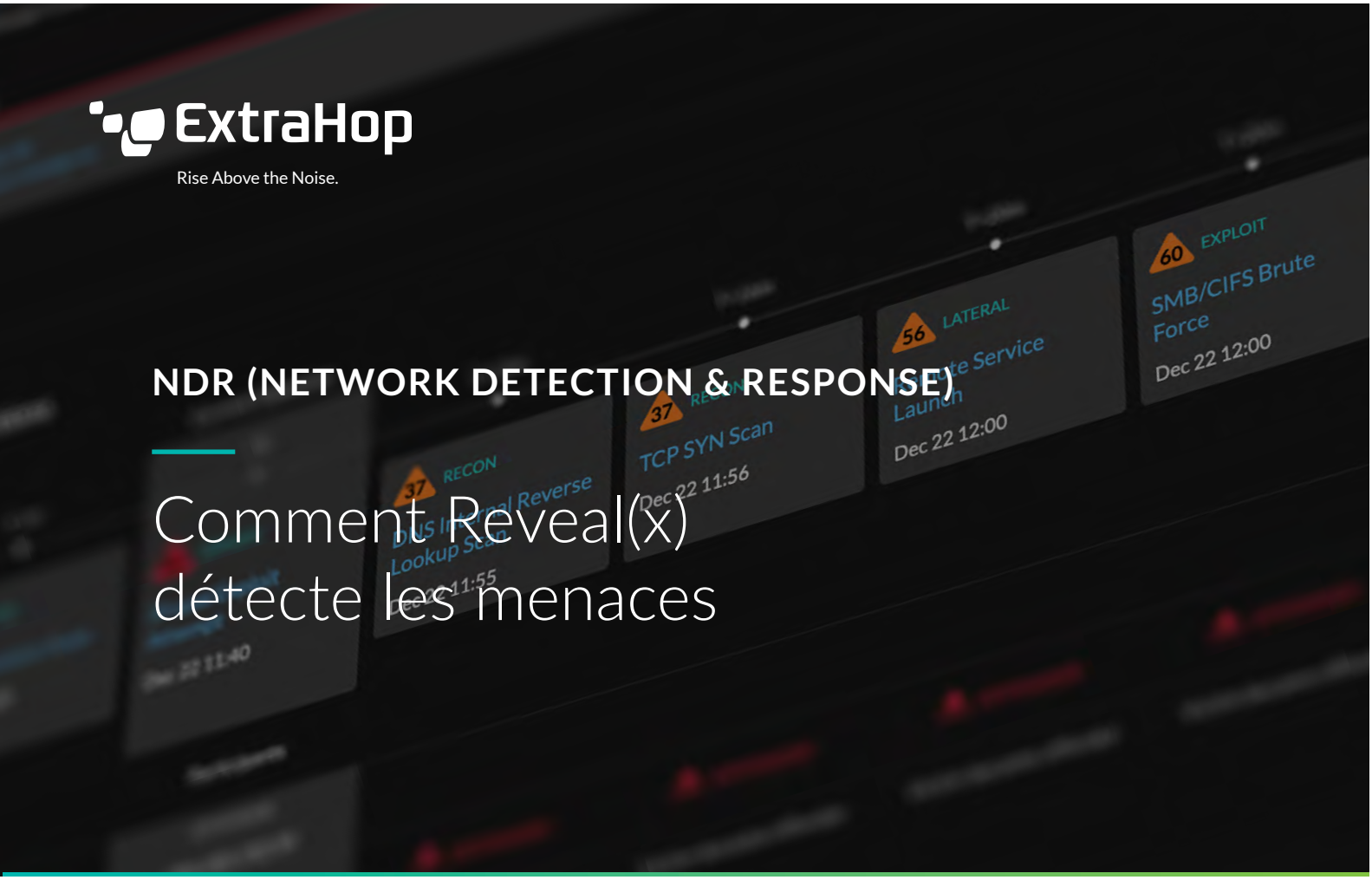
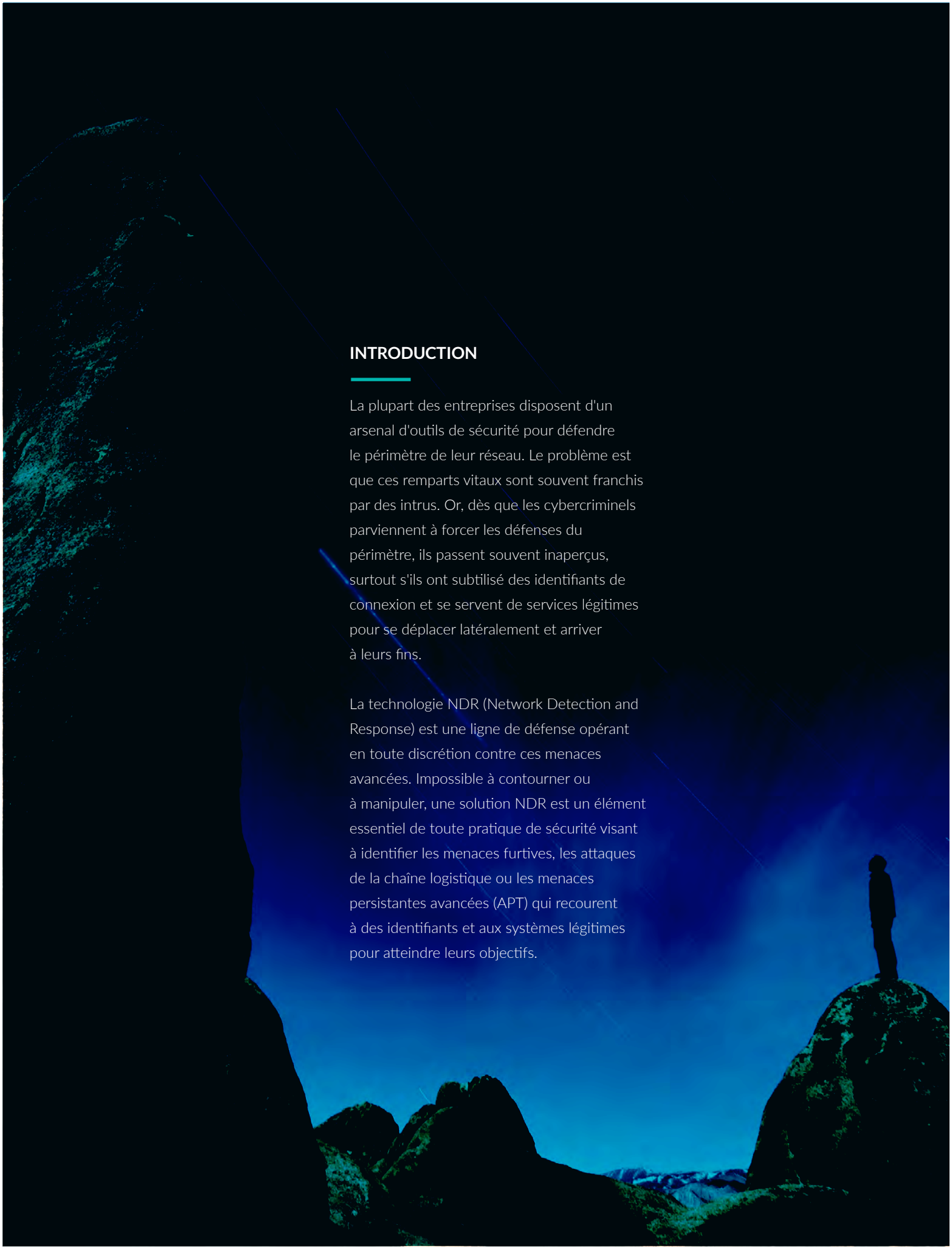


RÉSUMÉ

Ce livre blanc présente Reveal(x), la solution NDR (Network Detection & Response) d'ExtraHop qui offre des fonctionnalités de détection après compromission et une sécurité périmétrique renforcée, avec une précision supérieure aux systèmes de détection d'intrusion (IDS) classiques.

Ce document explore les aspects techniques de Reveal(x) qui permettent aux équipes de sécurité de neutraliser les menaces dans un délai particulièrement court. Grâce à une approche à large spectre alliant détection en temps réel des vulnérabilités et analyse comportementale pilotée par Machine Learning, la solution identifie les tactiques, techniques et procédures (TTP) furtives des attaquants après compromission.

SOMMAIRE



INTRODUCTION

La plupart des entreprises disposent d'un arsenal d'outils de sécurité pour défendre le périmètre de leur réseau. Le problème est que ces remparts vitaux sont souvent franchis par des intrus. Or, dès que les cybercriminels parviennent à forcer les défenses du périmètre, ils passent souvent inaperçus, surtout s'ils ont subtilisé des identifiants de connexion et se servent de services légitimes pour se déplacer latéralement et arriver à leurs fins.

La technologie NDR (Network Detection and Response) est une ligne de défense opérant en toute discrétion contre ces menaces avancées. Impossible à contourner ou à manipuler, une solution NDR est un élément essentiel de toute pratique de sécurité visant à identifier les menaces furtives, les attaques de la chaîne logistique ou les menaces persistantes avancées (APT) qui recourent à des identifiants et aux systèmes légitimes pour atteindre leurs objectifs.

COMMENT REVEAL(X) DÉTECTE LES MENACES

> “ ExtraHop Reveal(x) réduit de 50 % le délai de détection des menaces et de 84 % celui de leur neutralisation.
>
> **FORRESTER, RAPPORT *TOTAL ECONOMIC IMPACT***

Le réseau est l'endroit idéal pour détecter ces activités malveillantes se produisant après la compromission initiale, et ce pour plusieurs raisons :

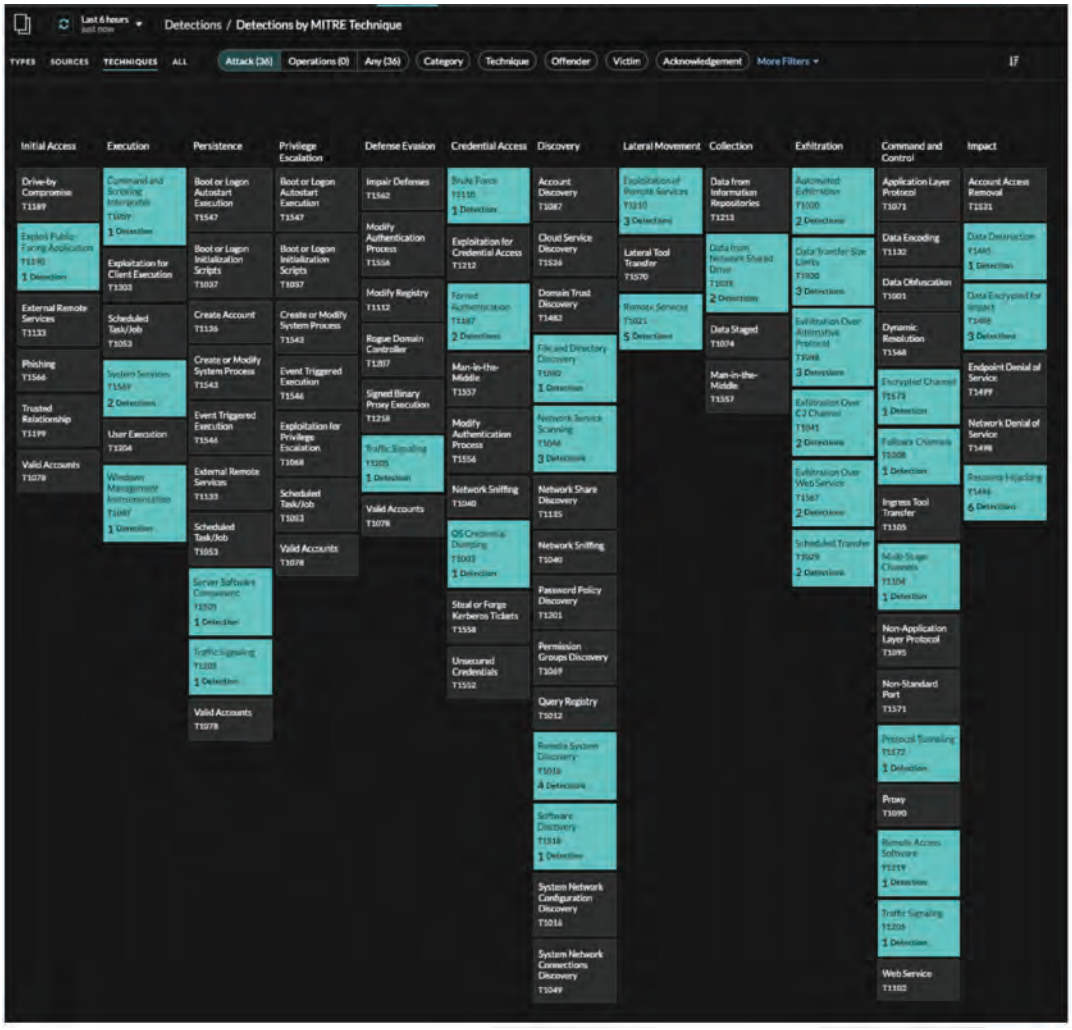
- **Le réseau ne cache rien s'il est placé sous observation.** Les données de journalisation et des endpoints sont utiles à la détection des menaces, mais il est possible de les désactiver, de les contourner, voire de les modifier. Le trafic réseau surveillé de façon passive, en revanche, échappe à ces tentatives d'altération. Les cybercriminels n'ont aucun moyen de savoir si leur activité sur le réseau fait l'objet d'un suivi.
- **Le comportement des pirates sur le réseau et les techniques qu'ils déploient ne sont pas aussi variés et polymorphes que sur les endpoints.** Les cybercriminels ont une foule de moyens à leur disposition pour exécuter du code à distance sur un système et voler des données, mais les techniques d'exfiltration des données via le réseau ne sont pas légion. Avec ces comportements réseau dans le collimateur, il y a plus de probabilités de confondre un attaquant. On peut utiliser les signaux réseau pour détecter les diverses tactiques, techniques et procédures (TTP) déployées par les cybercriminels, à chaque étape du framework MITRE ATT&CK.
- **Le réseau offre une visibilité plus étendue et plus approfondie que les autres options.** Il est possible de découvrir et de surveiller tout équipement communiquant sur le réseau, et ce dès son apparition. Les communications réseau de l'équipement comportent des détails identifiables, dont les utilisateurs, les logiciels, les systèmes d'exploitation, etc.

Reveal(x) assure des détections périmétriques améliorées, plus précises que la détection d'intrusion traditionnelle, tout en offrant une couche de défense supplémentaire vitale en cas d'intrusion. Sa mission est de détecter l'activité pendant tout le déroulement de l'attaque. La solution repère notamment les activités problématiques après compromission, comme l'usage abusif d'appels de procédure distante Windows, ou le comportement anormal d'équipements ou d'utilisateurs à privilèges faibles. Grâce à cette approche comportementale de la détection, il est possible d'identifier efficacement les attaques, moyennant un taux de faux positifs nettement plus faible qu'avec les anciens systèmes de détection d'intrusion (IDS) basés sur les signatures. Ces derniers génèrent un volume d'alertes trop élevé pour être vraiment rentables, mais subsistent pourtant dans beaucoup d'environnements d'entreprise. Reveal(x) s'acquitte des mêmes missions qu'un IDS, mais va plus loin encore en offrant un contexte plus étoffé et plus de fiabilité. Cette solution assure ainsi une protection contre un grand nombre de tactiques, techniques et procédures (TTP) des attaquants pour toutes les catégories du framework MITRE ATT&CK, avec lequel il est intégré.

“

L'un des pires cauchemars [des attaquants], c'est un TAP réseau hors bande qui capture vraiment toutes les données et comprend les comportements anormaux, surveillé par une personne qui y prête toute l'attention voulue. Vous devez maîtriser votre réseau. Connaissez-le sur le bout des doigts, car les pirates ne se gêneront pas pour l'étudier.

ROB JOYCE, FORMER HEAD OF NSA TAILORED ACCESS OPERATIONS



Le framework MITRE ATT&CK est intégré à l'interface NDR de Reveal(x).

Ce livre blanc explique comment Reveal(x) détecte les menaces à tous les stades du déroulement des attaques. Nous expliquerons ici les différents types de détecteurs que nous proposons pour la reconnaissance, l'exploitation, le déplacement latéral, les activités Command & Control, l'élévation des privilèges réseau et l'exfiltration de données, pour ne citer que quelques-unes des tactiques, techniques et procédures des attaquants.

- Reconnaissance
- Exploitation initiale
- Implantation durable
- Installation d'outils
- Déplacement latéral
- Collecte des données exfiltrées et exploitation

SPECTRE DES DÉTECTIONS

Reveal(x) met en œuvre une foule de méthodes, notamment la détection s'appuyant sur des règles, l'analyse comportementale par Machine Learning, l'analyse au sein de groupe de pairs et l'apprentissage profond pour détecter l'ensemble des activités liées à une attaque. Au lieu de s'appuyer sur une seule méthode, cette panoplie de techniques couvre de manière plus globale les tactiques, techniques et procédures (TTP) des attaquants.

	Bonnes pratiques de sécurité L'activité enfreint la politique de sécurité, s'écarte des bonnes pratiques de sécurité ou présente un risque. Citons par exemple les ports, les protocoles et les services vulnérables ou non conformes.	**Attaques connues** Adresses IP, domaines, noms de fichiers, chaînes de charge active ou comportements de protocole observés lors d'attaques antérieures.	**Attaques inconnues** Attaques sans élément d'identification connu au préalable, mais qui présentent un comportement anormal à rapprocher d'un stade de déroulement d'une attaque.
Basées sur des règles prédéfinies	Les détections s'appuyant sur des règles identifient les problèmes en comparant les comportements observés sur le réseau aux bonnes pratiques en matière de sécurité. Grâce à cette approche, il est possible d'exposer des risques tels que l'utilisation du protocole vulnérable SMBv1 ou des mots de passe envoyés en clair, etc.	À l'instar des règles des systèmes de détection d'intrusion (IDS), Reveal(x) met en œuvre une logique de détection complexe pour identifier les attaques connues à leurs attributs. Cette logique permet d'identifier la plupart des exploitations de vulnérabilités qui utilisent le réseau, ainsi que les techniques de déplacement latéral employées. Développées par les chercheurs en menaces d'ExtraHop, ces détections basées sur des règles sont fournies et mises à jour via le cloud.	Sans objet.
Basées sur des règles personnalisées	Les entreprises peuvent aussi créer des détections reposant sur des règles personnalisées pour identifier des violations de politiques, par exemple le déplacement de données en clair entre des segments de réseau abritant des données médicales ou à caractère personnel. Ces règles peuvent être propres à chaque environnement. Reveal(x) comporte une fonctionnalité d'écriture de scripts pour une analyse en temps réel des protocoles d'entreprise.	Les clients peuvent aussi créer des détecteurs pour identifier les menaces et limiter les risques propres à leur environnement ou à leur entreprise, gage d'une couverture totale.	Les détections basées sur des règles personnalisées peuvent faire office de « déclencheurs » pour protéger les actifs critiques, notamment les bases de données et serveurs de fichiers importants. Les entreprises peuvent créer des détections basées sur des règles personnalisées qui se déclenchent dès qu'un équipement se connecte en dehors d'une plage d'adresses IP prescrite ou sur plusieurs segments réseau.
Machine Learning	Sans objet.	Reveal(x) utilise le Machine Learning pour modéliser les comportements des entités sur le réseau et identifier en contexte les comportements révélateurs de techniques d'attaque connues.	Reveal(x) déploie plusieurs techniques de Machine Learning pour détecter les activités malveillantes sur la base de comportements anormaux, notamment les dérogations par rapport à un groupe de pairs, l'élévation de privilèges, etc.

Détections basées sur des règles prédéfinies

Reveal(x) assure une détection basée sur des règles, similaire à celle d'un système de détection d'intrusion traditionnel, à ceci près que la solution repère des schémas comportementaux, et non des hachages MD5 ou autres méthodes de signature faciles à éluder. Prenons l'exemple du malware TrickBot. Une approche de détection basée sur la signature IDS ne rechercherait que des chaînes codées de manière irréversible, spécifiques aux modules du programme, comme « </dinj> », une chaîne rencontrée dans le module dllinject de certains variants de Trickbot. C'est une chaîne facile à modifier. L'attaquant peut la renommer comme bon lui semble pour passer sous les radars. Une approche comportementale de détection de TrickBot s'appuierait sur l'observation des caractéristiques de la connexion SSL lancée par le malware, comme l'utilisation d'un certificat autosigné de création très récente où Cert Issuer et Cert Subject seraient à zéro. Il serait nettement plus difficile pour l'attaquant d'atteindre ses objectifs s'il devait modifier ces comportements. Cette approche de la détection permet d'identifier des tactiques et des techniques connues (dont les tentatives d'exploitation de vulnérabilités et les outils de piratage), tout en étant nettement plus compliquée à contourner qu'une mise en correspondance de signatures avec comparaison de chaînes. Développée par les chercheurs en menaces d'ExtraHop, la logique qui sous-tend les détections est transmise aux capteurs lors de mises à jour dans le cloud. Les détecteurs intégrés sont actualisés en permanence dans le cloud. Tous les clients disposent ainsi des versions les plus récentes dans les plus brefs délais, dès que de nouvelles détections de vulnérabilités sont disponibles.

Reveal(x) déchiffre le trafic et inspecte la charge active des transactions. L'équipe d'experts en menaces peut ainsi accéder aux indicateurs fiables d'une attaque (comme le champ post_render d'une demande HTTP) qui passeraient inaperçus sans déchiffrement du trafic ou si l'analyse ne livrait pas les détails de la charge active.

*Reveal(x) examine des détails tels que le champ **post_render** des transactions HTTP pour détecter de manière fiable les tentatives d'exploitation de failles.*

“

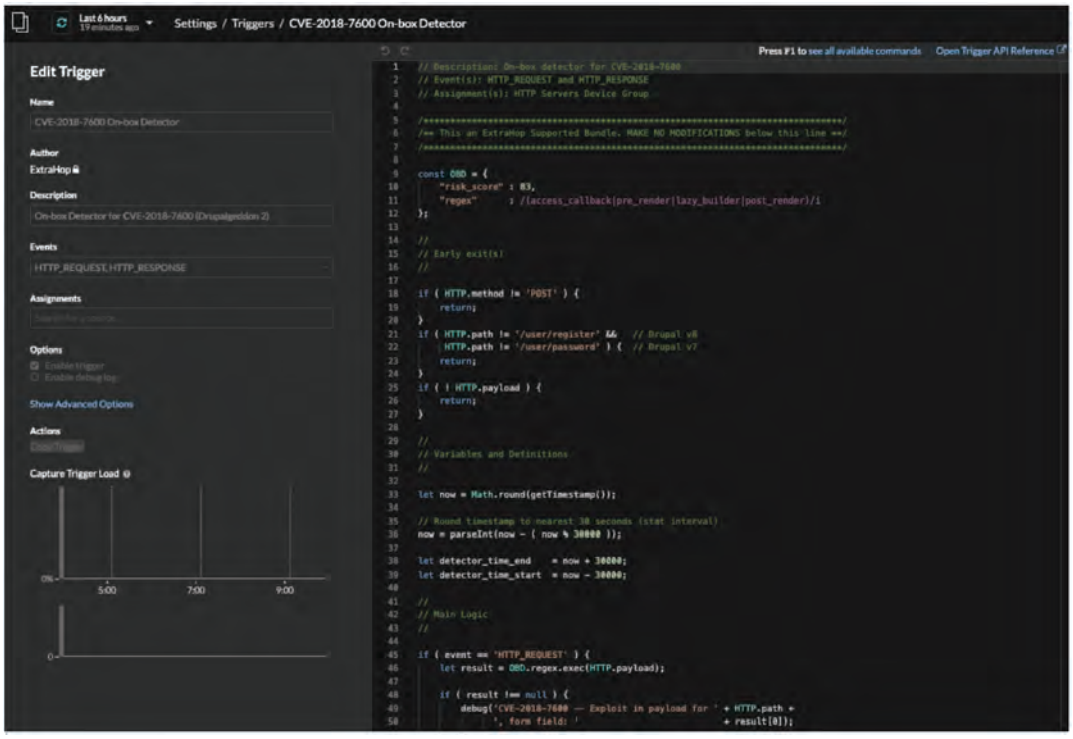
De nos jours, la détection des menaces dépend nettement plus du contexte local qu'on ne le croit.

ANTON CHUVAKIN, ANCIEN ANALYSTE DE GARTNER

Détections basées sur des règles personnalisées

Même avec des centaines de détecteurs prêts à l'emploi, aucune solution NDR ne peut prendre en compte toutes les exigences particulières des entreprises. Pour répondre aux besoins de chaque structure, Reveal(x) propose aux utilisateurs de créer des détections personnalisées à l'aide d'un moteur de scripts sophistiqué. Les entreprises peuvent notamment créer des détections pour des violations de politiques propres à des serveurs isolés ou à des grappes de serveurs qui hébergent des applications ou des données critiques. Il est aussi possible de lier les détections personnalisées au framework MITRE ATT&CK et de les afficher dans l'interface de la solution selon la représentation en matrice correspondante (MITRE ATT&CK Matrix).

Le moteur de scripts de Reveal(x) permet d'accéder à une logique complexe appliquée à l'analyse à états et en temps réel du trafic réseau — dont l'accès à plus de 5 000 indicateurs intégrés, 50 types d'événements, ainsi qu'un accès direct à la charge active en vue d'une analyse personnalisée. Les utilisateurs peuvent programmer des événements déclencheurs en JavaScript pour créer leurs détections personnalisées et ainsi répondre aux besoins de leur entreprise.



Machine Learning

Le Machine Learning (ML) présente l'avantage de pouvoir détecter des comportements d'attaque qui échappent aux méthodes basées sur les règles ou les signatures, et ce avec une plus grande précision en matière de détection des tactiques, techniques et procédures d'attaque connues.

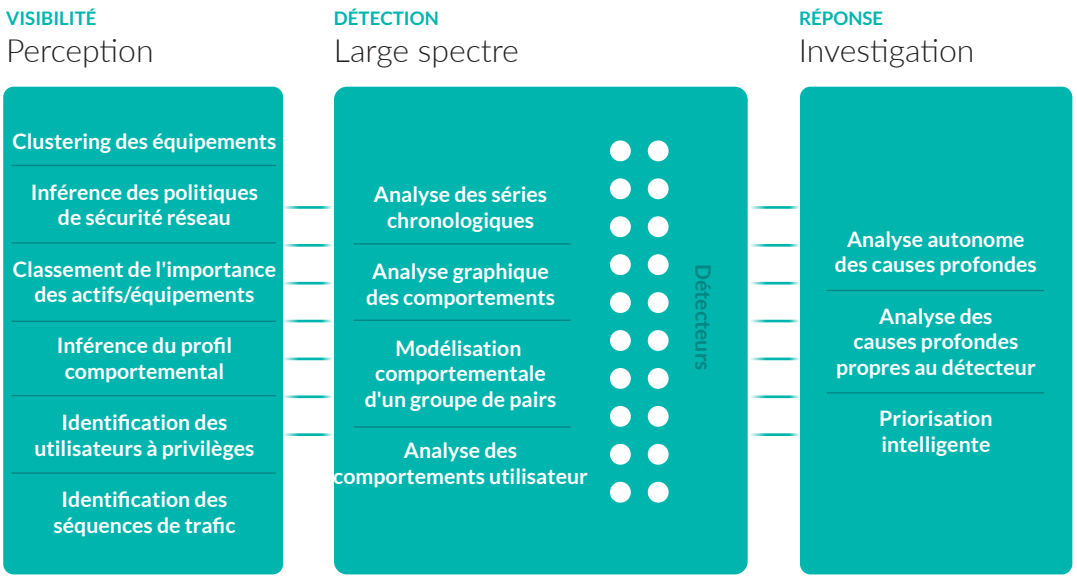
Les attaquants tendent à privilégier les tactiques « live off the land », qui consistent à exploiter des services légitimes pour opérer dans la clandestinité. Comment les outils IDS traditionnels peuvent-ils détecter un attaquant qui se fond dans la masse en utilisant des identifiants de connexion et des services légitimes ? C'est là que le Machine Learning entre en scène. Il détecte les attaques dans un environnement en modélisant le comportement de chaque entité et en identifiant en contexte les comportements révélateurs de techniques d'attaque connues. Prenons l'exemple de PsExec, un utilitaire de gestion utilisé couramment par les administrateurs IT. Les attaquants y ont aussi recours, mais la diffusion d'alertes à chaque utilisation de PsExec serait aussi inutile qu'intempestive. Le moteur ML de Reveal(x) observe l'historique de comportement des équipements sur le réseau et repère les cas d'utilisation inattendue et malveillante de PsExec en se basant sur des indices contextuels, notamment la propriété et le rôle de l'équipement, l'heure d'accès, etc.

Reveal(x) tire parti de l'analyse et de la détection optimisées par le Machine Learning dans trois sous-systèmes : perception, détection et investigation.

Reveal(x) utilise le ML pour détecter les attaques, mais aussi pour aider les analystes à les examiner et à y répondre plus rapidement en automatisant la collecte d'informations et en replaçant ces informations en contexte.

Pour y parvenir, ExtraHop articule son analyse ML autour d'une approche recourant à plusieurs sous-systèmes, très similaire à celle des véhicules autonomes, qui orchestre une foule de sous-systèmes ML sophistiqués et brevetés, prévus pour extraire des informations, identifier les menaces et les remettre en contexte.

Reveal(x) tire parti de l'analyse et de la détection optimisées par le Machine Learning dans trois sous-systèmes : perception, détection et investigation. Chaque sous-système présente plusieurs composants aux fonctionnalités distinctes. Les composants ML d'un même sous-système et de sous-systèmes différents collaborent et échangent des données et des conclusions :



Par exemple, le ML de Reveal(x) analyse les séquences de trafic réseau pour identifier les actifs à privilèges au sein de votre environnement. Reveal(x) peut ainsi savoir quand un équipement procède à une élévation de privilèges anormale. Ces fonctionnalités de ML peuvent également servir à cerner automatiquement le degré de criticité d'un équipement donné en observant son comportement et ses habitudes d'accès et en mettant dynamiquement à jour le score de risque des détections impliquant des équipements critiques.

Reveal(x) peut aussi repérer quand, contre toute attente, un équipement adopte un comportement différent de ses pairs — par exemple, quand le téléphone d'une salle de réunion tente de lancer une session SSH, ce qu'aucun autre téléphone de ce type n'a jamais fait dans cet environnement.

Par rapport à la détection basée sur des règles de type IDS, le Machine Learning a l'avantage de mémoriser les caractéristiques d'une situation normale. La détection IDS repose sur les indicateurs statiques présents dans le trafic réseau sur un court laps de temps. Reveal(x), lui, analyse le comportement sur plusieurs fenêtres temporelles à l'aide de modèles prédictifs. Grâce à ces modèles, la solution peut détecter avec une plus grande précision des activités comme le regroupement et l'exfiltration de données. Elle sait aussi si le trafic dans la base de données d'un client est normal.

> “Nous n'avons pas de meilleurs algorithmes que les autres ; nous avons simplement plus de données.
>
> **PETER NORVIG, DIRECTEUR DE RECHERCHE, GOOGLE**

Reveal(x) génère des « fiches de détection » qui rassemblent toutes les informations d'investigation utiles, dont les détails sont faciles à consulter en quelques clics. Si le type d'attaque est connu, la fiche met en correspondance la détection avec le framework MITRE ATT&CK, fournissant ainsi aux analystes une indication sur le stade de l'attaque en cours.

Dans le cas de détections par Machine Learning, la fiche Reveal(x) précise également le comportement ayant déclenché la détection ; les renseignements de ce type permettent de mieux comprendre les mécanismes du Machine Learning de Reveal(x), ce qui renforce la confiance des utilisateurs.

Le Machine Learning n'est-il pas utilisé par tous, à l'heure actuelle ?

Non. L'utilisation abusive des termes « Machine Learning » et « intelligence artificielle » dans les documents marketing peut donner l'illusion que le ML est partout. Néanmoins, tous les produits n'ont pas recours à ces techniques. Plus important encore, toutes les techniques de ML ne se valent pas. En matière de cybersécurité, on trouve tous les niveaux de qualité dans les approches de ML.

En général, trois fonctionnalités distinguent l'implémentation du Machine Learning version ExtraHop des autres produits de sécurité :

1. **Chez ExtraHop, les fonctionnalités de Machine Learning sont plus nombreuses et de meilleure qualité.** L'efficacité du Machine Learning dépend fortement des éléments qui alimentent les algorithmes. Citons les comportements et les interactions des protocoles réseau, comme les méthodes transactionnelles des bases de données, les requêtes SQL, les comportements des utilisateurs, etc. Reveal(x) extrait plus de 5 000 caractéristiques du trafic réseau pour nourrir le Machine Learning. Les capteurs ExtraHop sont spécialement conçus pour procéder à cette extraction à des débits atteignant 100 Gbit/s.

> Sans visibilité sur le trafic chiffré dans l'environnement réseau, les analystes naviguent à l'aveuglette. Les analystes peuvent configurer Reveal(x) pour tenir le trafic chiffré à l'œil, même s'il est protégé par la confidentialité persistante.
>
> **DAVE SHACKLEFORD, ÉVALUATION PRODUIT DE REVEAL(X) PAR LE SANS INSTITUTE**

2. **ExtraHop tire parti de la vitesse et de l'évolutivité du cloud.** Reveal(x) s'appuie sur les ressources de calcul évolutives du cloud pour entraîner et exécuter en permanence des centaines de modèles de Machine Learning — une approche unique en son genre sur le marché NDR. Reveal(x) peut ainsi assurer des détections beaucoup plus sophistiquées et fiables que ses concurrents qui pratiquent le Machine Learning localement sur l'équipement capteur, où les ressources informatiques sont limitées. De plus, l'hébergement dans le cloud permet à ExtraHop de déployer rapidement des mises à jour.
3. **ExtraHop a une plus grande capacité de déchiffrement.** Reveal(x) déchiffre le trafic chiffré jusqu'au chiffrement SSL/TLS 1.3. Il peut accéder aux détails de la couche Application (couche 7 du modèle OSI), dont les messages d'erreur et autres informations relatives à la charge active. Ces dernières données très utiles sont injectées dans les fonctionnalités de Machine Learning.

Pour en savoir plus sur le fonctionnement du Machine Learning dans le cloud mis en œuvre dans Reveal(x), lisez nos articles de blog : *Tricks of the Trade: How Reveal(x) Uses Machine Learning* et *ExtraHop Cloud Scale ML: A Deep Dive*

Données collectées pour améliorer les détections

En plus de l'ensemble des données de base du trafic réseau, complètement réassemblé et analysé en temps réel, Reveal(x) puise dans plusieurs autres sources de données pour améliorer la détection des attaques. Ces données d'amélioration sont fournies automatiquement aux appliances Reveal(x) par des mises à jour dans le cloud.

- **Cyberveille** - Reveal(x) propose un flux de cyberveille sur les menaces, mais les utilisateurs peuvent aussi utiliser leurs propres flux de cyberveille au format STIX. Les correspondances s'affichent dans l'interface utilisateur de Reveal(x).
- **Définitions de ransomwares** - À l'instar des autres malwares, les souches de ransomware présentent des indicateurs : domaines, adresses IP, nom de fichier de la demande de rançon, extensions spéciales données aux fichiers chiffrés, etc.
- **Mises à jour des nœuds Tor** - Reveal(x) surveille les adresses IP associées aux nœuds Tor, utilisés pour masquer l'identité des attaquants.
- **Pistage par empreinte du matériel** - Reveal(x) identifie les marques et modèles d'équipements à l'aide d'un large éventail de techniques — de l'analyse du trafic DHCP jusqu'à l'utilisation d'une demi-douzaine d'autres protocoles.
- **Pistage par empreinte (fingerprinting) des services cloud** - En utilisant des adresses IP et noms d'hôtes connus, Reveal(x) est capable d'identifier des services cloud tels que DropBox, Google Drive, AWS, Azure, etc.
- **Pistage par empreinte (fingerprinting) des logiciels et systèmes d'exploitation** - Presque tous les systèmes d'exploitation et les suites logicielles sur le réseau présentent des empreintes numériques uniques qui peuvent servir à les identifier, souvent avec un degré de détail suffisant pour distinguer les versions majeures ou mineures du logiciel.

SOUTIEN AUX ANALYSTES

Dans le meilleur des mondes, tous les SOC seraient gérés par des analystes dotés de longues années d'expérience et d'une intuition sans faille. La réalité est bien différente. La plupart des équipes de sécurité l'ont compris et sont en train de former des analystes junior. Avec ExtraHop, les analystes SOC peuvent valider les détections en toute confiance et comprendre la gravité potentielle d'un événement, le tout en quelques clics. Pour ce faire, Reveal(x) recueille automatiquement des informations contextuelles propres à chaque détection et les présente aux analystes sous la forme de fiches de détection interactives.

Score de risque	Priorise la détection en fonction de sa gravité.
Framework MITRE ATT&CK	Identifie la tactique, technique ou procédure MITRE ATT&CK à laquelle correspond la détection.
Temps et durée	Indique la série chronologique de la détection par rapport à d'autres événements. Si l'événement est en cours, un marqueur spécial le précise en regard de la détection.
Filtrage des détections des mêmes participants en un seul clic	Si l'attaquant ou la victime figurent dans d'autres détections, la fiche de détection précise le nombre et le type des détections concernées. La fiche comporte un lien vers une liste de détections impliquant les mêmes protagonistes.
Numéro de ticket, statut et collaborateur assigné	Extrait des informations relatives aux tickets d'incident pour éviter aux analystes de devoir effectuer des recherches dans le système de gestion des tickets.
Description de l'attaque	Descriptions de l'attaque résumant la cause du déclenchement de la détection, le modus operandi de l'attaque et sa cible potentielle.
Informations relatives à l'attaquant et à la victime	Informations relatives à l'équipement de l'attaquant et de la victime, dont les rôles, le nom de l'équipement, l'adresse IP et des liens vers des cartes d'activités.
Ressources connexes	Liste des utilisateurs, équipements ou fichiers touchés comportant des liens vers les métadonnées. En ayant une vue d'ensemble des données et équipements concernés par l'événement, les analystes peuvent en mesurer la gravité potentielle.
Indicateurs	Dans le cas des détections basées sur des modèles prédictifs, les détails du protocole (méthode et code statut) s'affichent dans un graphique sparkline pour l'activité du protocole, le comportement normal sur la période et le pic d'activité.
Étapes de l'investigation	Visualisation dynamique sur la carte d'activités de tout le trafic entre les équipements. Recherches automatiquement personnalisées des indicateurs ou des enregistrements, avec affichage des équipements, fichiers, noms d'utilisateur ou transactions associés à la détection. Comparaison des comportements de groupes de pairs filtrée automatiquement. Lien en un clic vers la capture complète de paquets. Ces recherches et filtres isolent des données plus détaillées qui aident souvent les analystes à confirmer une détection précise.
Facteurs inclus dans le score de risque	La méthode de calcul fait intervenir la probabilité que l'attaque se produise, le niveau de qualification requis et les répercussions potentielles pour l'entreprise.
Explication détaillée de l'attaque	Explication de l'attaque précisant notamment son modus operandi et les mobiles éventuels des cybercriminels ; particulièrement utile aux analystes moins expérimentés ou aux autres membres de l'équipe qui ne sont pas des experts en sécurité. Grâce à ces informations, les analystes peuvent gagner le temps qui aurait été nécessaire à la recherche de renseignements en ligne.
Pistes de réduction des risques	Pour chaque détection, une liste de pistes est proposée pour prévenir ou limiter le risque de l'attaque en question.
Liens utiles	Liens vers des pages Web de tiers réputés, comme le framework MITRE ATT&CK, la base de données CVE, OWASP et d'autres ressources répertoriant les tactiques ou techniques. Généralement, les analystes qui examinent une détection recherchent des informations sur Internet. Ces liens permettent de sauter cette étape et sont garants d'informations fiables.
Retour d'information	Les analystes peuvent qualifier les détections d'utiles ou non. Le retour d'information est instantané et exploitable par les équipes ExtraHop actives en data science et en cyberveille.

Données de base sur le type d'attaque, niveau de risque, recommandations de mesures préventives et liens vers les listes MITRE ATT&CK pour les tactiques concernées par la détection.

Données sur la victime et l'attaquant, dont le rôle de l'équipement et son adresse IP.

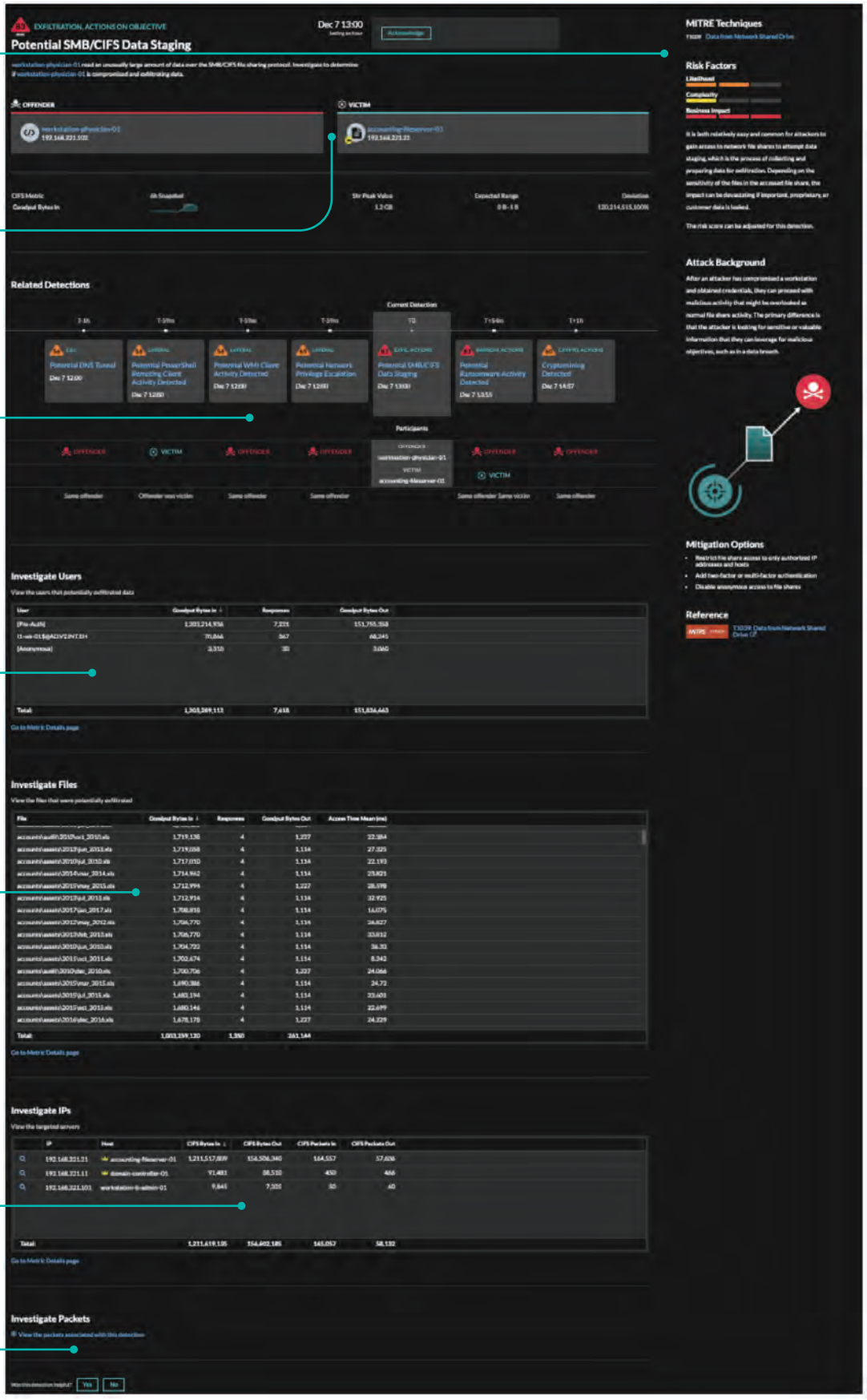
Chronologie des détections connexes indiquant les événements et activités liés à la victime et à l'attaquant.

Utilisateurs concernés par la détection.

Liste de fichiers consultés ou manipulés lors du comportement détecté.

Liste des adresses IP concernées par la détection. Il est possible de cliquer pour obtenir de plus amples informations.

Accès en un clic aux paquets pertinents pour les investigations numériques.



Comprendre facilement les informations contextuelles des équipements

Reveal(x) est également capable d'identifier de façon très détaillée les types et les fonctions des actifs, notamment en inférant la criticité de l'équipement grâce à l'analyse comportementale et en récoltant des informations telles que :

- les systèmes d'exploitation installés sur chaque équipement et le rôle de ce dernier. Reveal(x) peut ainsi déterminer si un équipement est un contrôleur de domaine, un serveur Web, un serveur DNS, une webcam IoT ou un téléphone de salle de réunion (entre autres), simplement en observant son comportement ;
- les utilisateurs qui se sont connectés à chaque équipement ou ont tenté de le faire ;
- l'agent EDR installé sur l'équipement (le cas échéant).

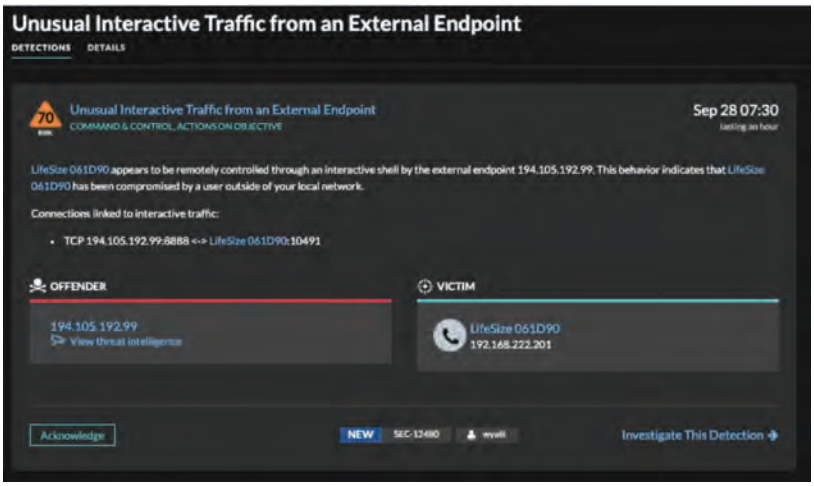
Avec ces fonctionnalités, Reveal(x) peut comparer les comportements dans un groupe d'équipements ou de pairs. Si un téléphone de salle de réunion se met à adopter un comportement inédit pour ce genre d'équipement, il sera considéré comme suspect. En comparant les comportements suspects entre pairs et en déterminant si une attaque vise principalement les équipements IoT, ou l'une ou l'autre catégorie d'équipements, les analystes peuvent cerner la portée d'une attaque et accélérer la réponse et la prévention.

Exemples de workflows Détection-Validation

TRAFIC INTERACTIF INHABITUEL D'UN ENDPOINT EXTERNE

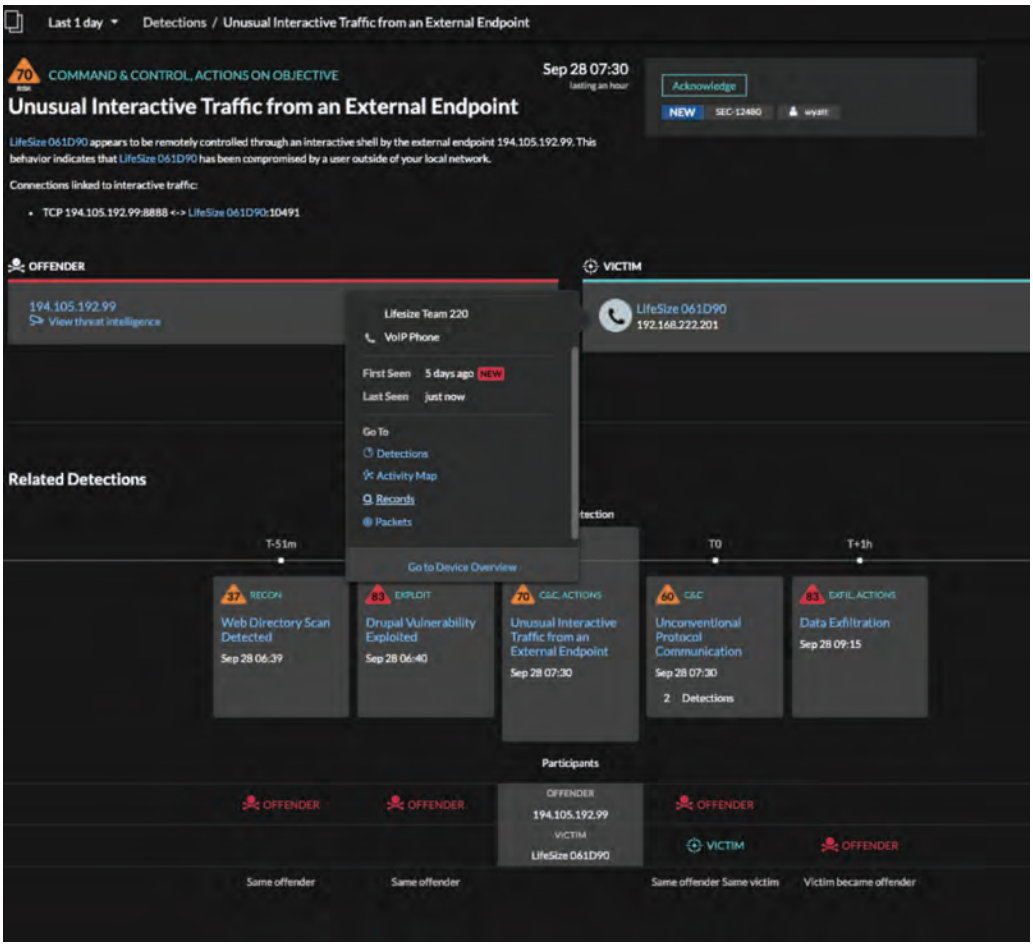
DÉBUT DU WORKFLOW

Cliquez sur « Investigate This Detection » pour connaître les détails et le contexte.



Visualisation des détections connexes, des liens vers la documentation MITRE ATT&CK et OWASP et des informations de cyberveille reprises sur la fiche de détection.

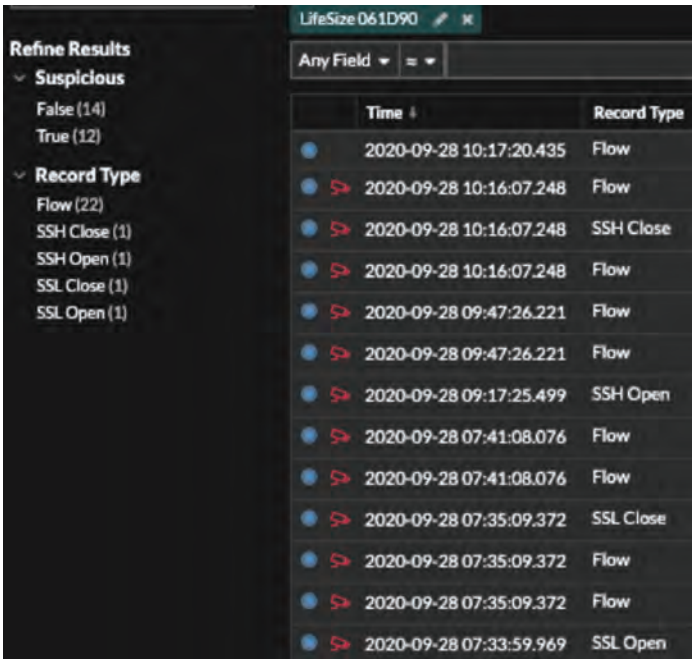
Passez le pointeur de souris sur l'attaquant ou la victime pour accéder aux enregistrements transactionnels complets ou aux paquets pour le trafic détecté.



Les enregistrements transactionnels font état de plusieurs consultations et fermetures rapides de SSH et SSL à partir d'une adresse IP qui correspond à nos informations de veille sur les menaces.

Cette validation s'est faite en deux clics à compter de la détection initiale.

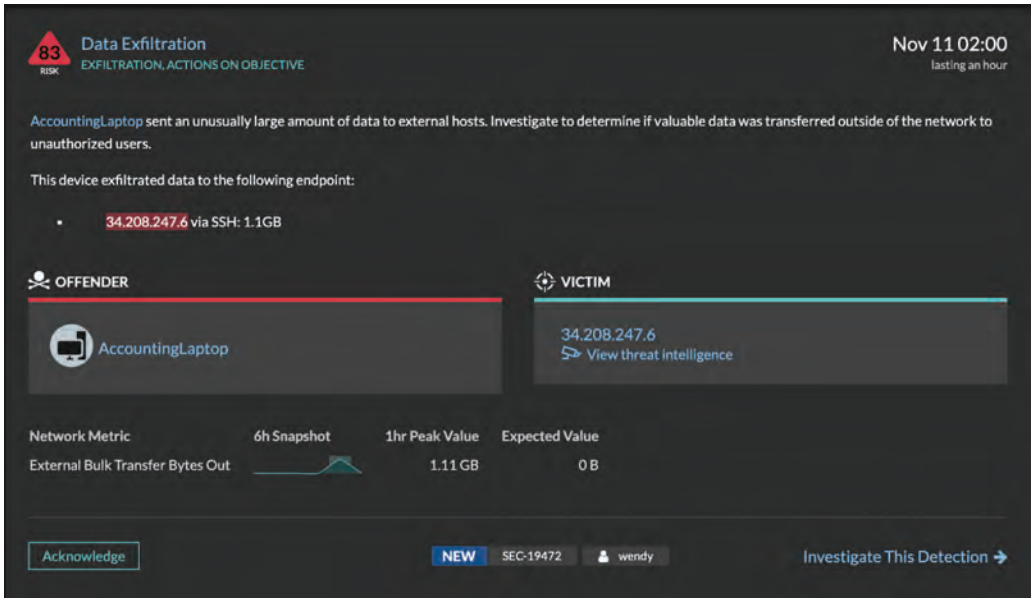
FIN DU WORKFLOW



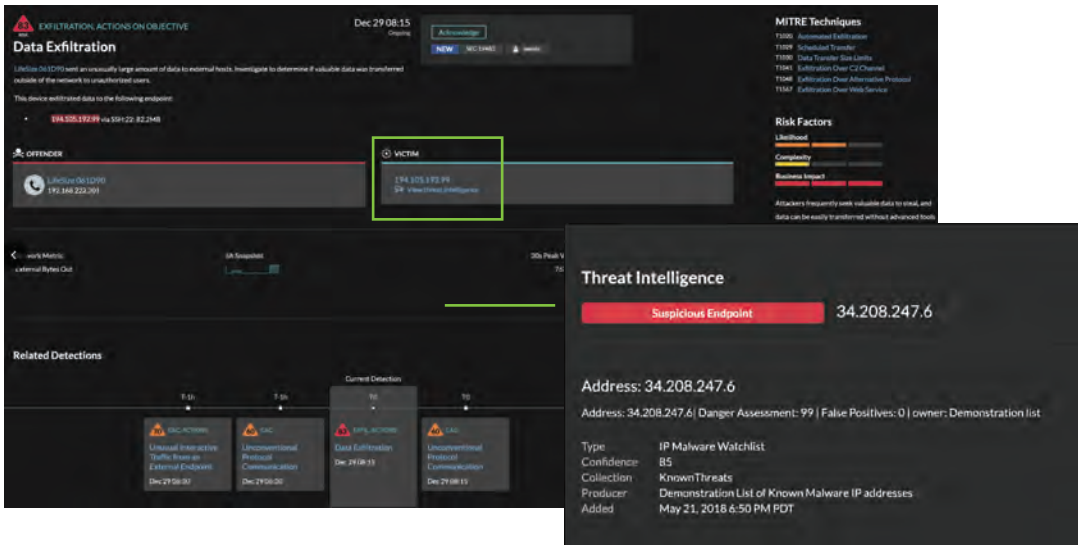
EXFILTRATION DE DONNÉES

DÉBUT DU WORKFLOW

Cliquez sur « Investigate This Detection » pour connaître les détails et le contexte.

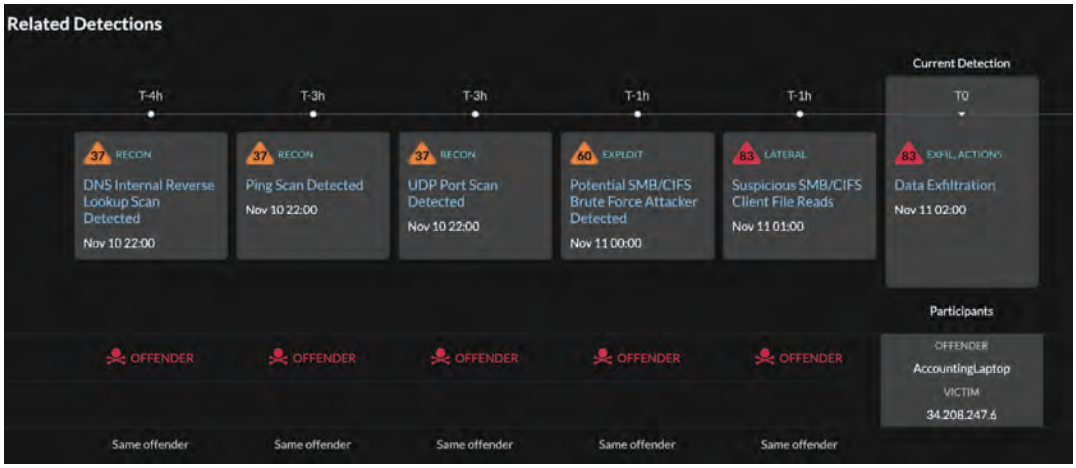


Cliquez sur « View threat intelligence » pour accéder aux informations de cyberveille d'une source externe.

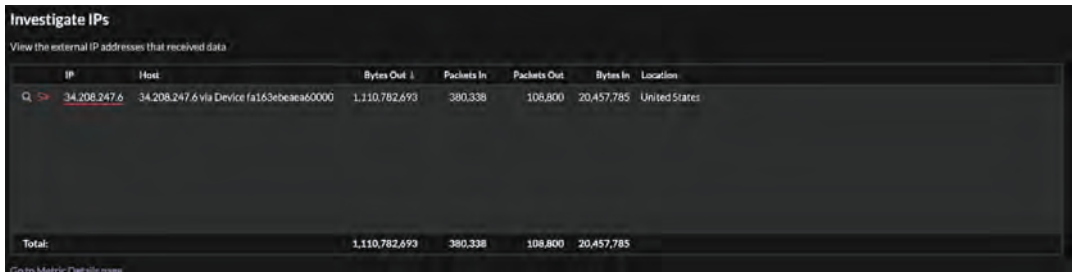


Faites défiler pour voir les détections connexes, les liens vers la documentation MITRE ATT&CK et OWASP et les informations de cyberveille que contient la fiche de détection.

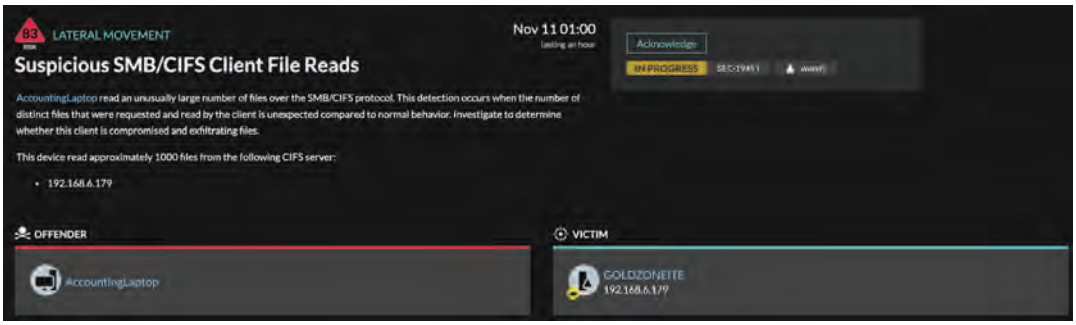
Remarquez les lectures suspectes de fichiers clients SMB/CIFS juste avant la détection d'exfiltration de données.



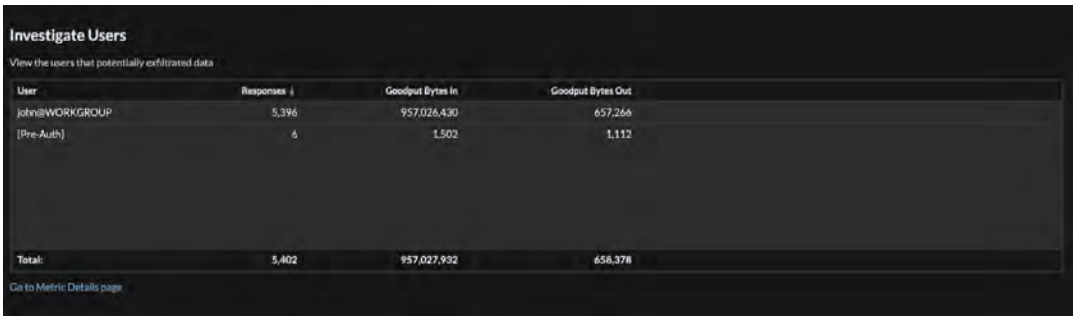
Examinez les adresses IP et les hôtes associés à la détection pour quantifier le trafic et connaître son destinataire.



Cliquez sur « Suspicious SMB/CIFS Client File Reads » dans la chronologie des détections connexes. On voit que AccountingLaptop a interagi.



Sur la base du trafic SMB/CIFS, Reveal(x) est en mesure de désigner l'utilisateur employé par l'attaquant pour s'authentifier sur le serveur et fournit ainsi du contexte sur les comptes potentiellement compromis.



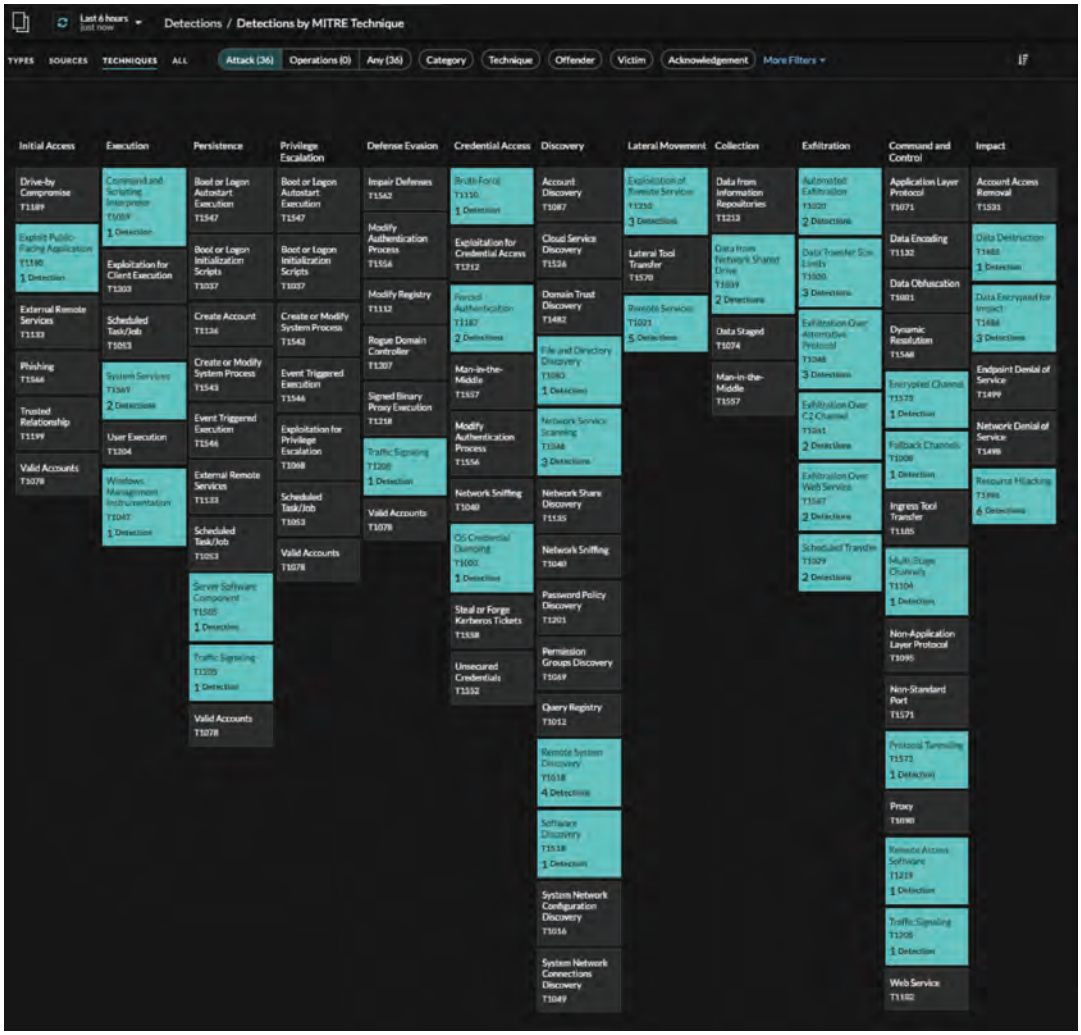
En faisant défiler jusqu'à la section « Investigate Files », on peut obtenir une liste détaillée des fichiers consultés sur le serveur GOLDZONEITE.

FIN DU WORKFLOW

Intégration du framework MITRE ATT&CK

Pour faciliter la tâche d'investigation et de validation des analystes, il faut notamment leur fournir un maximum de contexte. En plus des informations reprises dans chaque fiche de détection, Reveal(x) inscrit les détections dans le contexte plus large du framework MITRE ATT&CK. Les analystes peuvent mettre en concordance la détection et le stade de l'attaque, et prendre connaissance des techniques détectées tout au long de la chaîne d'attaque. Ils peuvent ainsi se faire rapidement une idée des activités des attaquants sur le réseau dans le laps de temps sélectionné. Ces détections sont reprises dans Reveal(x) et sont opérationnelles sans la moindre configuration. Cependant, les analystes peuvent utiliser l'outil de personnalisation pour créer des détections et les mettre en concordance avec le framework MITRE ATT&CK.

La représentation graphique MITRE ATT&CK Matrix a recours à une évolution plus détaillée de la chaîne d'attaque Lockheed Martin pour mettre en correspondance le stade d'une attaque à la technique détectée.



Deux points de vue sur la couverture MITRE ATT&CK :

Type de technique et catégorie

Reveal(x) propose deux grands modes de filtrage des détections en fonction du framework MITRE ATT&CK : le type de technique et la catégorie d'actif.

Le *filtrage par type de technique* affiche toutes les techniques ATT&CK liées aux détections actuelles, ainsi que le nombre de détections associées à cette technique. Les analystes sont alors en mesure de préciser la technique d'attaque qui les intéresse et de visualiser les détections qui y sont liées.

Avec le *filtrage par catégorie*, les analystes peuvent évaluer les détections sous l'angle du stade de l'attaque. Les détections sont filtrées en fonction du stade de l'attaque, quel que soit le type d'actifs auquel elles se rapportent. À titre d'exemple, les détections d'exfiltrations de données peuvent être rattachées à la fois à des équipements IoT et à des endpoints Windows. Ces détections sont valables pour les équipements gérés et non gérés.

CONCLUSION

La détection des menaces est plus que jamais une gageure. Les attaquants se sont adaptés. Ils se jouent des mécanismes de détection d'ancienne génération comme les signatures de hachage et la correspondance littérale de chaînes. Ils ont appris à contourner ou à désactiver la journalisation des activités et autres sources de données.

La technologie NDR tire parti de l'analyse comportementale optimisée par le Machine Learning pour offrir des détections particulièrement fiables et des défenses difficiles à éluder par les attaquants. Mais ne nous croyez pas sur parole, écoutez plutôt Rob Joyce, ancien chef de la division Tailored Access Operations de la NSA, qui a déclaré : « L'un des pires cauchemars [des attaquants], c'est un TAP réseau hors bande qui capture vraiment toutes les données et comprend les comportements anormaux, surveillé par une personne qui y prête toute l'attention voulue. Vous devez maîtriser votre réseau. Connaissez-le sur le bout des doigts, car [les pirates] ne se gêneront pas pour l'étudier. »

Découvrez Reveal(x) par vous-même avec notre démo gratuite en ligne

Pour plus d'informations

Pour en savoir plus sur la façon dont Reveal(x) peut remédier aux principaux incidents de sécurité au sein de votre entreprise, lisez ces articles de blog ou assistez à notre démonstration en ligne gratuite (la seule de ce type sur le marché NDR).

The Tricks of Our Trade: How Reveal(x) Uses Machine Learning to Detect Threats

ExtraHop Cloud-Scale ML: A Deep Dive

Supervised vs. Unsupervised Machine Learning: Which is Better for Threat Detection, and Why?

Putting Machine Learning to Work for Enterprise IoT Security

ANNEXE A

Exemples de fonctions de Machine Learning au niveau de la couche Application

La plupart des NDR ne proposent qu'une analyse limitée de la couche Application (couche 7). Ils n'ont donc pas accès à des fonctionnalités de Machine Learning très pertinentes. Vous trouverez ci-dessous quelques exemples de fonctions axées sur la couche Application que permet d'analyser Reveal(x), ainsi que des exemples de leur utilisation pour détecter les comportements malveillants.

Remarque : Reveal(x) analyse beaucoup plus de protocoles de la couche Application que ceux énumérés ci-dessous. Ces exemples illustrent les types de fonctions de Machine Learning qui ne sont disponibles qu'après chiffrement et réassemblage complet.

Bases de données — couche Application (couche 7) : méthodes, erreurs, demandes, réponses, instructions SQL
Pourquoi c'est important : les méthodes et les messages d'erreur des bases de données sont essentiels à une détection fiable des attaques en force ciblant un serveur de base de données.

Kerberos — couche Application (couche 7) : nom d'utilisateur principal, nom de principal du service, types de messages de demande et de réponse, types d'erreurs
Pourquoi c'est important : les erreurs de tickets Kerberos en double sont un indice clé pour détecter avec précision le moment où un attaquant s'est emparé d'un ticket et le réutilise. Les demandes Kerberos d'un nom de principal du service (SPN) qui n'existe pas sont cruciales pour détecter les recherches de noms d'utilisateur.

DNS — couche Application (couche 7) : types d'enregistrements, codes de réponse, requêtes de l'hôte
Pourquoi c'est important : le DNS fait fréquemment l'objet d'utilisations abusives par les attaquants pour effectuer des opérations de reconnaissance (par exemple le balayage) et des communications C&C (par exemple la tunnellisation). Dans ces cas, il est utile d'avoir une visibilité sur les requêtes de l'hôte DNS et les types d'enregistrements DNS.

LDAP — couche Application (couche 7) : erreurs, demandes, réponses, messages en texte brut, messages SASL, noms uniques de la liaison, requête de recherche.
Pourquoi c'est important : les erreurs et les noms de comptes LDAP sont des éléments importants pour détecter les activités d'authentification malveillantes telles que les tentatives d'attaques en force.

SMB/CIFS — couche Application (couche 7) : erreurs, chemins d'accès, nom d'utilisateur, demandes, réponses, lectures, écritures, alertes
Pourquoi c'est important : l'activité d'écriture et les noms de fichiers CIFS sont des éléments pertinents dans la détection de ransomwares. Quant aux messages d'erreur de connexion, ils sont importants pour détecter les attaques en force.

SSH — couche Session (couche 5) : type d'enregistrement, version, algorithme de chiffrement, algorithme MAC, algorithme de compression, algorithme KEX, implémentation client, implémentation serveur
Pourquoi c'est important : les détails de l'algorithme SSH sont nécessaires pour détecter avec précision les activités de tunnellisation suspectes.

SSL/TLS — couche Session (couche 5) : versions, alertes, type de contenu, hachage JA3, détenteur du certificat, dates d'échéance du certificat, domaines (SNI), suites de code, tailles des enregistrements
Pourquoi c'est important : les détails de l'émetteur du certificat SSL/TLS sont pertinents pour détecter avec précision le trafic chiffré malveillant.

ANNEXE B

Exemples de détections dans Reveal(x)

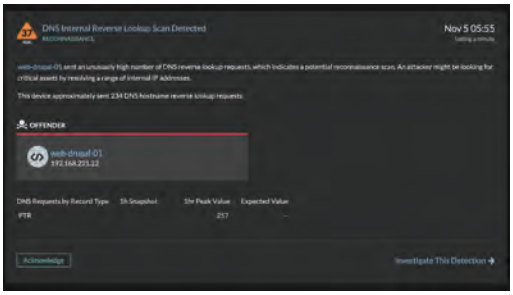
Les attaquants peuvent facilement modifier les outils qu'ils utilisent pour éviter la détection s'appuyant sur les signatures, mais il leur est presque impossible d'éviter d'adopter certains comportements réseau indispensables pour atteindre leurs cibles. Reveal(x) utilise un éventail de techniques, dont l'analyse comportementale optimisée par le Machine Learning, pour détecter les activités malveillantes dans chaque catégorie du framework MITRE ATT&CK. Les exemples ci-dessous illustrent l'étendue de la couverture offerte par Reveal(x).

Remarque : il s'agit ici d'exemples de catégories de détections ; la liste n'est pas exhaustive.

Reconnaissance

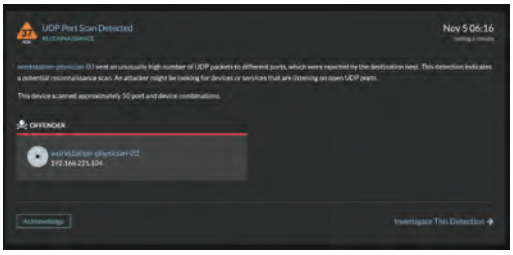
Avant même d'envoyer un e-mail de phishing ou de tenter un exploit Web, les attaquants chevronnés doivent recueillir des informations sur leur cible. Cependant, cette opération de reconnaissance ne cesse pas dès qu'ils ont accès à un système. Une fois entrés dans le réseau, les attaquants poursuivent leur mission de reconnaissance pour s'orienter et décider des étapes à suivre pour arriver à leurs fins. Ils effectuent souvent des analyses du réseau pour découvrir les équipements, les services, les serveurs de fichiers et les répertoires. Cette activité peut ressembler à s'y méprendre à une analyse légitime des vulnérabilités.

Reveal(x) détecte une grande variété d'activités d'analyse, mais les entreprises sont nombreuses à avoir recours en interne à des analyseurs de vulnérabilités. C'est la raison pour laquelle Reveal(x) applique une analyse heuristique pour les identifier, permettant ainsi aux analystes de déterminer plus facilement si l'analyse est légitime ou non. Ce type de détection peut être néanmoins désactivé.



Détection d'une analyse d'une résolution DNS inverse interne

Les serveurs DNS recèlent une mine de données utiles dans la phase de reconnaissance d'une attaque, notamment les noms d'hôtes et les adresses IP de ressources importantes. Les instances malveillantes activement implantées peuvent exploiter le DNS interne pour cartographier de grandes sections des réseaux cibles en effectuant des résolutions DNS inverses séquentielles (en convertissant les adresses IP internes en noms d'hôtes). Ces noms d'hôtes comprennent souvent des conventions de nommage utiles, tels que dc.acme.local, qui permettent aux attaquants de concentrer leurs attaques sur les cibles les plus intéressantes de l'entreprise.



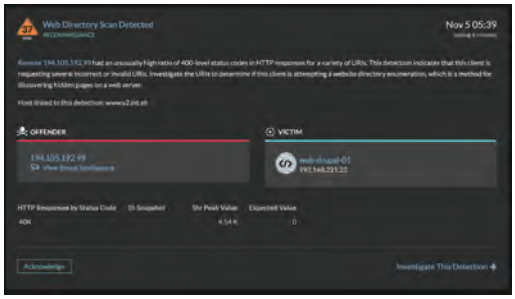
Analyse des ports UDP

Avec des outils d'attaque comme NMAP, les pirates peuvent analyser les plages CIDR à la recherche d'un large éventail d'hôtes et de ports de pare-feu ouverts. Ils ont ainsi à leur disposition des informations utiles pour créer des canaux C&C et des voies d'exfiltration de données. Ils disposent aussi d'indices sur les ports susceptibles d'offrir une surface d'attaque supplémentaire.

ANNEXE B

Exemples de détections dans Reveal(x)

Reconnaissance (suite)



Analyse de répertoire Web

L'analyse de répertoire Web est un mode de reconnaissance courant. Toutes les infrastructures d'hébergement Web présentent des failles, qu'il s'agisse de permissions mal configurées ou de l'absence de nettoyage des saisies de données dans les champs de formulaire. La situation est d'autant plus compliquée que les entreprises tardent à installer les correctifs sur ces serveurs en raison de leur nature critique. En analysant les répertoires Web, les attaquants peuvent déterminer le type d'infrastructure Web utilisée par l'entreprise tout en cherchant les failles et les erreurs de configuration de sécurité courantes.

D'autres problèmes se posent. Il est en effet probable que les entreprises ne collectent pas les données des journaux Web ou qu'elles ne les exploitent pas pour se protéger. Reveal(x) épaule les équipes de sécurité, non seulement en identifiant les attaques potentielles, mais aussi en fournissant des informations détaillées sur les URL analysées et les codes d'erreur associés aux réponses. Il peut identifier les faiblesses que les attaquants tentent d'exploiter et remédier rapidement à tout problème de sécurité.

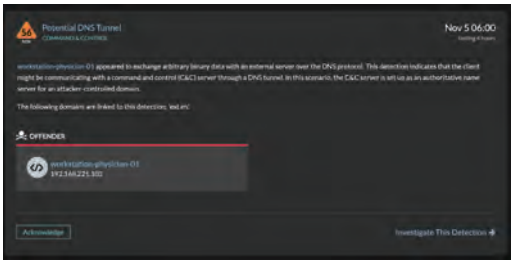
ANNEXE B

Exemples de détections dans Reveal(x)

Commande et contrôle (C&C)

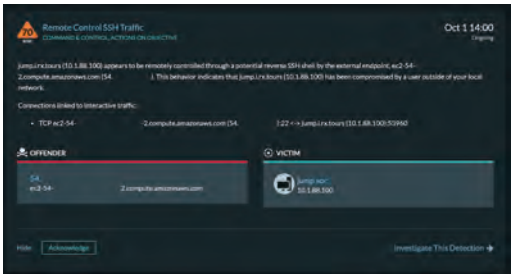
À moins que l'attaquant n'ait un accès physique aux équipements en réseau, il doit passer par ce réseau pour prendre la main à distance sur les systèmes. Cette activité C&C peut se dérouler à l'aide de protocoles de contrôle tels que RDP, SSH ou telnet, d'un protocole personnalisé, voire sous le couvert d'un autre protocole, tel que DNS.

En plus de faire correspondre le trafic avec les adresses IP et les domaines malveillants répertoriés dans les flux de cyberveille, Reveal(x) utilise des modèles de Machine Learning comportemental pour reconnaître les modèles de trafic associés aux activités C&C courantes.



Tunnel DNS potentiel

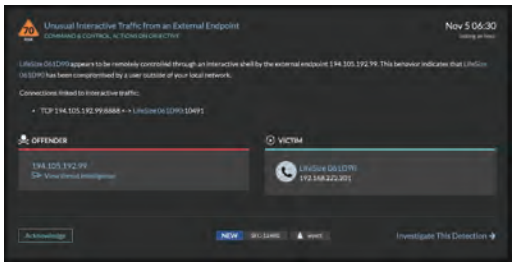
Un paquet DNS comporte différents champs que peuvent exploiter les attaquants, notamment dans le cadre du C&C. En configurant les malwares pour qu'ils répondent à certains bits, adresses IP, URI, etc., le DNS peut servir à commander de grands botnets ou des machines individuelles. Il est également exploité pour exfiltrer des données sans consommer beaucoup de bande passante.



Reverse SSH

La technique de communication Reverse SSH (SSH inversé) a recours à un large éventail d'outils malveillants. Reverse SSH peut être considéré comme un code ou un script qui rappelle un serveur distant en établissant une connexion SSH et en permettant à un utilisateur distant d'accéder à un équipement. Les hôtes sont souvent contaminés par des pièces jointes d'e-mails, des téléchargements malveillants ou des sites Web piratés.

Il arrive que des fournisseurs légitimes aient recours à ce type de communication à diverses fins, dont la validation de clés de licence. Cependant, la technique n'est généralement pas légitime. Habituellement, Reverse SSH est l'une des premières étapes employées pour s'infiltrer dans un environnement cible.



Trafic interactif inhabituel d'un endpoint externe

Les méthodes employées pour tunnelliser le trafic C&C sont légion. Souvent, elles ont recours à des protocoles existants dans un réseau pour sévir en toute impunité. Reveal(x) tire parti de sa capacité à intégrer du trafic en temps réel dans des environnements à haut débit pour surveiller les protocoles chiffrés et non chiffrés et y trouver des indices d'activités C&C. Cette surveillance ne se cantonne pas aux séquences de trafic détectables par l'analyse du trafic chiffré. Elle recherche également du texte brut et des chaînes codées qui sont révélateurs d'un environnement distant.

ANNEXE B

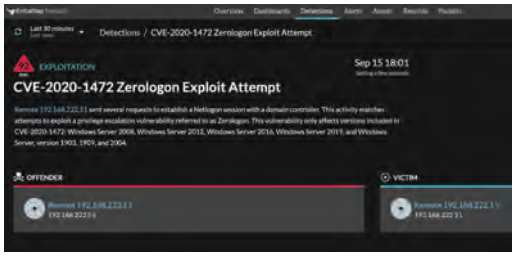
Exemples de détections dans Reveal(x)

Exploitation

Une fois qu'ils ont identifié leurs cibles au sein du réseau, les attaquants utilisent des outils comme Cobalt Strike, Metasploit et PowerShell Empire (pour n'en citer que quelques-uns) pour accéder aux systèmes exposés en exploitant les vulnérabilités. La détection à ce stade du cycle de vie de l'attaque est cruciale, car les attaquants n'ont pas encore accédé aux systèmes sensibles. La détection et la réponse aux attaques à ce stade permettent d'éviter les répercussions financières et l'atteinte à la notoriété.

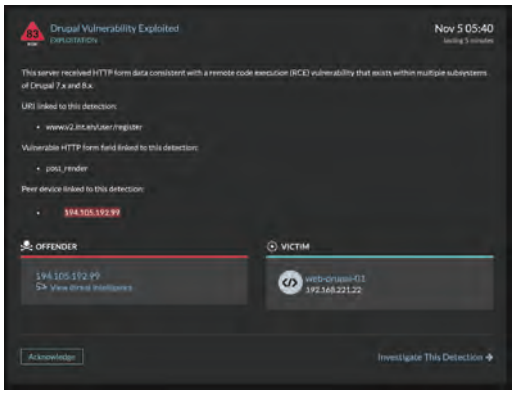
Attaque DCSync détectée

Une attaque DCSync facilite l'accès aux réseaux d'entreprise sans qu'il soit nécessaire d'exploiter un code supplémentaire ou de se connecter à un contrôleur de domaine. Les contrôleurs de domaine devant se répliquer, il suffit de profiter de l'occasion. Un attaquant disposant des bons privilèges peut usurper l'identité d'un contrôleur de domaine et déclencher la réplication de la base de données Active Directory. Il obtient ainsi l'accès à des comptes utilisateur dont il pourra se servir pour d'autres attaques post-exploitation. Reveal(x) détecte ce type d'attaque en recherchant un comportement inhabituel de DCSync et en alertant les équipes SecOps.



Zerologon

Les chercheurs ont démontré, dans le cadre d'un code PoC (preuve de concept) accessible au public, que des attaquants non authentifiés pouvaient exploiter cette vulnérabilité pour obtenir des privilèges d'administrateur complets sur les systèmes Active Directory. En falsifiant une session Netlogon authentifiée, les validations PoC publiques exploitent la fonctionnalité de modification de mot de passe pour réinitialiser le mot de passe de compte machine du contrôleur de domaine. Certaines méthodes réinitialisent le mot de passe à sa valeur initiale. S'il réinitialise le mot de passe à une valeur connue, le pirate pourra orchestrer une attaque (de type DCSync par exemple) pour répliquer les identifiants des tickets et des services, et s'offrir un accès illimité aux services et aux données de toute l'entreprise.



Exploitation d'une vulnérabilité de Drupal

Drupal, comme tous les systèmes de gestion de contenu, est vulnérable à une foule d'attaques. Des correctifs sont publiés en permanence pour remédier à ces vulnérabilités, mais leur déploiement par les administrateurs système est perfectible, vu les délais nécessaires à la gestion du changement. Ces failles, lorsqu'elles sont exploitées, peuvent doter les cybercriminels d'un arsenal de possibilités, jusqu'à l'exécution de code à distance. Reveal(x) analyse les demandes Web entrantes pour y déceler une exploitation potentielle de ces types de vulnérabilités.

ANNEXE B

Exemples de détections dans Reveal(x)

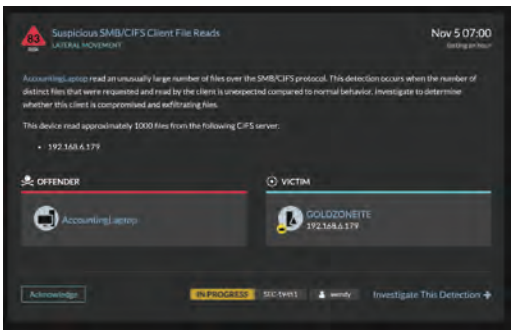
Déplacement latéral

Les attaquants sont opportunistes et s'insinuent dans le réseau par tous les moyens. Une fois à l'intérieur, ils doivent se déplacer latéralement pour obtenir un accès à distance à leurs systèmes cibles. Les détections de déplacement latéral visent les activités et les comportements dont les attaquants usent pour se propager d'un système à un autre, élever les privilèges et siphonner les données. Les menaces internes peuvent commencer à sévir à ce stade du cycle de vie de l'attaque, étant donné qu'elles connaissent déjà le système et les chemins d'accès, mais ne disposent pas des privilèges nécessaires pour modifier les données ou s'en emparer.

Grâce au Machine Learning, Reveal(x) peut détecter l'élévation de privilèges et les exploits orchestrés pour accéder à des systèmes distants au sein du réseau. Il peut repérer les mouvements de données inhabituels quand les attaquants les rassemblent avant leur exfiltration.

Activité de client WMI potentielle

Les cybercriminels recourent souvent à Windows Management Instrumentation (WMI) pour parvenir à leurs fins. Citons l'exécution de code authentifié sur des machines Windows distantes, le vol de données, la persistance, etc. En créant une référence du comportement des postes de travail et en surveillant le comportement WMI en particulier, Reveal(x) assure des détections efficaces des activités WMI suspectes. Reveal(x) fournit des données d'investigation numérique au niveau des paquets pour chaque instance trouvée et fait correspondre ces instances à des campagnes pour aider les équipes de sécurité à circonscrire un incident.



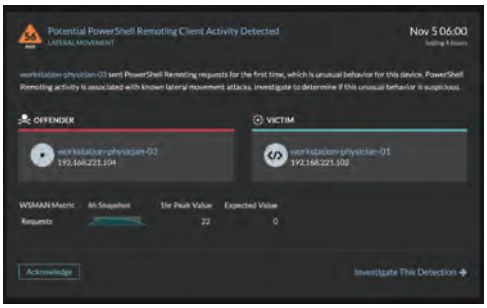
Lectures suspectes de fichiers SMB/CIFS

Les incidents de sécurité impliquent fréquemment le vol ou le chiffrement de données sensibles stockées sur des serveurs de fichiers distants. Les attaquants exploitent des fichiers existants pour se déplacer latéralement dans un réseau. Reveal(x) surveille les protocoles SMB/CIFS pour détecter des comportements inhabituels, souvent révélateurs de campagnes d'exfiltration et de cryptomalware. Les équipes SecOps disposent d'informations détaillées sur les fichiers altérés, consultés ou placés sur des disques de serveurs de fichiers. Elles peuvent ainsi rationaliser le processus d'investigation et de réponse en cas d'incident.

ANNEXE B

Exemples de détections dans Reveal(x)

Déplacement latéral (suite)



Détection d'accès distant PowerShell potentiel

PowerShell est l'un des outils les plus puissants dont disposent les administrateurs Windows et les attaquants. La console PowerShell peut s'activer facilement dans l'interface des systèmes d'exploitation Windows tout en fournissant un langage de script intuitif pour programmer l'automatisation des tâches. Les attaquants y ont souvent recours pour maintenir l'accès à des endpoints compromis (avec l'intention de les utiliser comme nœuds C&C), pour contrôler ces derniers à distance et pour une foule d'autres tâches.

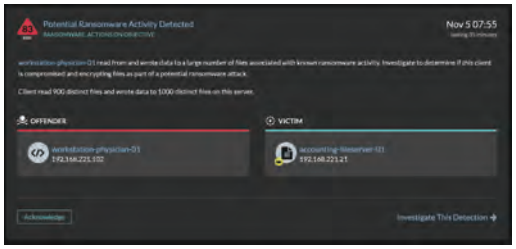
Reveal(x) surveille les endpoints Windows pour découvrir des activités réseau inhabituelles liées à PowerShell et analyse l'activité en question pour trouver des indices d'activités malveillantes. Reveal(x) est en mesure de fournir aux équipes SecOps des fonctionnalités de détection en cas d'accès à distance à un endpoint par le truchement de PowerShell.

ANNEXE B

Exemples de détections dans Reveal(x)

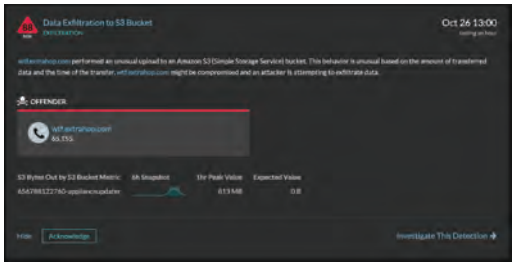
Actions répondant aux objectifs

Les cybercriminels poursuivent des objectifs très divers : sabotage, espionnage, fraude, vol de propriété intellectuelle, vol d'informations personnelles, chiffrement contre rançon, ou simplement l'appât du gain à la faveur de l'installation de logiciels malveillants comme le cryptominage ou de l'exécution de botnets. Reveal(x) dispose de plusieurs méthodes pour détecter les actions répondant aux objectifs à atteindre, y compris les ransomwares.



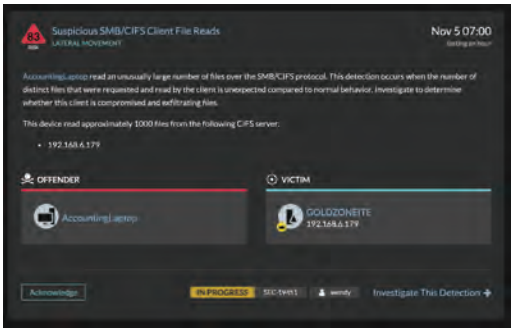
Activité potentielle d'un ransomware

Les ransomwares modernes agissent en chiffrant les fichiers d'un utilisateur, soit localement, soit sur des partages de fichiers distants, puis en envoyant la clé de déchiffrement à un serveur central. En procédant de cette manière, les pirates s'assurent que la probabilité de déchiffrement sans versement de rançon est extrêmement faible, voire nulle. Reveal(x) surveille l'activité sur le réseau en vue d'y déceler des signes que des ransomwares sont en train de chiffrer des fichiers sur des partages de fichiers distants ou à renvoyer des signaux à des serveurs C&C. Dans certains cas, il est même possible d'extraire les clés de chiffrement du trafic réseau stocké pour restaurer les fichiers.



Exfiltration inattendue de compartiments S3

Les cybercriminels ne sont pas motivés que par la perspective d'un gain rapide. Souvent, ils convoitent la propriété intellectuelle ou les informations confidentielles. Les pirates doivent trouver le moyen de sortir une copie des données visées du réseau de l'entreprise. Les compartiments AWS S3 (buckets) sont un emplacement propice à l'exfiltration des données, ces serveurs étant souvent affectés aux opérations internes légitimes. Pour faire face à cette attaque, Reveal(x) fait la distinction entre trafic S3 standard et anormal. Cette visibilité garantit la sécurisation des données de l'entreprise.



Regroupement potentiel de données SMB/CIFS

Lors des campagnes d'attaque, les pirates tentent souvent d'exfiltrer les données d'un réseau visé. Pour parvenir à leurs fins, ils doivent d'abord copier les données sur un endpoint compromis et les compresser avant téléchargement. Reveal(x) surveille l'accès au serveur de fichiers afin d'y repérer des séquences inhabituelles de déplacement ou de copie. La détection du regroupement potentiel de données est donc rapide. Les équipes SecOps disposent ainsi du temps nécessaire pour réagir avant la fuite des données.