrer plus de temps aux investigations ou à la traque des menaces. La détection, quant à elle, offre une visibilité sur la séquence d'attaque et fournit les données d'analyses requises pour mettre en évidence toute activité anormale appelant une investigation approfondie. La visibilité, enfin, sous-tend à la fois la prévention et la détection. Seule, son efficacité est toutefois limitée. Pour que les campagnes d'attaque apparaissent plus clairement, il convient d'exploiter les bonnes analyses afin de rassembler et de mettre en corrélation les données télémétriques récoltées auprès des différentes sources.

À propos des changements de configuration

Lorsqu'une étape du test ne produit pas la détection escomptée, MITRE offre une sorte de « seconde chance » aux fournisseurs de solutions. Ces derniers peuvent en effet modifier leur configuration initiale afin d'améliorer la détection d'une technique donnée. La nuance « changement de configuration » désigne par conséquent une détection générée suite à une telle modification en vue d'obtenir un meilleur résultat. MITRE fait ce choix pour que les fournisseurs puissent affiner l'efficacité de leurs outils de sécurité.

Bien sûr, dans des conditions réelles, lorsqu'un attaquant passe à travers les mailles du filet, il y a peu de chances que celui-ci remette la balle au centre. Pour plus de réalisme, nous pensons donc qu'il est judicieux de ne pas tenir compte de ce type de détections (voir figure 5) dans la comparaison des résultats.

Voici quelques exemples de changements de configuration[3] :

- Une règle, ancienne ou nouvelle, ou bien une fonction (p. ex. une liste rouge) est activée ou modifiée pour se déclencher lors d'un second test. Les détections potentiellement générées relèveront donc de la nuance « changement de configuration – logique de détection ».
- Des données collectées en back-end indiquent qu'un compte a été créé, mais celles-ci n'apparaissent pas par défaut pour l'utilisateur final. Le fournisseur adapte les paramètres du back-end afin d'inclure ces données télémétriques dans l'interface utilisateur. Une détection de type Télémétrie, associée à la nuance « changement de configuration – UX », sera donc attribuée pour la technique Création de compte.

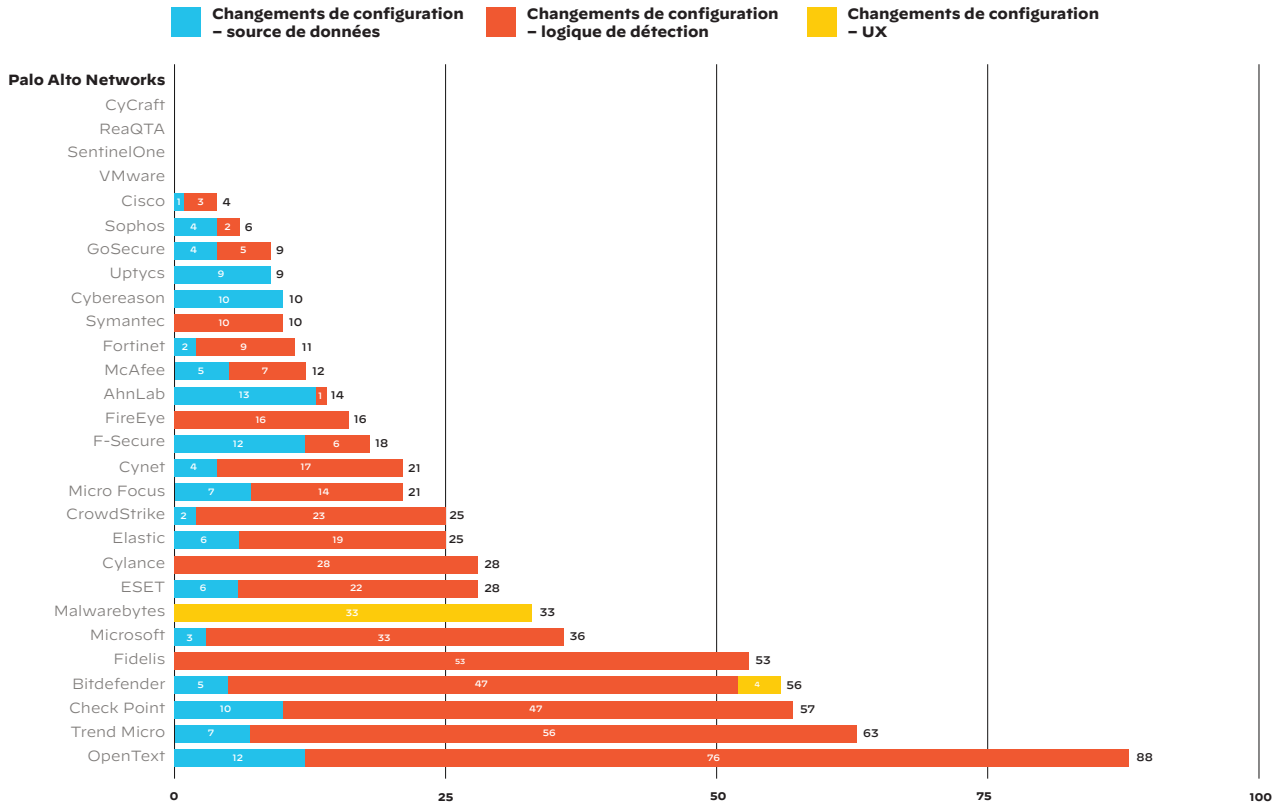


Figure 5 : Nombre de changements de configuration par fournisseur dans la phase 3

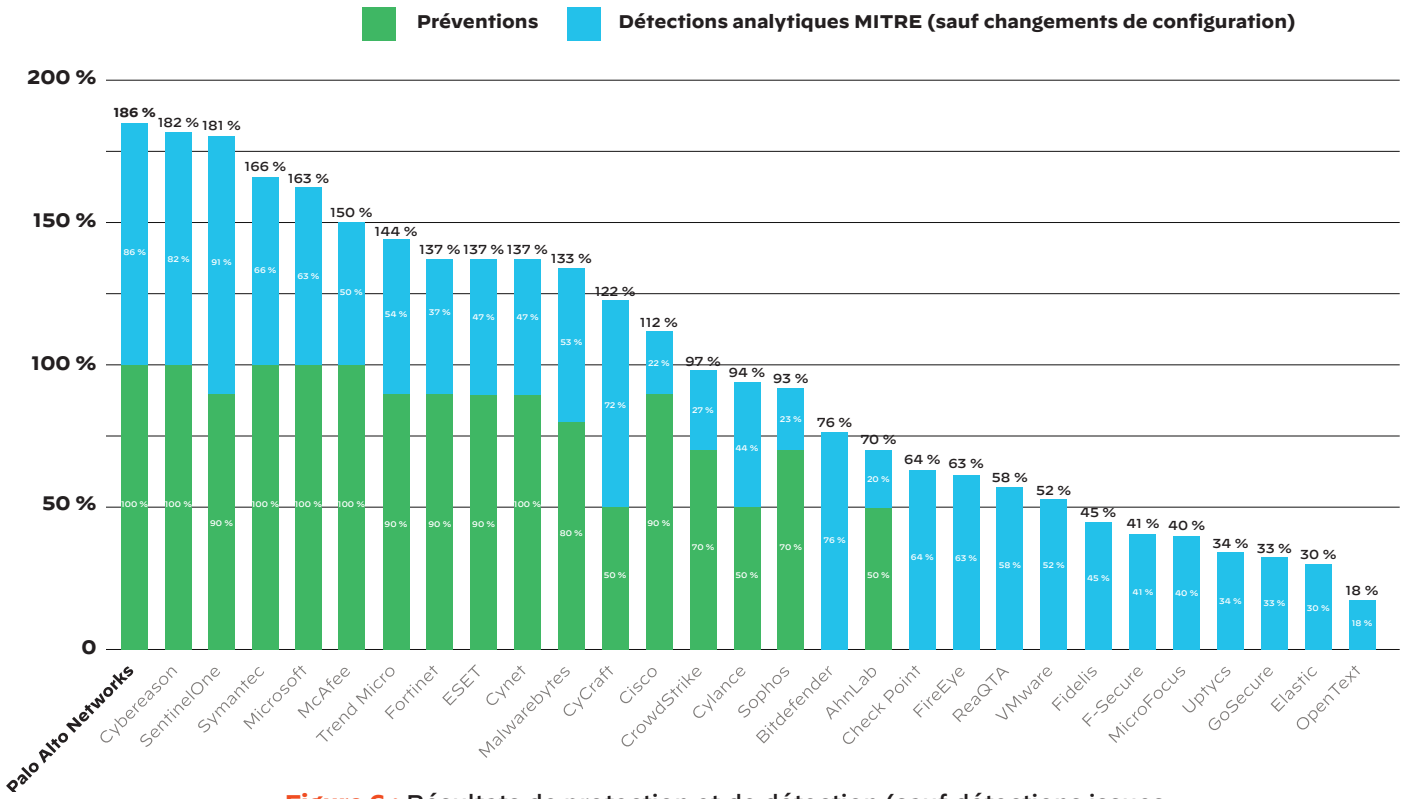


Figure 6 : Résultats de protection et de détection (sauf détections issues d'un changement de configuration, contrairement à la figure 4)

Les chiffres ne disent pas tout

Pour bien comprendre les résultats des tests MITRE, il est important d'observer également les captures d'écran transmises par les fournisseurs, qui nous renseignent sur le contexte dont dispose l'analyste de sécurité.

Par exemple, Cortex XDR est la seule solution unifiée capable de mettre en corrélation et de rassembler les données issues des réseaux, des terminaux et de sources tierces dans une vue causale, avant de procéder à des analyses complètes pour identifier les anomalies de cet ensemble de données. La figure 7 illustre ceci via une capture d'écran de Cortex XDR prise au cours de l'étape 5.C.2 de l'évaluation. Ici, nous observons une chaîne d'attaque détaillée par l'intermédiaire d'une vue croisée de plusieurs hôtes, qui montre que l'attaquant s'est déplacé latéralement de Linux à Windows via le protocole SMB. Cette vue rassemble les données issues des terminaux et des réseaux. Grâce à notre moteur d'analyses, Cortex XDR a pu détecter la technique de Mouvement latéral.

La figure 8 propose un autre exemple correspondant à l'étape 17.A.6 de l'évaluation, où l'on peut voir que du code est injecté via un appel de procédure distante (RPC) au sein d'une session chiffrée HTTPS. Notre solution a généré une détection en surveillant les appels RPC en tant que source de données, malgré le chiffrement et les tentatives de dissimulation via un changement de port. Résultat : l'utilisateur obtient une visibilité sur la connexion de commande et contrôle (CnC). Ce niveau de transparence est dû à la surveillance détaillée des appels RPC via l'agent Cortex XDR.

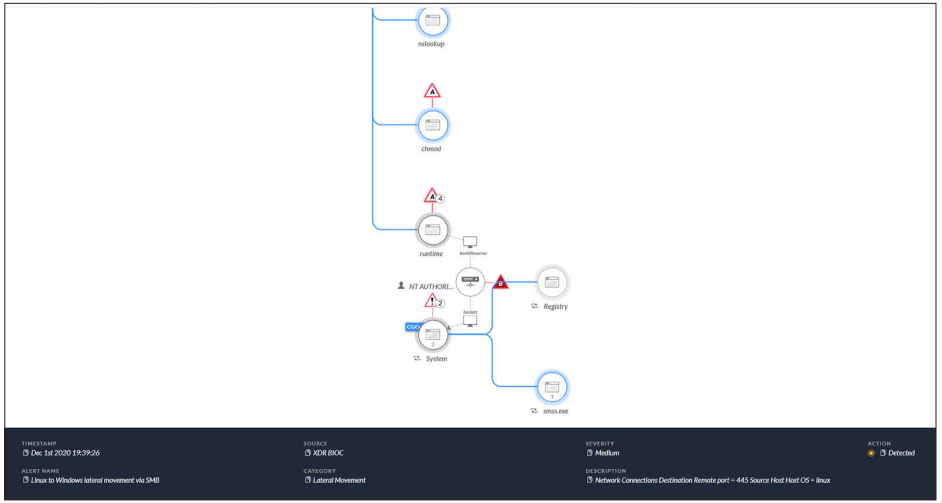


Figure 7 : Vue croisée d'une chaîne d'attaque à l'étape 5.C.2

CORTEX XDR BY PALO ALTO NETWORKS

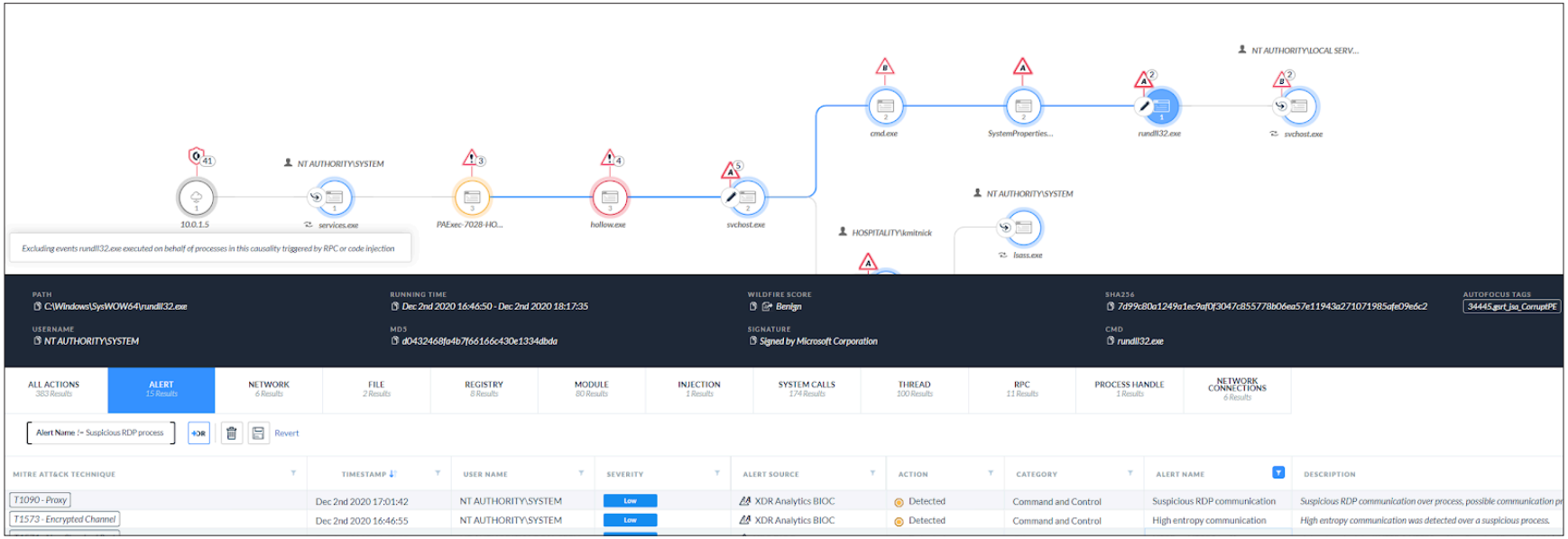


Figure 8 : À l'étape 17.A.6, Cortex XDR a surveillé les appels RPC passés dans une session HTTPS malgré les tentatives de dissimulation

CORTEX XDR BY PALO ALTO NETWORKS

En rassemblant les données des terminaux et les données réseau contenant des informations App-ID™, Cortex XDR a ainsi pu identifier le moment où l'équipe Red Team de MITRE a effectué un mouvement latéral via SSH entre les hôtes Windows et Linux. C'est ce que montre l'étape 5.B.1 de l'évaluation (figure 9), où Cortex XDR a su fournir une visibilité sur les modalités de latéralisation de l'attaquant pour révéler les protocoles utilisés.

Ces quelques exemples confirment que l'avantage de Cortex XDR ne se résume pas aux chiffres de détection fournis dans les résultats de l'évaluation. Notre solution offre une représentation précise et complète d'une attaque, avec toutes ses subtilités, en collectant des données de multiples sources. Elle exploite ensuite notre moteur d'analyses afin de proposer à l'administrateur une vue de causalité intégrale, sans devoir passer par une investigation et une corrélation manuelles.

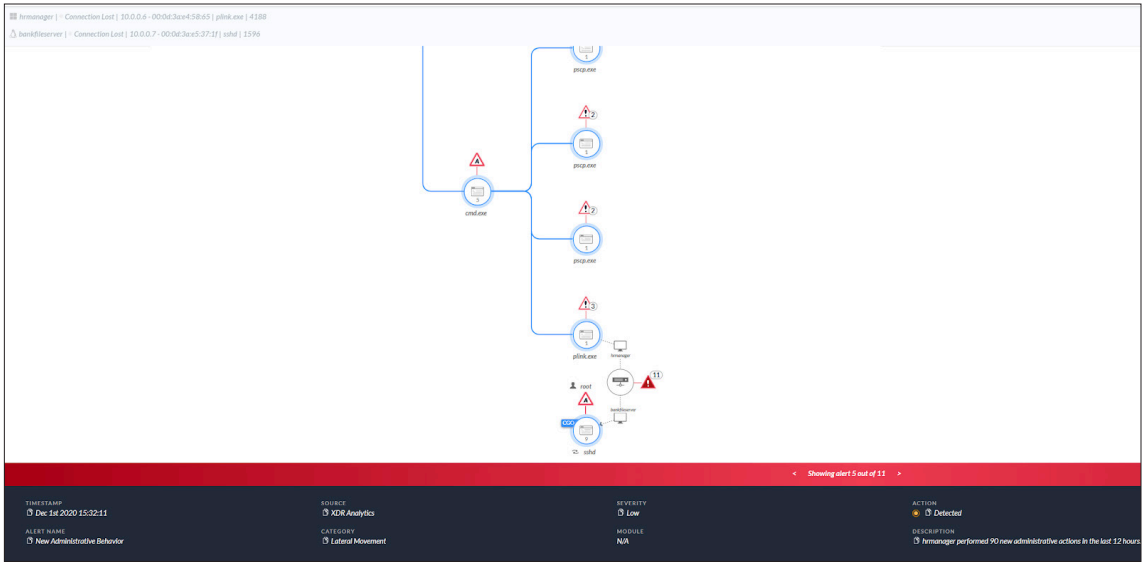


Figure 9 : Mouvement latéral de Windows vers Linux via SSH à l'étape 5.B.1

CORTEX XDR BY PALO ALTO NETWORKS

Pour aller plus loin

Nous savons que l'interprétation des résultats MITRE ATT&CK n'est pas toujours aisée pour les équipes de sécurité. Aussi, nous vous encourageons à parcourir également cet article (en anglais) de Josh Zelonis, Field CTO chez Palo Alto Networks. Sa lecture vous aidera à mieux comprendre les nuances de l'évaluation grâce à une explication approfondie des métriques de visibilité et d'analyse.

Si vous souhaitez en savoir plus sur les scénarios d'attaque émulés au cours de cette évaluation, ainsi que sur les technologies les plus à même de vous protéger et de détecter ces techniques, demandez à visionner notre webinar en replay Carbanak+FIN7: MITRE ATT&CK Results Unpacked (Carbanak+FIN7 : décryptage des résultats MITRE ATT&CK).

Ne ratez pas le train du XDR

Les solutions étendues de détection et de réponse (XDR) sont de plus en plus en vogue sur le marché. Envie de savoir pourquoi ? Téléchargez notre *eBook consacré au XDR*. Au sommaire :

- Limites des systèmes de détection et de réponse actuels
- Exemples concrets des capacités du XDR à améliorer les opérations de sécurité
- Définition et principaux critères d'évaluation des solutions XDR

Plus d'infos sur MITRE

Pour plus d'informations sur le framework ATT&CK, rendez-vous sur MITRE.org. Vous pouvez également utiliser l'outil ATT&CK Navigator afin de parcourir, annoter et visualiser les techniques ATT&CK.

À propos de MITRE Engenuity

Les évaluations ATT&CK de MITRE Engenuity sont financées par les fournisseurs. Elles aident ces derniers ainsi que les utilisateurs finaux à mieux comprendre les capacités d'un produit de sécurité face au framework public ATT&CK®. La base de connaissances ATT&CK, conçue et maintenue par MITRE, s'appuie sur des signalements réels de tactiques et de techniques employées par les cyberattaquants. Accessible gratuitement, elle est plébiscitée par les professionnels de la sécurité dans l'industrie et les pouvoirs publics qui la consultent afin de combler des lacunes en matière de visibilité, de défense ou de processus, et donc de renforcer leur protection réseau. La méthodologie et les résultats de MITRE Engenuity sont rendus publics pour que les entreprises puissent mener à bien des analyses et aboutir à leurs propres interprétations. Ces évaluations ne représentent aucun classement ni cautionnement.

MITRE ENGENUITY™

A Foundation for Public Good

Références

1. « Detection and Protection Categories », ATT&CK Evaluations, MITRE Engenuity, consulté le 21 mai 2021, https://attackevals.mitre-engenuity.org/enterprise/carbanak_fin7/#detection-categories.
2. Ibid.
3. Ibid.

paloalto® NETWORKS

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam
Pays-Bas

+31 20 888 1883.

www.paloaltonetworks.fr

cortex_eb_essential-guide-mitre-round-3-052621-fr