UN APPRENTISSAGE FACILE

Une édition spéciale de Palo Alto Networks

XDR

pour les nuls

- Découvrez ce qu'est XDR, et ce qu'il n'est pas
- Brisez la chaîne d'attaque avec XDR
- Découvrez quelques cas d'usage XDR

Proposé par

CORTEX XDR BY PALO ALTO NETWORKS

Lawrence Miller

À propos de Palo Alto Networks

Palo Alto Networks, le leader mondial en cybersécurité, façonne l'avenir tourné sur le cloud à l'aide d'une technologie qui transforme la façon dont opèrent les utilisateurs et organisations. Notre mission est d'être le partenaire de choix en cybersécurité et de protéger notre mode de vie numérique. Nous contribuons à relever les plus gros défis de sécurité du monde à l'aide d'innovations continues qui saisissent les toutes dernières trouvailles en intelligence artificielle, analytique, automatisation et orchestration. En livrant une plateforme intégrée et en donnant les moyens voulus à un écosystème croissant de partenaires, nous sommes à la pointe de la protection de dizaines de milliers d'organisations à travers les clouds, réseaux et périphériques mobiles. Notre vision est celle d'un monde où chaque jour est plus sûr que le précédent. Pour de plus amples informations, consultez www.paloaltonetworks.com.

XDR

Une édition spéciale de Palo Alto Networks

par Lawrence Miller

pour les nuls®

XDR pour les Nuls®, une édition spéciale de Palo Alto Networks

Publié par
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-87903-9 (pbk); ISBN 978-1-119-87904-6 (ebk)

Remerciements de l'éditeur

Cet ouvrage a été réalisé avec la participation des personnes suivantes :

Rédacteur projet : Elizabeth Kuball

Rédacteur chargé des acquisitions : Ashley Coffey

Responsable éditorial : Rev Mengle

Représentant du développement commercial : Cynthia Tweed

Éditeur de production : Mohammed Zafar

Introduction

Année après année, le défi de la sécurisation des données stratégiques s'intensifie alors que l'adoption rapide de tendances comme le cloud computing, l'Internet des objets (IoT) et la transformation numérique augmente le risque pour les données sensibles des entreprises. Dans le même temps, les pirates tirent parti de bon nombre de ces mêmes tendances technologiques pour accroître la puissance et l'ampleur d'attaques toujours plus sophistiquées.

Les équipes de sécurité ont déployé des outils, mis en œuvre des processus et embauché du personnel pour répondre aux nouvelles menaces au fur et à mesure de leur apparition, mais elles sont dépassées en nombre et en efficacité. Mais le fait d'ajouter continuellement de nouvelles fonctionnalités aux systèmes existants crée rapidement un fouillis d'outils mal intégrés dont l'utilisation demande beaucoup de temps, d'énergie et de compétences, toutes choses qui sont très limitées. Les processus statiques qui ne s'adaptent pas à l'évolution rapide des tendances et des environnements, comme le cloud et le télétravail, deviennent rapidement obsolètes et inefficaces. Quant aux analystes de sécurité, ils sont chargés de la tâche quasi impossible de trier un déluge incessant d'alertes, mais ils reçoivent souvent une formation limitée et des outils tout aussi limités. La combinaison d'un trop grand nombre d'alertes et d'un contexte insuffisant entraîne la perte de visibilité et de contrôle des équipes de sécurité. En fin de compte, l'entreprise est encore plus à la merci des attaques.

La détection et la réponse étendues (XDR) sont apparues comme une réponse à cette complexité. XDR est une catégorie de solutions de détection, d'investigation et de réponse aux menaces qui fonctionnent ensemble sur tous les vecteurs de menaces dans l'infrastructure d'une entreprise, y compris le réseau, les terminaux, le cloud et les identités, plutôt que sur un seul aspect de l'infrastructure. Étant directement intégrés dans l'architecture, les outils XDR sont conçus pour fournir des informations sur les menaces et des recommandations qui optimisent le fonctionnement des équipes de sécurité.

À propos de ce livre

XDR pour les Nuls vous aide à vous familiariser avec la catégorie XDR de solutions de sécurité et ce qu'elle signifie pour votre entreprise. Ce livre est composé de cinq petits chapitres qui explorent les questions suivantes :

- L'état actuel de la détection et de la réponse, y compris les menaces, les limites et les défis (chapitre 1).
- Ce qu'est XDR et ce qu'il n'est pas (chapitre 2)
- Comment XDR brise le cycle de vie des attaques pour les arrêter (chapitre 3)
- Différents cas d'utilisation XDR (chapitre 4)
- Capacités et fonctionnalités XDR indispensables (chapitre 5)

Chaque chapitre est rédigé comme un tout indépendant du reste de l'ouvrage. Si un sujet vous intéresse, vous pouvez donc passer directement au chapitre qui s'y rapporte. Lisez ce livre dans le sens qui vous convient (je vous déconseille toutefois de le lire à l'envers ou de droite à gauche).

Quelques suppositions idiotes

On dit que la plupart des hypothèses ont perdu leur utilité, mais je vais tout de même en faire quelques-unes :

Je suppose principalement que vous travaillez pour une organisation qui cherche un meilleur moyen d'améliorer l'efficacité de sa stratégie de sécurité, en particulier ses capacités de détection et de réponse. Vous êtes peut-être un responsable informatique, par exemple un responsable de la sécurité des systèmes d'information (CISO), un directeur des systèmes d'information (CIO) ou un directeur de la technologie (CTO), ou encore un vice-président ou un directeur de la sécurité. Ou peut-être êtes-vous architecte ou ingénieur réseau ou sécurité. Ce livre est donc destiné principalement aux techniciens qui ont une connaissance générale des concepts et technologies modernes des opérations de sécurité.

Si vous vous reconnaissez dans l'une de ces hypothèses, alors ce livre s'adresse à vous. Si aucune de ces hypothèses ne vous correspond, poursuivez tout de même votre lecture. XDR est une technologie incontournable, et votre équipe vous remerciera d'être devenu un expert en la matière.

Icônes utilisées dans ce livre

Tout au long de ce livre, j'utilise des icônes spéciales pour attirer l'attention du lecteur sur certaines informations importantes. Voici ce qu'elles signifient :

RAPPEL

Cette icône signale des informations importantes à inscrire obligatoirement dans votre mémoire non volatile, votre matière grise ou votre crâne, à côté des dates d'anniversaire !

JARGON TECHNIQUE

Si vous cherchez à atteindre le septième niveau du nirvana pour les nerds, vous allez être servi ! Cette icône explique le jargon technique qui se cache derrière le jargon ; il s'agit de l'étoffe dont les nerds sont faits !

CONSEIL

Les conseils sont appréciés, jamais attendus. J'espère que vous apprécierez ces informations utiles.

ATTENTION

Ces alertes soulignent les choses contre lesquelles votre mère vous a mis en garde. En fait, probablement pas, mais elles offrent des conseils pratiques pour vous permettre d'éviter des erreurs potentiellement coûteuses ou frustrantes.

Au-delà de ce livre

Ce sujet est tellement vaste qu'il est impossible de tout aborder dans cet ouvrage. Donc, si à la fin du livre vous pensez : « Mince alors, ce livre était génial ! Où puis-je en savoir plus ? », rendez-vous sur `www.paloaltonetworks.com/cortex/cortex-xdr`.

DANS CE CHAPITRE

- Constater l'urgence d'une meilleure approche en matière de sécurité
- Comprendre les limites des outils de détection et de réponse traditionnels
- Lutter contre la lassitude face aux alertes et le manque de compétences en matière de sécurité

Chapitre 1
État des lieux de la détection et de la réponse aux menaces

Dans ce chapitre, j'explique comment les menaces modernes ont évolué pour devenir potentiellement plus destructrices ; pourquoi les approches traditionnelles de prévention, de détection et de réponse ne sont pas suffisantes ; et comment la lassitude face aux alertes et la pénurie de compétences en cybersécurité augmentent les risques pour votre organisation.

Analyse du paysage moderne des menaces

Ces derniers temps, les atteintes à la protection des données et les attaques par ransomware sont devenues si fréquentes qu'elles méritent pratiquement leur propre colonne dans les journaux, aux côtés de la météo, des sports et du trafic routier. Le fait que ces événements de sécurité soient courants ne les rend pas moins dangereux pour autant. Chaque minute pendant laquelle un cybercriminel opère dans votre environnement entraîne des dommages considérables.


ATTENTION

Selon le Ponemon Institute, entre 2020 et 2021, le coût moyen d'une atteinte à la protection des données a augmenté de 10 % pour atteindre 4,24 millions de dollars. Il s'agit de la plus forte augmentation annuelle des coûts au cours des sept dernières années.

Bien sûr, vous connaissez et vivez déjà cette réalité, et vous vous efforcez de détecter les menaces et de réagir aussi rapidement et efficacement que possible, bien avant que la perte de données ne puisse se produire. Toutefois, il s'agit d'une bataille difficile face aux tactiques, techniques et procédures (TTP) de plus en plus sophistiquées utilisées par les cybercriminels. Les pirates peuvent désormais compromettre un environnement presque à volonté, sans utiliser les méthodes traditionnelles comme les logiciels malveillants basés sur des fichiers. Au lieu de cela, ils ont recours à des méthodes qui compromettent les fichiers système autorisés, lancent des attaques dans le registre d'un appareil ou utilisent de manière malveillante des utilitaires comme PowerShell. La multiplication de méthodes d'attaque nouvelles et plus évasives a rendu nécessaire l'élaboration de nouvelles stratégies et tactiques de détection et de réaction, en plus de la prévention des menaces.

RAPPEL

La capacité d'une organisation à rester à la pointe du paysage des menaces modernes nécessite des outils efficaces et une équipe d'analystes de sécurité compétente. Malheureusement, le fait de disposer d'un bon équilibre entre la technologie et les experts qualifiés tend à être l'exception pour la plupart des organisations, plutôt que la règle.

Reconnaître les limites des technologies et des approches traditionnelles

Alors que vos équipes de sécurité s'efforcent de prévenir les attaques contre votre organisation, vous devez vous préparer à l'inévitable réalité : aucun environnement n'est totalement sécurisé. Une menace finira par s'introduire dans votre environnement.

Un éventail vertigineux d'outils de gestion de logs, de détection et de réponse a été mis sur le marché pour aider les équipes de sécurité à détecter les menaces. Chacun de ces outils a ses avantages et inconvénients et peut être utile contre des attaques, comme les incidents à partir de logiciels malveillants connus basés sur des fichiers ou les attaques conçues pour pénétrer dans une seule partie de l'infrastructure. Cependant, la plupart de ces outils sont conçus pour un seul objectif et aucun d'entre eux n'est particulièrement bien adapté à la gestion de menaces sophistiquées.

ATTENTION

Selon ESG Research, 66 % des organisations estiment que l'efficacité de leur détection et de leur réponse aux menaces est limitée parce qu'elle repose sur de multiples outils ponctuels indépendants.

Dans les sections suivantes, j'examine de plus près certains des outils de gestion de logs, de détection et de réponse les plus courants utilisés par les équipes de sécurité, et je vous éclaire sur leurs défis et leurs limites.

Détection et réponse sur les terminaux

Les outils de *détection et de réponse sur les terminaux* (Endpoint Detection and Response, EDR) sont une catégorie d'outils utilisés pour détecter et examiner les menaces sur les terminaux. Les outils EDR fournissent généralement des capacités de détection, d'analyse, d'investigation et de réponse.

L'EDR a fait son apparition en 2013 pour faciliter les analyses criminalistiques nécessitant une télémétrie très détaillée des terminaux afin d'effectuer une rétro-ingénierie des logiciels malveillants et de comprendre exactement ce qu'un cybercriminel a fait sur un appareil compromis.

Les outils EDR surveillent les événements générés par les agents afin de détecter toute activité suspecte. Les alertes créées par les outils EDR aident les analystes des opérations de sécurité à identifier les incidents, à les analyser et à y remédier. Les outils EDR collectent également des données de télémétrie sur les activités suspectes et peuvent enrichir ces données avec d'autres informations contextuelles provenant d'événements corrélés. Grâce à ces fonctions, l'EDR contribue à raccourcir les délais d'intervention des équipes de réponse aux incidents.

Cependant, le système EDR ne peut à lui seul assurer la détection des menaces pour l'entreprise, car il se concentre uniquement sur le terminal. Il n'offre pas de visibilité sur le trafic réseau des appareils sans l'installation d'agents sur le réseau et les appareils en réseau — comme les routeurs, les commutateurs, les serveurs, les appareils de l'Internet des objets (IoT), les appareils AVEC (Apportez votre équipement personnel de communication) et les systèmes de contrôle industriel (ICS) — ainsi que sur les ressources cloud comme les charges de travail, les réseaux cloud et les offres de plateforme en tant que service (PaaS).

Plateforme de protection des terminaux

Une *plateforme de protection des terminaux* (Endpoint Protection Platform, EPP) est un agent logiciel installé sur les terminaux pour empêcher les attaques de logiciels malveillants basés sur des fichiers et détecter les activités nuisibles. L'EPP est l'évolution des solutions traditionnelles d'antivirus et d'anti-programmes malveillants basées sur l'hôte et est généralement considérée comme la première ligne de défense d'un terminal.

Les capacités de détection varient selon les solutions EPP, mais la plupart utilisent une combinaison de techniques de détection et de prévention, notamment :

- Les indicateurs statiques de compromission (IOC), c'est-à-dire la détection basée sur les signatures.
- *Une liste blanche* (autorisation) ou *liste noire* (blocage) des applications, URL (Uniform Resource Locator), ports et adresses.
- L'Analyse comportementale et le Machine Learning
- Le Sandboxing pour faire détoner (ou tester) les menaces présumées, comme les fichiers exécutables.

Une solution EPP doit être gérée dans le cloud pour permettre la surveillance continue et la collecte de données d'activité, ainsi que la possibilité de prendre des mesures correctives à distance, que le terminal soit utilisé sur le réseau de l'entreprise ou à distance. En outre, les solutions EPP sont assistées par des données cloud. En d'autres termes, l'agent sur le terminal n'a pas à maintenir une base de données locale de tous les IOC connus ; au lieu de cela, il peut consulter une ressource cloud pour trouver les derniers verdicts sur les objets qu'il n'est pas en mesure de classer et tirer parti des renseignements sur les menaces en temps réel.

Une solution EPP est conçue uniquement pour prévenir ou contrôler et, par conséquent, n'est pas axée sur la détection ou la collecte d'informations pour se défendre contre les attaques modernes. La plupart des plateformes EPP ne disposent pas non plus des capacités de réaction nécessaires pour enquêter sur les incidents. Par conséquent, une solution de type EPP ne fournit pas à elle-seule les caractéristiques essentielles pour arrêter les attaques modernes.

Gestion des informations et des événements liés à la sécurité

Les outils logiciels de *gestion des informations et des événements de sécurité* (SIEM) assurent la collecte, la corrélation et l'analyse en temps quasi réel des événements de sécurité, ainsi que la notification des alertes de sécurité générées par divers périphériques et applications réseau.

De nombreuses organisations allouent une grande partie de leur budget de sécurité aux outils SIEM afin de rassembler les logs provenant de dispositifs de sécurité et d'environnements de serveurs disparates. À l'origine, les SIEM étaient principalement conçus comme des collecteurs de logs afin de créer des rapports de conformité. Au fil du temps, leur utilisation s'est étendue à la détection des menaces et les SIEM sont désormais le référentiel d'alertes central de nombreux centres d'opérations de sécurité (SOC).

Un SIEM centralise les alertes et regroupe les données des logs afin de les analyser et de les normaliser. Les équipes de sécurité peuvent voir les

données des logs en un seul endroit, mais comme elles ne sont généralement pas assemblées de manière significative, les analystes de première ligne chargés de leur donner un sens ne peuvent souvent pas utiliser les outils qui contiennent les données sources plus riches pour valider les alertes. Dans l'ensemble, les SIEM manquent de profondeur d'analyse pour les sources de données clés, comme les données des terminaux et du réseau, et ils peuvent être difficiles à déployer, à configurer et à maintenir, en partie parce qu'ils sont dépourvus de ces connaissances prêtes à l'emploi.

Détection et réponse réseau et analyse du comportement des utilisateurs et des entités

Les outils de *détection et de réponse réseau* (Network Detection and Response, NDR) et les outils *d'analyse du comportement des utilisateurs et des entités* (User and Entity Behaviour Analytics, UEBA) représentent une nouvelle catégorie d'outils d'analyse de la sécurité qui ont vu le jour pour relever les défis que pose le SIEM en matière de détection des attaques inconnues. Ces outils utilisent le Machine Learning pour développer une ligne de base de l'activité à partir de la télémétrie recueillie, puis recherchent des actions atypiques qui peuvent indiquer un comportement malveillant. Ces technologies permettent aux organisations d'identifier des attaques jusqu'alors inconnues en reconnaissant des modèles de trafic inhabituels.

Cependant, ces outils ont aussi leurs limites. Les produits basés sur le réseau sont limités au réseau et ne peuvent pas surveiller ou suivre les événements locaux, comme les informations sur les processus recueillies sur les terminaux. Le NDR a également une profondeur très limitée ; si l'EDR est profond et étroit, le NDR reste large et peu profond.

RAPPEL

La complexité des attaques modernes exige l'analyse de multiples sources de données pour identifier et confirmer les activités malveillantes. La superposition d'outils unidimensionnels entraîne des dépenses importantes pour les équipes de sécurité, crée des angles morts potentiels et exige un effort manuel considérable de la part des analystes de sécurité pour passer d'une console à l'autre et donner un sens à une attaque.

Trop d'alertes, trop peu de temps et de personnel

Les outils de détection et de prévention génèrent des milliers d'alertes chaque jour, ce qui dépasse largement le volume que les équipes de sécurité sont en mesure de traiter efficacement. Ces alertes proviennent de nombreuses sources déconnectées, laissant aux analystes de sécurité le soin de reconstituer le puzzle (voir la figure 1-1).

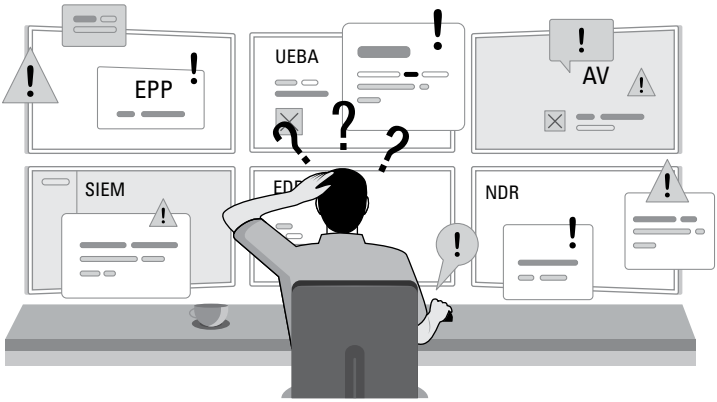

FIGURE 1-1 : Les outils cloisonnés ralentissent les investigations et les réponses.

L'analyse d'une menace nécessite généralement un certain nombre d'étapes :

1. Examiner les données de log disponibles pour commencer à reconstituer ce qui a pu se produire.
2. Comparer manuellement les données aux sources de renseignements sur les menaces pour déterminer si les indicateurs sont connus pour être malveillants
3. Rechercher des événements connexes à l'aide des IOC pour déterminer si l'alerte fait partie d'une attaque plus vaste.
4. Rassembler le contexte autour de l'incident, y compris les systèmes, les hôtes, les actifs, les ressources, les adresses IP et les fichiers associés à chaque alerte.
5. Établir une chronologie et identifier la cause profonde d'une alerte.
6. Vérifier si les liens entre les nouvelles informations et les alertes sont traités par d'autres membres de l'équipe afin de coordonner les efforts.
7. Évaluer si l'alerte doit être transmise à un échelon supérieur, rejetée ou rapidement corrigée et classée

Toutes ces étapes prennent beaucoup de temps et nécessitent de multiples outils dans un SOC traditionnel, et il ne s'agit là que du triage. Le résultat net est que les analystes n'ont le temps de traiter que les alertes « hautement prioritaires » qu'ils rencontrent chaque jour ; pendant ce temps, un nombre déconcertant d'alertes « moins prioritaires » ne sont pas traitées du tout. Et sans le contexte adéquat pour classer une alerte comme « élevée » ou « faible », le SOC peut en fait passer à côté de ce qui est vraiment important et/ou poursuivre des problèmes qui ne sont pas vraiment essentiels.

QUE FAIT UNE ÉQUIPE AU SEIN D'UN SOC ?

Les équipes chargées des opérations de sécurité, grandes et petites, partagent certaines fonctions clés. Un modèle traditionnel pour de nombreuses équipes SecOps et les SOC divise ces fonctions en une structure d'analystes à plusieurs niveaux, en fonction du niveau d'expérience. Voici les principales responsabilités de ces niveaux :

- **Niveau 1 — Triage :** c'est à ce niveau que la majorité des analystes de sécurité passent généralement leur temps. Les analystes de niveau 1 sont généralement les analystes les moins expérimentés, et leur fonction principale est de surveiller les logs d'événements pour détecter toute activité suspecte. Lorsqu'ils estiment que quelque chose doit faire l'objet d'une investigation plus approfondie, ils rassemblent le plus de contexte possible à partir d'une multitude de sources dans un rapport sous la forme d'un incident qui spécifie l'utilisateur, l'hôte, l'adresse IP et tous les IOC connexes, et font remonter l'incident au niveau 2.
- **Niveau 2 — Investigation :** les analystes de niveau 2 approfondissent l'activité suspecte pour déterminer la nature de la menace et l'ampleur de son infiltration dans l'environnement, ce qui inclut l'établissement d'une chronologie pour comprendre l'enchaînement et la corrélation des événements afin de déterminer la cause profonde. Ils doivent mener une investigation plus approfondie pour comprendre jusqu'où l'attaque est allée. Ces analystes coordonnent ensuite une intervention pour remédier au problème. Il s'agit d'une activité à fort impact qui nécessite souvent une plus grande expérience de l'analyste.
- **Niveau 3 et supérieurs — Chasse aux menaces :** ce niveau est occupé par les analystes les plus expérimentés, qui prennent en charge la réponse aux incidents complexes et passent le temps restant à rechercher dans les données d'investigation et de télémétrie les menaces qui n'ont pas été identifiées comme suspectes par les logiciels de détection. L'entreprise moyenne consacre peu de temps aux activités de chasse aux menaces, car les activités des niveaux 1 et 2 consomment énormément de ressources d'analyse.

Bien que ce modèle soit le plus courant, il n'est pas nécessairement idéal. La plupart des personnes ne sont pas faites pour surveiller des logs toute la journée. La lassitude face aux alertes est réelle, et les menaces se glissent parmi tout le bruit généré par la myriade de capteurs d'un SOC. Il peut être difficile de retenir les analystes pour cette tâche : ils préfèrent de loin contribuer de manière significative aux investigations (et peuvent avoir des approches nouvelles et innovantes qui ne sont jamais révélées, car ils n'ont pas les compétences techniques requises pour les processus d'investigation traditionnels). Les entreprises consacrent bien trop peu de temps à la chasse aux menaces et à l'amélioration des processus, car la majorité des heures des ressources sont consacrées à la découverte et à l'atténuation des menaces.

En outre, les analystes de sécurité chargés du triage des alertes ne disposent souvent pas d'un contexte suffisant pour déterminer le risque réel que représente une attaque pour l'organisation. L'alerte est donc transmise à un groupe de niveau supérieur pour une validation plus poussée, ce qui exige encore plus de temps, de travail et de ressources, créant ainsi des inefficacités à tous les niveaux.

RAPPEL

La plupart des entreprises reçoivent des milliers d'alertes provenant d'une multitude de solutions de surveillance, mais la recrudescence de bruit est contre-productive. La détection avancée ne consiste pas à *multiplier* les alertes, mais à les *améliorer* et à les rendre plus exploitables. Pour parvenir à ce type de détection avancée, il faut intégrer toutes les technologies de détection utilisées, ainsi que des analyses sophistiquées qui examinent les données des terminaux, du réseau et du cloud pour trouver et valider l'activité des pirates dans votre environnement.

Même avec des outils de détection des menaces plus performants et plus complets, le traitement des alertes — et des incidents éventuels — nécessite une validation et un triage supplémentaires par des intervenants qualifiés. Malheureusement, ces praticiens de la sécurité ne sont pas assez nombreux, et cet important déficit de compétences a un impact sur la capacité des organisations à garder le rythme face aux pirates (voir la figure 1-2).

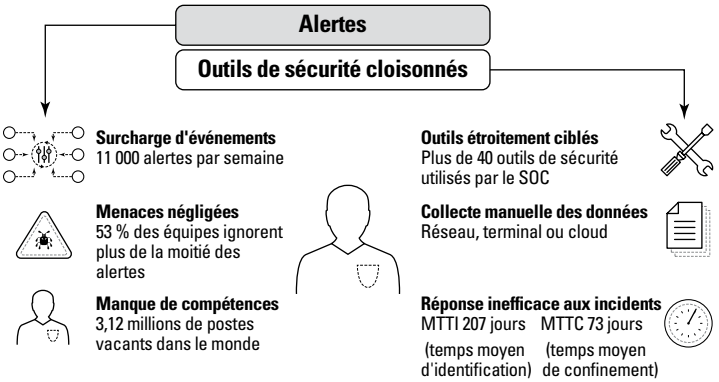

FIGURE 1-2 : Les nombreux défis d'un analyste de sécurité.

Les cybercriminels utilisent des outils et des techniques hautement automatisés pour trouver des vulnérabilités et obtenir un accès initial à votre environnement. Cette situation ne fait qu'exacerber le manque de compétences, car les pirates sont en mesure de développer leurs outils

automatisés plus rapidement et à moindre coût que les organisations ne peuvent ajouter du personnel de sécurité qualifié. Vous devez donc rechercher des outils qui peuvent :

- Rendre votre personnel moins expérimenté plus efficace et efficient
- Automatiser la détection de menaces complexes
- Simplifier les investigations
- Aider les analystes à améliorer leurs compétences

CONSEIL

Dans son *étude de 2020 sur la main-d>œuvre en cybersécurité*, l'International Information Systems Security Certification Consortium (ISC)[2] fait état d'une pénurie de 3,12 millions de professionnels de la cybersécurité qualifiés dans le monde. Selon Cyberseek, il existe aujourd'hui plus de 300 000 offres d'emploi dans le domaine de la cybersécurité aux États-Unis, un chiffre qui devrait augmenter considérablement dans les années à venir.

De nombreuses entreprises choisissent d'externaliser leurs fonctions de détection et de réponse, en totalité ou en partie, auprès de prestataires de services de sécurité gérés (Managed Security Services Provider, MSSP) ou de fournisseurs de services de détection et de réponse gérés (MDR). L'externalisation de cette fonction est courante (et considérée comme une bonne pratique dans de nombreux cas), en particulier pour les équipes disposant de budgets de sécurité plus modestes et les organisations qui ne souhaitent pas gérer leur propre sécurité ou ne disposent pas des ressources nécessaires pour y parvenir. Cependant, les organisations qui souhaitent une visibilité et un contrôle complets ne devraient pas être contraintes d'externaliser leur sécurité simplement parce que leurs outils sont inadéquats. Il convient également de noter que la pile technologique est tout aussi importante pour une équipe de sécurité externalisée ; les prestataires qui utilisent des outils anciens seront confrontés aux mêmes inefficacités que les équipes de sécurité internes.

Ce qu'il faut vraiment, c'est un ensemble de technologies permettant de réduire le nombre total d'alertes tout en permettant aux analystes moins expérimentés d'évaluer eux-mêmes les menaces avec efficacité et confiance, en veillant à ce que seules les alertes à haute fiabilité soient transmises aux analystes plus expérimentés.

DANS CE CHAPITRE

- **Commencer par une prévention des menaces à toute épreuve pour réduire le bruit**
- **Assurer une visibilité de bout en bout de votre environnement**
- **Réduire les enquêtes manuelles pour accélérer et améliorer la réponse aux incidents**
- **Maximiser la valeur de vos investissements en matière de sécurité**

Chapitre 2
Définition du XDR

La détection et la réponse étendues (XDR) constituent une nouvelle approche de la détection et de la réponse aux menaces. Le terme *XDR* a été inventé en 2018 par Nir Zuk, directeur de la technologie (CTO) et cofondateur de Palo Alto Networks. La raison fondamentale de la création de XDR était de stopper les attaques plus efficacement, de détecter les techniques et tactiques des pirates qui ne peuvent être empêchées, et d>aider les équipes du centre des opérations de sécurité (SOC) à mieux répondre aux menaces qui nécessitent une enquête.

Selon Forrester Research, XDR « optimise la détection, l'investigation, la réponse et la traque des menaces en temps réel. XDR associe les détections pertinentes sur les terminaux pour la sécurité avec la télémétrie des outils de sécurité et d'entreprise comme l'analyse et la visibilité du réseau (NAV), la sécurité de la messagerie électronique, la gestion des accès et identités, la sécurité dans le cloud, etc. ».

Le *X* de XDR signifie *étendu*, mais il représente en réalité toute source de données, car examiner les composants individuels d'un environnement de manière isolée n'est pas très efficace. XDR adopte une approche proactive de la détection et de la réponse aux menaces, en offrant une visibilité sur les réseaux, les clouds et les terminaux, tout en appliquant l'analyse et l'automatisation pour faire face aux menaces actuelles de plus en plus sophistiquées.

Dans ce chapitre, vous apprendrez ce qu'est XDR et les principales exigences d'une solution XDR.

Assurer une prévention robuste des menaces

Le fondement de XDR est une prévention des menaces à toute épreuve. Une solution XDR doit bloquer avec précision plus de 99 % des menaces qui peuvent être bloquées automatiquement en temps réel ou quasi réel, sans aucune vérification manuelle. Grâce à une prévention hors pair des menaces, votre équipe peut se concentrer sur l'identification et le blocage d'attaques plus sophistiquées et furtives au lieu de perdre du temps à enquêter sur chaque menace qui passe à travers vos défenses.

Pour vaincre les menaces qui pèsent sur les terminaux, vous avez besoin d'une solution robuste dotée d'un antivirus de nouvelle génération (NGAV) intégré, capable de détecter et de bloquer chaque étape d'une attaque, depuis l'exploitation initiale et l'installation du logiciel malveillant jusqu'aux actions illicites exécutées par un pirate exécutant ce logiciel. Chaque couche de défense doit être suffisamment intelligente pour déjouer les techniques d'évasion d'un pirate et s'adapter en permanence pour arrêter les menaces les plus récentes.

CONSEIL

Recherchez les capacités suivantes d'un NGAV dans une solution XDR :

- Analyse locale et prévention des menaces basées sur le Machine Learning
- Prévention des menaces basée sur le comportement pour l'analyse dynamique des processus en cours d'exécution
- Prévention des attaques à l'aide d'un code malveillant exploitant une faille de sécurité
- Prévention des menaces connues en fonction des renseignements sur les menaces, comme les hachages de fichiers
- Intégration automatisée à l'aide d'un service de prévention des logiciels malveillants basé sur le cloud, avec rapports d'analyse et prise en charge de fichiers d'une taille minimale de 100 Mo.
- Signatures immédiates pour assurer une protection rapide et partager les renseignements sur les menaces
- Capacité de protection de Shell inversé
- Mises à jour transparentes du moteur de détection des menaces
- Profils de sécurité et exceptions
- Analyse ad hoc et programmée des terminaux
- Protection contre les logiciels malveillants, les ransomwares et les attaques sans fichier

- Agent unique et léger pour la protection, la détection et la réponse au niveau des terminaux

Votre solution XDR doit également réduire votre surface d'attaque et protéger les données sensibles grâce à des fonctions de protection des terminaux, y compris les suivantes :

- Pare-feu hôte
- Chiffrement du disque
- Contrôle des périphériques USB (Universal Serial Bus)
- Règles de prévention personnalisables

Enfin, votre solution XDR doit être compatible avec un client de sécurité réseau pour les terminaux afin de fournir un accès distant sécurisé, une prévention des menaces et un filtrage des URL (Uniform Resource Locator).

Assurer une visibilité et une détection complètes

La visibilité et la détection sont essentielles à l'atténuation des menaces. Si vous ne pouvez pas *voir* une menace, vous ne pouvez pas l'identifier ou l'examiner et vous ne pouvez certainement pas l'arrêter. Les cybercriminels s'appuient sur le cloud et le Machine Learning pour mener des attaques massives et multiformes qui leur permettent d'établir une persistance et d'exfiltrer des données précieuses et de la propriété intellectuelle. Cela signifie que la solution XDR doit disposer de solides capacités de visibilité et de détection, notamment les suivantes :

- **Large visibilité et compréhension du contexte :** les produits ponctuels cloisonnés conduisent à des données cloisonnées, ce qui n'est pas efficace. Vous ne pouvez pas espérer vous défendre efficacement contre les attaques si vous n'êtes pas au moins aussi agile dans votre propre environnement que les pirates. La solution XDR doit avoir des capacités de visibilité et de détection sur l'ensemble de votre environnement, en intégrant la télémétrie de vos terminaux, réseaux et environnements cloud. En outre, elle doit être capable de mettre en corrélation ces sources de données pour comprendre comment divers événements sont liés et quand un certain comportement est (ou n'est pas) suspect en fonction du contexte (voir la figure 2-1).

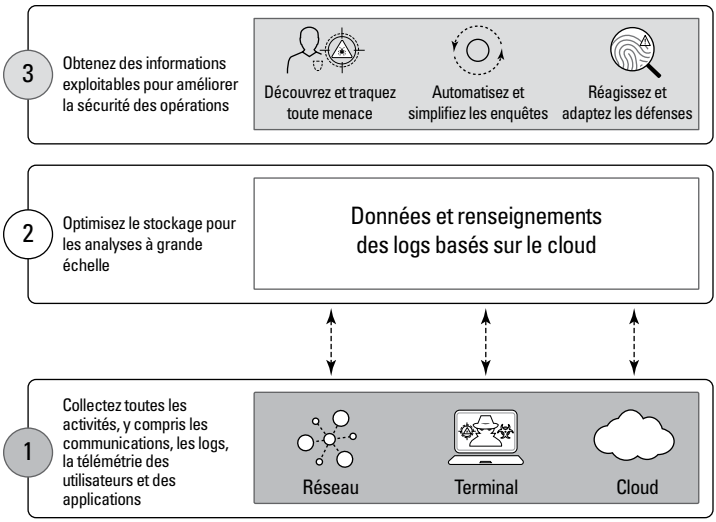

FIGURE 2-1 : XDR brise les cloisonnements traditionnels de la détection et de la réponse.

- **Conservation des données :** Les cybercriminels sont patients et persistants. Ils savent qu'ils sont plus difficiles à détecter s'ils avancent lentement, en laissant s'écouler les périodes de conservation des logs des technologies de détection auxquelles ils sont confrontés. La solution XDR ne doit pas leur faciliter la tâche. Vos systèmes de détection doivent collecter, corréler et analyser les données provenant du réseau, des terminaux et du cloud au sein d'un référentiel unique, offrant une rétention historique de 30 jours ou plus.
- **Analyse du trafic interne et externe :** les techniques de détection traditionnelles se concentrent principalement sur les pirates externes, ce qui donne une vision incomplète des potentiels cybercriminels. La détection ne peut pas se contenter de rechercher les attaques provenant de l'extérieur du périmètre. Elle doit également établir le profil des menaces internes et les analyser afin de rechercher les comportements anormaux et potentiellement malveillants et d'identifier l'utilisation abusive des informations d'identification.
- **Renseignements intégrés sur les menaces :** vous devez être équipé pour faire face à des attaques inconnues. Une méthode pour équilibrer la balance consiste à tirer parti des attaques connues que d'autres organisations voient en premier. La détection doit s'appuyer sur les renseignements sur les menaces recueillis dans un réseau mondial d'entreprises. Lorsqu'une organisation du

réseau étendu identifie une attaque, vous pouvez utiliser les connaissances acquises lors de cette attaque initiale pour identifier les attaques ultérieures dans votre propre environnement.

- **Détection personnalisable :** la protection de votre organisation présente des défis uniques associés à des systèmes spécifiques, à différents groupes d'utilisateurs et à divers types de pirates. Les systèmes de détection doivent également être hautement personnalisables en fonction des besoins spécifiques de votre environnement. Ces défis exigent une solution XDR qui prenne en charge les détections personnalisées et prédéfinies.
- **Détection basée sur le Machine Learning :** avec des attaques qui ne ressemblent pas à des logiciels malveillants traditionnels, comme celles qui compromettent des fichiers système autorisés, utilisent des environnements de script et attaquent le registre, la technologie de détection doit utiliser des techniques analytiques avancées pour analyser toute la télémétrie collectée. Ces approches comprennent le Machine Learning supervisé et semi-supervisé.

CONSEIL

Recherchez une solution XDR qui répond aux exigences clés suivantes en matière de visibilité et de détection :

- L'analyse comportementale permet d'établir le profil du comportement et de détecter les anomalies révélatrices d'une attaque en analysant le trafic réseau, les événements liés aux terminaux et ceux liés aux utilisateurs au fil du temps
- Capacités de Machine Learning supervisé et non supervisé
- Règles de détection prédéfinies et personnalisables basées sur le comportement
- Règles personnalisées permettant de détecter rétroactivement les attaques
- Exclusions d'alertes granulaires pour le réglage optionnel des alertes concernant les terminaux, réseaux, clouds ou tiers
- Le partage d'informations sur les menaces permet de distribuer des renseignements provenant de sources multiples aux pare-feux, agents terminaux et services de détection et de réponse, à partir d'un service d'analyse des logiciels malveillants basé dans le cloud
- Capacité à consommer des flux de renseignements sur les menaces provenant de sources tierces dans les formats JSON (JavaScript Object Notation) et CSV (Comma-Separated Values)
- Détection des techniques d'attaque tout au long du cycle de vie de l'attaque, y compris la découverte, le mouvement latéral, le contrôle et le pilotage, et l'exfiltration

- Capacité démontrée à détecter les tactiques et techniques des pirates grâce aux évaluations de tactiques, techniques et connaissances communes contradictoires (ATT&CK) de MITRE
- Marquage des tactiques et techniques ATT&CK de MITRE dans les alertes et les règles de détection
- Gestion des actifs avec découverte des appareils malveillants
- Évaluation des vulnérabilités
- Inventaire des hôtes avec des informations détaillées sur les utilisateurs, les systèmes et les applications

Automatisation des enquêtes et des réponses

Lorsque vous êtes alerté de menaces potentielles dans votre environnement, vous devez être en mesure de les trier et de les examiner rapidement et de manière efficace. C'est là où les systèmes traditionnels de détection et de réponse échouent, surtout lors d'une attaque qui touche plusieurs parties de votre environnement. Les solutions XDR peuvent améliorer considérablement ce processus grâce à des capacités d'enquête et de réponse qui incluent les fonctionnalités suivantes :

- **Corrélation et regroupement d'alertes et de données télémétriques connexes :** lorsqu'il s'agit d'attaques contre votre organisation, le temps est un facteur essentiel. Au moment où vous recevez une alerte, le pirate est déjà à pied d'œuvre pour mener à bien sa mission et atteindre ses objectifs dans votre environnement. Vous devez être capable de comprendre rapidement l'attaque et sa chaîne de causalité complète. Cela signifie que votre outil XDR doit d'abord réduire le bruit en regroupant automatiquement les alertes connexes et en hiérarchisant efficacement les événements qui requièrent le plus d'attention. Votre outil XDR doit ensuite être en mesure d'établir une chronologie de l'attaque, en assemblant les journaux d'activité de votre réseau, de vos terminaux et de vos environnements cloud. En visualisant l'activité et en séquençant les événements, il est possible de déterminer la cause profonde de la menace et d'évaluer les dommages et la portée potentiels (voir la figure 2-2).

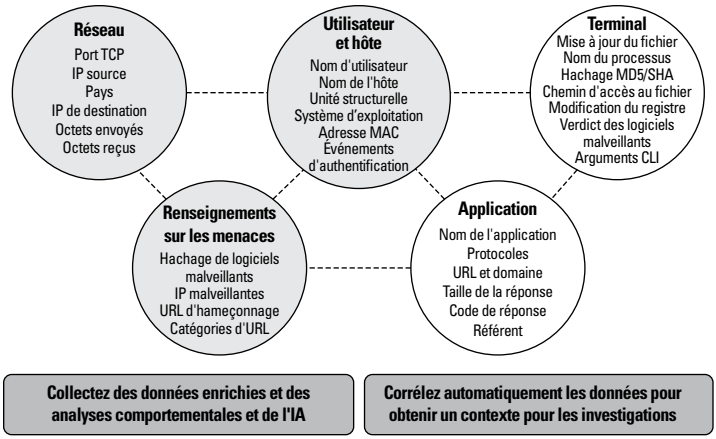

FIGURE 2-2 : XDR met en corrélation et assemble des données enrichies.

- **Enquête rapide sur les incidents grâce à un accès instantané à tous les artefacts, événements et renseignements sur les menaces en un seul endroit :** identifiez rapidement l'activité des pirates en examinant les principaux artefacts comme les journaux d'événements, les clés de registre, l'historique du navigateur, et bien plus encore. Les outils open source d'aujourd'hui obligent les équipes à rassembler des preuves à partir d'un assortiment hétéroclite d'agents et de scripts. Les agents à usage unique pour la forensique, la protection des terminaux et la détection et la réponse peuvent réduire les performances et ajouter à la complexité. Pour résoudre un incident, vous devez trouver le point d'entrée et traquer les éléments restants, même si les adversaires ont tenté de brouiller les pistes.
- **Interfaces utilisateur consolidées avec possibilité de pivoter rapidement :** lorsqu'ils commencent à creuser dans les alertes, vos analystes de sécurité ont besoin d'un environnement de travail rationalisé qui leur permette de pivoter dans les données de n'importe quelle source en un seul clic. Les analystes ne doivent pas perdre de temps à passer d'un outil à un autre.
- **Chasse aux menaces manuelle et automatisée :** de plus en plus d'organisations mènent une chasse proactive aux adversaires actifs, permettant à leurs analystes de développer des hypothèses d'attaque et de rechercher des activités pertinentes dans l'environnement. Pour favoriser la chasse aux menaces, il faut des capacités de recherche puissantes permettant de trouver des preuves pour prouver les hypothèses, ainsi que des renseignements intégrés sur

les menaces pour rechercher les activités déjà observées dans le réseau étendu. Ces renseignements sur les menaces doivent être intégrés et automatisés de manière à indiquer clairement si une menace a déjà été vue auparavant sans exiger des tonnes de travail manuel d'analyse (par exemple, ouvrir 30 onglets différents sur un navigateur pour rechercher une adresse IP malveillante connue dans de nombreux flux de renseignements sur les menaces).

- **Orchestration des réponses :** une fois les menaces détectées et examinées, l'étape suivante consiste à prendre des mesures correctives et à appliquer des politiques de manière efficace. Votre système doit être capable d'orchestrer une réponse coordonnée aux menaces actives et de prévenir les futures attaques sur l'ensemble de votre réseau, de vos terminaux et de vos environnements cloud. Cela induit une communication entre les technologies de prévention (c'est-à-dire qu'une attaque bloquée sur le réseau met automatiquement à jour les politiques sur les terminaux), soit de manière native, soit par le biais d'interfaces de programmation d'applications (API). Cela permet également à un analyste de prendre des mesures d'intervention directement via l'interface XDR.

CONSEIL

Recherchez les capacités d'investigation et de réponse suivantes dans une solution XDR :

- Analyse automatisée des causes profondes de toute alerte, y compris les alertes réseau, si les données relatives aux terminaux sont disponibles
- Visualisation des chaînes d'exécution menant à une alerte
- Affichage de l'analyse chronologique pour voir toutes les actions et alertes dans une chronologie
- Recherche d'indicateurs de compromission (IOC) et de comportements de terminaux, d'hôtes en ligne et hors ligne, de logs de trafic réseau provenant de pare-feux et de logs d'authentification provenant de fournisseurs de gestion des identités
- Langage d'interrogation avancé avec prise en charge des caractères génériques, des expressions régulières, de JSON, de l'agrégation de données, de la manipulation des champs et des valeurs, de la fusion de données provenant de sources disparates et de la visualisation des données
- Capacité d'un analyste à pivoter facilement entre les vues avec filtrage granulaire et tri des résultats de requête
- Regroupement automatique des informations pertinentes relatives au protocole Internet (IP) ou au hachage, y compris les

renseignements sur les menaces, les événements et les incidents connexes dans une vue unique afin de simplifier les enquêtes et de bloquer l'accès aux adresses IP ou aux domaines malveillants

- Identification du blocage d'un événement par un agent de terminal, un pare-feu ou une autre technologie de prévention, et possibilité de visualiser, de suspendre ou d'interrompre à distance les processus en cours ou de télécharger des fichiers binaires
- Assemblage automatisé des alertes de sécurité, comme les alertes de pare-feu, aux données des terminaux
- Suppression du bruit et suppression des binaires non significatifs et des bibliothèques de liens dynamiques (DLL) de la chaîne
- Identification et mise en contexte des tactiques, techniques et procédures (TTP) auprès de l'analyste SOC afin d'utiliser les connaissances acquises pour faciliter les futures enquêtes
- Intégration avec les solutions d'orchestration, d'automatisation et de réponse à la sécurité (SOAR) et de gestion des informations et des événements de sécurité (SIEM)
- La notation des incidents permet de classer et de hiérarchiser les incidents à haut risque afin de se concentrer rapidement sur les menaces les plus critiques ; la création de notes pour les incidents est basée sur les attributs des alertes, y compris les utilisateurs ou les hôtes dans une alerte
- Mise en quarantaine des fichiers malveillants et suppression de leurs répertoires de travail
- Recherche et suppression rapides des fichiers à l'échelle de l'organisation grâce à une fonctionnalité de recherche et de destruction, qui indexe les fichiers des terminaux
- Accès direct aux terminaux avec Live Terminal pour exécuter des commandes ou des scripts Python, PowerShell ou système ; examen et gestion des processus actifs ; et visualisation, suppression, déplacement ou téléchargement de fichiers

Améliorer l'efficacité de la sécurité

XDR est censé accélérer considérablement votre retour sur investissement (ROI) en matière de sécurité. Cela signifie accroître l'efficacité de votre équipe de sécurité pour lui permettre de prévenir ou de surmonter les pénuries de personnel, d'améliorer l'intégration entre vos outils existants et de renforcer l'efficacité de votre prévention au fil du temps grâce à une infrastructure évolutive et à l'intelligence artificielle (IA).

Pour répondre à ces critères, la solution XDR doit avoir les capacités suivantes :

- **Orchestration de la sécurité :** les mêmes attributs qui rendent l'orchestration importante pour simplifier les enquêtes lui permettent également de maximiser le retour sur investissement de votre pile de sécurité. Chaque organisation dispose de solutions de sécurité qui peuvent être mises à contribution pour répondre aux menaces en cours. L'un des aspects essentiels de tout système de détection et de réponse consiste à tirer parti des investissements dans ces solutions existantes, en veillant à ce que toute réponse puisse être entreprise de manière cohérente dans toute l'entreprise.
- **Ingestion de données tierces :** chaque organisation dispose aujourd'hui d'un ensemble d'outils de sécurité disparates et cloisonnés. Plus une solution XDR est capable d'avoir une visibilité sur les données provenant de chacun de ces différents outils, plus la sécurité qu'elle sera en mesure d'offrir sera complète. Les meilleures solutions XDR auront la flexibilité d'ingérer des données provenant d'autres outils dans votre environnement afin de maximiser la valeur et l'efficacité.
- **Stockage et calcul évolutifs :** compte tenu de la persistance des pirates actuels, il ne serait pas judicieux d'écarter la télémétrie qui peut fournir d'importantes preuves forensiques de l'activité du cybercriminel dans des attaques « lentes et discrètes » qui peuvent durer des mois, voire des années. Vous avez également besoin de la puissance analytique pour pouvoir utiliser efficacement toute cette télémétrie. Les plateformes XDR basées sur le cloud offrent cette accessibilité et cette échelle pratiquement illimitées.
- **Amélioration au fil du temps :** la détection d'attaques de plus en plus sophistiquées nécessite une IA et un Machine Learning intégrés, ainsi que l'automatisation et l'orchestration pour réduire les efforts manuels et permettre aux analystes de sécurité d'être plus efficaces. Les solutions XDR doivent tirer les leçons des précédentes expériences, réduire les risques futurs et renforcer continuellement la prévention en appliquant les connaissances acquises par la détection, l'enquête et la réponse.
- **Rapports et tableaux de bord :** les équipes de sécurité doivent être en mesure de comprendre et de communiquer la politique de sécurité de l'organisation et les paramètres opérationnels. Les solutions XDR doivent être capables de fournir de meilleurs résultats en matière de sécurité et de résumer l'état de la sécurité au moyen de rapports et de tableaux de bord intuitifs et personnalisables.

Ami ou ennemi ? Définition d'une véritable solution XDR

La technologie XDR est de plus en plus acceptée et reconnue par la communauté des analystes, les fournisseurs de solutions de sécurité et les utilisateurs finaux dans leur ensemble, mais comme d'autres catégories de solutions de sécurité, elle se décline en plusieurs catégories. Et comme certaines catégories de solutions XDR ne sont qu'une nouvelle mouture de la détection et de la réponse sur les terminaux (EDR), les fournisseurs ne partagent pas nécessairement les mêmes capacités. Cela vaut donc la peine d'examiner les solutions proposées d'un peu plus près.

Alors, comment faire la différence entre les différentes options disponibles sur le marché ? Selon un grand analyste du secteur, « seule une petite liste de fournisseurs peut vraiment offrir un produit XDR ». Comment pouvez-vous déterminer si une solution est véritablement XDR ou si c'est un autre fournisseur qui a pris le train en marche ? Les spécifications suivantes, bien que non exhaustives, peuvent aider à distinguer les acteurs sérieux des amateurs.

Une véritable solution XDR :

- Doit être capable d'absorber, de normaliser et de traiter des données provenant de toutes les sources de données (y compris de sources de données tierces)
- Doit permettre l'assemblage des données, et non une simple corrélation des données
- Est une solution « cloud native » qui peut évoluer à l'infini
- Combine de manière native le réseau, les terminaux, les identités et le cloud pour une analyse des données croisées
- Applique une logique intelligente et avancée pour afficher l'histoire complète d'un incident dans une seule vue
- Associe automatiquement les preuves et les artefacts au cadre ATT&CK de MITRE
- Offre une capacité intégrée pour effectuer des analyses forensiques approfondies
- Est soutenue par des équipes hors pair de recherche et de services de sécurité

La solution privilégie-t-elle la prévention ?

XDR signifie « extended detection and response » (détection et réponse étendues), et sa force réside dans la capacité d'interopérer à un niveau

(suite)

(suite)

d'intégration profond avec des dispositifs capables de bloquer, de perturber et de contenir les menaces et les attaques avant que des dommages ne se produisent. Les plus importants de ces dispositifs sont les pare-feux et les terminaux des réseaux de nouvelle génération, car le réseau contient le registre complet des communications et des terminaux et la façon dont les utilisateurs interagissent avec toutes les applications et les données.

La solution base-t-elle les détections uniquement sur le terminal ?

La solution peut-elle détecter les attaques basées sur l'identité, le cloud et les données du réseau, y compris entre des appareils non gérés ? Certains fournisseurs XDR affirment qu'ils voient les données du réseau alors qu'il s'agit en réalité du trafic réseau collecté par les agents des terminaux.

Une véritable solution XDR permettra de capter et interpréter n'importe quelle donnée avec l'activité de la menace et de l'étiqueter avec les TTP ATT&CK de MITRE afin de fournir une image plus détaillée du mouvement et des intentions des adversaires.

La solution dispose-t-elle de capacités d'enquête et de réponse natives ?

Une véritable solution XDR :

- Utilise les analyses de sécurité pour automatiser les recommandations de réponse
- Permet des actions de réponse natives sur le terminal
- Peut prendre en charge, mais ne nécessite pas, des intégrations avec d'autres outils comme SOAR pour la réponse
- Permet une réponse sur l'ensemble du réseau de terminaux et les points de mise en conformité cloud au lieu du terminal seulement
- Permet une prise en charge native de la recherche ad hoc dans toutes les sources de données tierces en utilisant des méthodes d'investigation et de recherche optimisées pour les analystes
- Optimise le triage et les investigations en faisant apparaître tous les artefacts malveillants, les hôtes, les utilisateurs et les alertes corrélées, mis en correspondance avec les techniques ATT&CK de MITRE
- Peut fournir des recommandations intelligentes pour des actions de réponse ciblées basées sur les techniques ATT&CK de MITRE

DANS CE CHAPITRE

- Examiner de plus près le cycle de vie des attaques
- Explorer un exemple d'attaque multidimensionnelle

Chapitre 3
Briser le cycle de vie des attaques avec XDR

Les pirates ont évolué, passant d'attaques directes contre un serveur ou un bien de grande valeur (« choc et effroi ») à un processus patient, en plusieurs étapes, qui mêle codes ou logiciels malveillants, furtivité et évasion dans une attaque coordonnée du réseau (« discrétion et lenteur »).

Dans ce chapitre, vous découvrez le cycle de vie des attaques et comment la détection et la réponse étendues (XDR) vous aident à briser ce cycle pour stopper les attaques contre votre environnement. Ce chapitre fournit une description générale des étapes courantes d'une attaque. De nombreuses équipes de sécurité ont adopté le cadre ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) de MITRE pour les aider à suivre les menaces à différents stades d'une attaque. Une véritable solution XDR doit être capable de détecter chaque étape effectuée par un adversaire et de faire correspondre chaque étape aux tactiques et techniques du cadre ATT&CK de MITRE afin de simplifier les investigations.

Comprendre le cycle de vie des attaques

Le cycle de vie des attaques illustre la séquence d'événements (ou d'étapes) que traverse un pirate pour infiltrer un réseau et exfiltrer (ou voler) des données précieuses. Ces étapes comprennent l'exploitation

initiale de la vulnérabilité, l'installation du logiciel malveillant, le contrôle et le pilotage, le mouvement latéral et l'exfiltration (voir la figure 3-1).

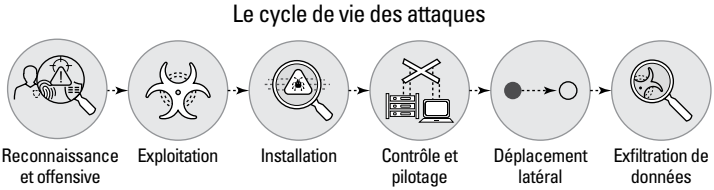

FIGURE 3-1 : Les attaques réussies se font en plusieurs étapes.

CONSEIL

Si vous arrivez à détecter les étapes initiales du cycle de vie, vous pourrez empêcher les pirates d'exécuter les étapes ultérieures d'une attaque. Les sections suivantes examinent de plus près le cycle de vie d'une attaque et la manière dont une solution XDR vous aide à briser ce cycle.

Reconnaissance

Les cybercriminels planifient méticuleusement leurs attaques. Ils recherchent, identifient et sélectionnent des cibles, en extrayant souvent des informations publiques des profils de médias sociaux des employés ciblés ou des sites Web de l'entreprise, qui peuvent être utiles pour l'ingénierie sociale et les plans de hameçonnage (phishing). Les pirates utilisent également divers outils pour rechercher les vulnérabilités du réseau, les services et les applications qu'ils peuvent exploiter, notamment des analyseurs de réseau, des scanners de vulnérabilité du réseau, des craqueurs de mots de passe, des scanners de ports et des scanners de vulnérabilité des applications Web.

XDR rompt le cycle de vie pendant la reconnaissance en surveillant et en inspectant en permanence les flux de trafic réseau afin de détecter et d'empêcher les analyses non autorisées de ports et de vulnérabilités, les analyses des hôtes et autres activités suspectes.

Offensive

Ensuite, les pirates déterminent les méthodes à utiliser pour compromettre un terminal cible. Ils peuvent choisir d'intégrer le code de l'intrus dans des fichiers apparemment inoffensifs, comme un document Microsoft Word ou un message électronique. Ou, dans le cas d'attaques très ciblées, ils peuvent personnaliser les produits livrables pour qu'ils correspondent aux intérêts spécifiques d'une personne au sein de l'organisation cible. Les pirates tentent ensuite de transmettre leur charge utile militarisée à un terminal cible, par exemple par courrier

électronique, par messagerie instantanée (MI), par téléchargement furtif (dans lequel le navigateur Web d'un utilisateur final est redirigé vers une page Web qui télécharge automatiquement le malware sur le terminal en arrière-plan) ou par partage de fichiers infectés.

Il est difficile de rompre le cycle de vie à cette phase de l'attaque, car l'offensive se produit généralement au sein du réseau du pirate. Toutefois, l'analyse des artefacts (tant les logiciels malveillants que les armes utilisés) peut fournir des renseignements importants sur les menaces afin de permettre une protection efficace contre les attaques « zero-day » lors de la tentative de livraison de la charge utile. XDR offre une visibilité sur l'ensemble du trafic réseau afin de bloquer efficacement les sites Web, les applications et les adresses IP malveillants ou à risque, et de prévenir les logiciels et codes malveillants connus et inconnus.

Exploitation

Une fois la charge utile livrée à un terminal cible, elle doit être déclenchée. Un utilisateur final peut déclencher involontairement un code malveillant, par exemple en cliquant sur un lien ou en ouvrant une pièce jointe infectée dans un e-mail, ou bien un pirate peut déclencher à distance ce même code pour une vulnérabilité connue du serveur sur le réseau cible.

Pour briser le cycle de vie à cette phase de l'attaque, il faut des capacités XDR, comme les suivantes :

- Gestion des vulnérabilités et des correctifs
- Détection et prévention des logiciels malveillants
- Renseignements sur les menaces (y compris les menaces connues et inconnues)
- Blocage des applications et des services risqués, non autorisés ou inutiles.

Enregistrement et surveillance de toutes les activités sur le réseau, les terminaux et cloud

JARGON TECHNIQUE

Un agent XDR efficace prévient les vulnérabilités connues, de type « zero-day » et non corrigées en bloquant les techniques d'exploitation que les pirates utilisent pour manipuler les applications. Bien qu'il existe des milliers de types d'attaques, ces pirates s'appuient généralement sur un petit ensemble de techniques d'exploitation qui changent rarement. En bloquant ces techniques, XDR empêche les tentatives d'exploitation avant que les terminaux ne puissent être compromis (voir la figure 3-2).

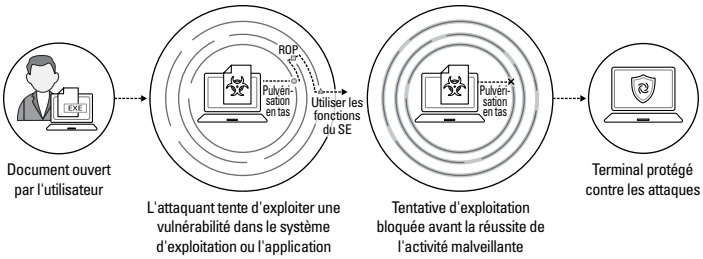

FIGURE 3-2 : Une solution XDR avancée se concentre sur les techniques et les comportements des attaques plutôt que sur les attaques elles-mêmes.

Installation

Ensuite, le pirate élèvera ses privilèges sur le terminal compromis (par exemple, en établissant un accès shell à distance et en installant des rootkits ou d'autres logiciels malveillants). Avec l'accès au shell à distance, le pirate prend le contrôle du terminal et peut exécuter des commandes en mode privilégié à partir d'une interface de ligne de commande (CLI), comme s'il était physiquement assis devant le terminal. Il se déplacera ensuite latéralement sur le réseau de la cible, en exécutant le code d'attaque, en identifiant d'autres cibles potentielles et en compromettant d'autres terminaux pour établir la persistance ou pérennité de son attaque.

La clé pour briser le cycle de vie à cette phase de l'attaque est d'empêcher toute installation sur le terminal et de limiter ou restreindre le mouvement latéral des pirates dans le réseau. XDR exploite les technologies de détection et de réponse sur les terminaux (EDR) et de la plateforme de protection des terminaux (EPP) pour empêcher toute installation. XDR surveille et inspecte également tout le trafic entre les zones ou les segments dans un modèle Zero Trust et fournit un contrôle granulaire des applications qui sont autorisées dans l'environnement.

Contrôle et pilotage

Les cybercriminels établissent des canaux de communication chiffrés vers les serveurs de commande et de contrôle sur Internet. Cette approche leur permet de modifier leurs objectifs et leurs méthodes d'attaque au fur et à mesure que de nouvelles cibles sont identifiées au sein du réseau de la victime. Elle leur donne aussi l'occasion d'échapper à toute nouvelle contre-mesure de sécurité que l'organisation peut tenter de déployer si des artefacts d'attaque sont découverts. La communication est essentielle à une attaque, car elle permet au pirate de diriger son offensive à distance et d'exécuter les objectifs de l'attaque. Le trafic de contrôle et de pilotage doit être résilient et furtif pour qu'une attaque réussisse.

Pour briser le cycle de vie à cette phase d'une attaque, il faut procéder comme suit :

- Inspecter tout le trafic réseau (y compris les communications chiffrées)
- Bloquer les communications sortantes de contrôle et de pilotage avec des signatures anti-contrôle et pilotage (ainsi que des téléchargements de fichiers et de modèles de données).
- Bloquer toutes les communications sortantes vers des URL et des adresses IP malveillantes connues.
- Bloquer les nouvelles techniques d'attaque qui utilisent des méthodes d'évasion des ports
- Empêcher l'utilisation d'anonymiseurs et de proxys sur le réseau
- Surveiller le système de noms de domaine (DNS) pour rechercher des domaines malveillants et lutter contre le DNS sinkholing ou le DNS poisoning
- Rediriger les communications sortantes malveillantes vers des honeypots afin d'identifier ou de bloquer les terminaux compromis et d'analyser le trafic d'attaque

Mouvement latéral et exfiltration

Les pirates ont souvent des objectifs multiples et différents, notamment le vol de données, la destruction ou la modification de systèmes, de réseaux et de données critiques, et le déni de service (DoS). Cette dernière étape du cycle de vie peut également être utilisée par un pirate pour lancer les premières étapes d'une attaque contre une autre cible. Par exemple, il peut compromettre l'extranet d'une entreprise pour pénétrer chez un partenaire commercial qui est la cible principale. Ces types d'attaques de la chaîne d'approvisionnement ont fait la une des journaux en 2020 avec l'attaque de SolarWinds.

Pour interrompre le cycle de vie à ce stade, il faut des outils XDR capables de détecter et de prévenir automatiquement l'exfiltration de données et d'autres actions malveillantes ou non autorisées.

Examen d'un exemple d'attaque

Pour mieux visualiser toutes les étapes du cycle de vie d'une attaque et leur rôle, examinons de plus près un exemple. Dans la figure 3-3, un cybercriminel exécute les étapes suivantes pour attaquer une cible :

1. Exploitation.

   L'attaquant exploite des bogues sur le serveur Web pour prendre le contrôle du serveur.

2. Installation.

   Le pirate utilise le contrôle du serveur pour installer mimikatz et avoir accès aux informations d'identification de l'administrateur.

3. Contrôle et pilotage.

   L'attaquant installe des logiciels malveillants supplémentaires et des outils d'accès à distance pour établir la persistance et les communications de contrôle et pilotage.

4. Déplacement latéral.

   L'adversaire se déplace latéralement sur le réseau, compromet plusieurs terminaux et accède à des applications de cloud privé et public.

5. Accès et exfiltration.

   Le pirate consulte les fichiers de configuration sur le serveur, trouve l'emplacement de la base de données principale, interroge la base de données et enregistre les résultats dans un fichier local. Les données collectées sont téléchargées vers un emplacement de stockage cloud « autorisé » ou « sanctionné ». L'attaquant supprime ensuite le fichier qui contient les données de la base de données, efface les logs locaux et ferme la session.

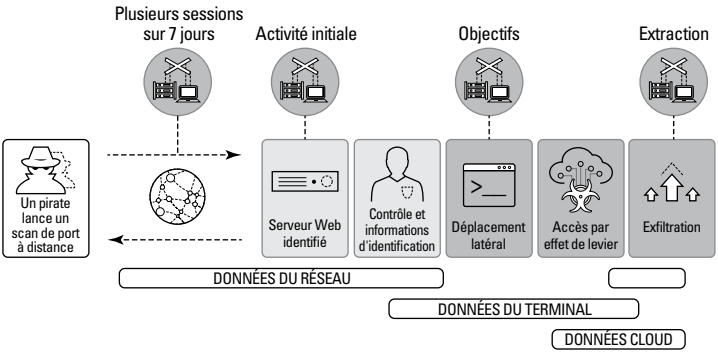

FIGURE 3-3 : Seule une solution XDR peut arrêter ces attaques avancées en plusieurs étapes, car elle collecte des données auprès de toutes les sources et peut détecter et stopper les tactiques d'attaque que d'autres outils ne peuvent pas identifier.

Une plateforme XDR rassemble et analyse une variété de types de données pour détecter et arrêter les tactiques des adversaires tout au long du cycle de vie de l'attaque.

DANS CE CHAPITRE

- Détecter les activités menaçantes avec XDR
- Gérer et valider des alertes
- Accélérer les investigations et les interventions
- Favoriser la chasse proactive aux menaces

Chapitre 4
Découvrir quelques cas d'utilisation XDR

Dans ce chapitre, je présente les cas d'utilisation les plus courants pour aider votre organisation à améliorer ses capacités de détection et de réponse, notamment la détection, le triage et la validation des alertes, l'automatisation des investigations et de la réponse, et la chasse aux menaces.

Détection

Pour stopper les cyberattaques et empêcher qu'elles n'aboutissent, vous devez vous concentrer sur la détection des attaques à chaque étape de leur cycle de vie. La détection et la réponse étendues (XDR) utilisent le Machine Learning pour découvrir les caractéristiques uniques de votre organisation, ce qui permet de différencier les activités menaçantes des activités normales, au-delà de ce qui est possible avec une analyse manuelle ou des règles de corrélation statiques. Cette capacité de Machine Learning alimente les analyses avancées, le profilage et la détection des menaces comportementales. Grâce à cette détection complète, une solution XDR améliore la capacité à détecter les activités néfastes, notamment les attaques ciblées, les initiés malveillants, etc.

Attaques ciblées

Les pirates tentent de mêler leurs activités à un usage légitime à chaque étape du cycle de vie de l'attaque. Grâce à la capacité de XDR à collecter des données de n'importe quelle source pour la détection et à assembler automatiquement les données de sécurité clés pour une analyse avancée des données croisées, vous pouvez détecter les attaques les plus furtives. Grâce à l'analyse, vous pouvez établir le profil du comportement des

utilisateurs et repérer les comportements anormaux, comme les tentatives d'un pirate de compromettre des appareils et de se déplacer latéralement sur le réseau, à la recherche de données sensibles afin de les exfiltrer.

Initiés malveillants

Les initiés malveillants utilisent leurs informations d'identification et leurs accès de confiance pour voler des données d'entreprise sans être détectés. XDR s'attaque à cette menace en recherchant des anomalies dans le comportement et l'activité des utilisateurs (voir la figure 4-1). Les solutions XDR peuvent rationaliser l'analyse en présentant une vue à 360 degrés de chaque utilisateur avec un score de risque clair.

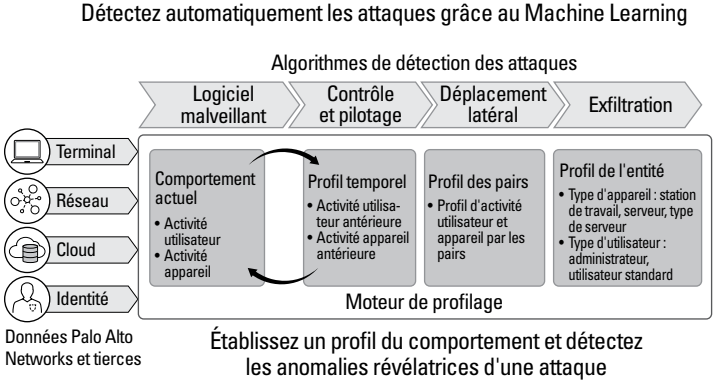

FIGURE 4-1 : L'analyse comportementale permet de découvrir des anomalies au niveau des utilisateurs, des applications et des appareils.

Risques involontaires

Les employés bien intentionnés peuvent, par inadvertance, exposer les organisations à des risques excessifs en raison de l'abus et de la mauvaise utilisation des accès autorisés. Une solution XDR permet aux organisations de suivre les meilleures pratiques de sécurité en surveillant l'activité des utilisateurs et en identifiant les comportements à risque afin de détecter lorsqu'un employé enfreint les politiques de sécurité, que ce soit par inadvertance ou non.

Terminaux compromis

Les pirates utilisent souvent des logiciels malveillants pour infiltrer les réseaux ciblés en compromettant un terminal et en se déplaçant latéralement dans le réseau. XDR rassemble les données de sécurité sur les réseaux et les terminaux pour rechercher le trafic anormal généré par les logiciels malveillants et autres activités néfastes. Ces données de sécurité permettent également d'enquêter sur l'ensemble de l'environnement afin de déterminer l'ampleur de l'attaque.

Par exemple, si un acteur de la menace ajoute une nouvelle valeur à la clé de registre Autorun, une solution XDR peut détecter la nouvelle valeur Autorun et générer une alerte décrivant clairement cette activité suspecte, y compris un contexte d'enquête enrichi avec la tactique et la technique ATT&CK de MITRE. La solution XDR peut même déterminer quel processus a ajouté la valeur Autorun et la séquence d'événements qui a conduit à la mise à jour pour fournir l'historique complet de l'attaque.

RAPPEL

XDR détecte les attaques actives avec une précision inégalée et augmente la capacité des équipes de sécurité à :

Détecter les activités malveillantes provenant de ressources internes et externes en trouvant des modèles parmi les activités qui se produisent sur le réseau, au niveau des terminaux et dans le cloud.

Utiliser des techniques d'analyse de pointe sur des quantités importantes de données de sécurité pour identifier les activités anormales sans augmenter le nombre de faux positifs.

Tirer parti des réponses internes et de la surveillance des menaces externes pour tirer des enseignements des attaques passées et rendre cette expérience accessible aux analystes moins avertis, en améliorant ainsi les performances de l'ensemble de l'équipe de sécurité.

Triage et enquête sur les alertes

Les solutions XDR simplifient le triage et l'analyse des alertes en révélant la cause profonde des alertes, ce qui permet de les examiner beaucoup plus rapidement. Si seules les données relatives au terminal sont disponibles, la cause fondamentale de celui-ci est présentée. Si des données sur le réseau et les terminaux sont disponibles, la plateforme XDR peut associer automatiquement l'activité du réseau aux événements des terminaux. Par exemple, une solution XDR ne se contente pas de déterminer quel exécutable d'un terminal est responsable d'une alerte réseau, elle peut aussi déterminer quelle application a lancé l'exécutable.

Compte tenu des défis posés par le déficit de compétences en matière de sécurité évoqué au Chapitre 1, XDR améliore la capacité d'un analyste moins expérimenté à détecter et à valider une attaque potentielle en regroupant les alertes en incidents et, au sein de ces incidents, en résumant les activités ou les actions sous forme de balises qui ajoutent du contexte. Cette flexibilité garantit que les connaissances sont capturées et exploitées pour l'ensemble de l'équipe.

XDR produit une chronologie des événements ayant conduit à l'alerte et fournit des renseignements intégrés sur les menaces. Tout cela permet

aux analystes de comprendre la cause profonde d'une alerte, la nature exacte de la menace et les mesures à prendre.

Voici comment XDR contribue à simplifier l'analyse des incidents et les enquêtes :

1. Évaluation.

   Le processus commence par l'évaluation par la solution XDR des alertes externes (provenant par exemple d'outils de sécurité tiers) et des alertes générées en interne (sur la base de règles et d'autres indicateurs) afin de déterminer les comportements potentiellement suspects.

2. Établissement de priorités.

   L'outil XDR regroupe ensuite automatiquement ces alertes en incidents, en attribuant à chacun un niveau de priorité afin de diriger les analystes vers les incidents qui représentent la plus grande menace. Les analystes peuvent cliquer sur chaque incident et consulter la liste complète des alertes, des appareils, des renseignements sur les menaces associées, ainsi que d'autres contextes permettant de comprendre toute la portée de l'alerte.

3. Analyse.

   XDR fournit une chaîne d'attaque visuelle (voir la figure 4-2), en tirant parti des diverses sources de télémétrie pour collecter tout ce qui est pertinent pour l'incident et fournir un contexte et une causalité supplémentaires, et pour assurer une analyse plus rapide et plus efficace. La chaîne d'attaque montre les étapes suivies par un pirate en révélant la séquence des processus qui ont conduit à l'étape finale de l'attaque. En plus d'afficher les alertes associées, y compris une alerte EPP pour l'agent XDR, elle identifie également la cause première.

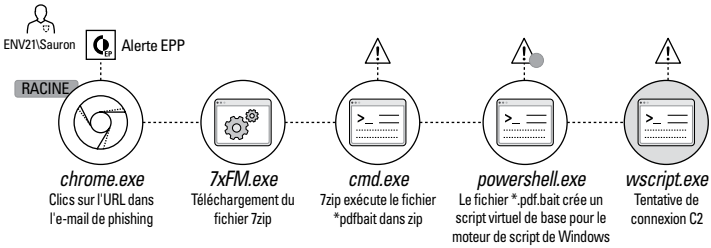

FIGURE 4-2 : Un exemple de chaîne d'attaque visualisée à l'aide de XDR.

4. Enrichissement.

   La chaîne d'attaque est ensuite enrichie d'informations contextuelles supplémentaires, notamment une vue détaillée de la façon

dont l'alerte a été générée, de sa cause première, des autres dispositifs impliqués (terminaux, réseau et cloud) et de la réputation de tous les artefacts forensiques.

Avec des milliers d'alertes arrivant chaque jour, l'automatisation du processus de triage et la fourniture aux analystes d'informations contextuelles enrichies sont les seuls moyens de gérer ce volume. Grâce à XDR, les équipes de sécurité peuvent concentrer leur temps et leur énergie là où elles auront le plus d'impact, c'est-à-dire pour remédier aux alertes susceptibles de causer le plus de dommages.

RAPPEL

Avec XDR, les analystes disposent d'une capacité accrue pour :

Réduire l'arriéré d'alertes grâce à la gestion des incidents, au regroupement intelligent des alertes et au contexte d'enquête.

Réduire dramatiquement les chances qu'une attaque passe inaperçue.

Analyser les alertes afin d'améliorer la détection, ainsi que pour s'assurer que la productivité et les défenses en aval ne sont pas affectées.

Appliquer de nouveaux déclencheurs comportementaux pour améliorer les délais de triage, et éventuellement transformer les règles de détection en règles de prévention pour une prévention en boucle fermée.

Enquêtes et réponses automatisées et simplifiées

Après le triage et la priorisation d'une alerte, une enquête plus approfondie est justifiée. L'automatisation de XDR accélère le processus d'investigation de toute alerte ou campagne de chasse et élimine les tâches manuelles fastidieuses en fournissant une image claire de la menace, en effectuant une analyse des causes profondes, en vérifiant la réputation et en résolvant l'attribution des attaques.

Les outils XDR commencent par regrouper toutes les données télémétriques dans un référentiel de données de sécurité, comme un lac de données cloud (voir la figure 4-3). Pour réduire le délai d'investigation, la solution XDR peut corréler et regrouper les alertes provenant de différents outils de détection en un petit nombre d'incidents précis et exploitables, y compris des informations sur les utilisateurs, les applications et les appareils. Elle peut également faciliter les investigations forensiques en interrogeant les terminaux pour déterminer quel processus ou exécutable a lancé une attaque.

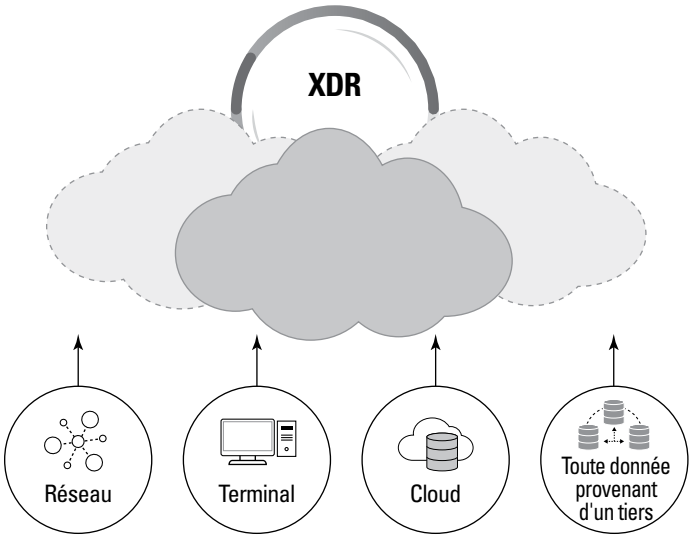

FIGURE 4-3 : Les outils XDR rassemblent les données de différents capteurs dans un référentiel de données basé sur le cloud.

Pour approfondir l'incident, une solution XDR détermine ensuite si le processus du terminal est malveillant. Pour ce faire, elle s'intègre aux sources et services de renseignements sur les menaces pour analyser le processus. Une solution XDR permet aux analystes de sécurité de vérifier facilement les attaques en présentant toutes les informations dont ils ont besoin dans une interface unique.

Les outils XDR peuvent également adapter les défenses, en appliquant les connaissances tirées d'incidents et de campagnes de chasse antérieures pour empêcher automatiquement la réapparition de toute menace découverte précédemment. Cet « apprentissage assisté » permet une détection précoce des attaques sur la base de ce qui a déjà été identifié dans l'environnement.

Une fois la menace validée, les intervenants peuvent choisir parmi des dizaines de techniques de réponse et de correction à distance pour stopper l'attaque, empêcher les attaques suivantes, restaurer les fichiers endommagés ou supprimés, etc. Les options de réponse comprennent l'isolement des terminaux, le blocage, la suppression ou la mise en quarantaine des fichiers, le rétablissement des fichiers et du registre dans un état approprié, l'accès direct aux terminaux et l'exécution de scripts. Ainsi, l'équipe de sécurité deviendra très efficace, nécessitera moins de formation, réduira la charge des intervenants plus expérimentés et minimisera les délais de résolution des incidents.

RAPPEL

Avec XDR, les intervenants en cas d'incident disposent d'une capacité accrue pour :

Trouver plus rapidement les menaces furtives en exploitant les renseignements sur les menaces et l'analyse comportementale.

Simplifier et accélérer les investigations et les interventions en effectuant des recherches approfondies et étendues dans la télémétrie recueillie sur les réseaux, les terminaux et le cloud.

Chasse aux menaces

Les solutions XDR améliorent vos capacités de chasse aux menaces grâce à l'identification automatique et ad hoc des activités malveillantes dans votre environnement. Les chasseurs de menaces peuvent effectuer des requêtes avancées et obtenir des résultats instantanés. Voici quelques exemples de la manière dont XDR fournit les capacités nécessaires pour différentes méthodes de chasse aux menaces :

- **Chasse basée sur des renseignements :** il s'agit du type d'exercice de chasse aux menaces le plus courant, dans lequel le chasseur a reçu un indice sur une menace avant de la rechercher. Qu'il s'agisse d'une piste provenant des renseignements sur les menaces, d'un nouvel indicateur de compromission (IOC), d'une information provenant d'une personne au sein de l'organisation ou d'une simple suspicion, la complexité de la chasse aux menaces basée sur les renseignements dépendra du niveau de détail fourni par les renseignements. À partir d'une source de données intégrée liée à plusieurs fournisseurs de renseignements sur les menaces, une solution XDR peut importer manuellement des artefacts ou des IOC à partir de différentes normes pour fournir des résultats de recherche rapides et solides.
- **Chasse sans piste :** venant juste après en terme d'approches communes de la chasse aux menaces, l'approche sans piste consiste pour le chasseur à utiliser ses propres connaissances ou des connaissances recherchées sur la manière dont un ordinateur, une application, un utilisateur, des données ou un réseau sont censés être utilisés et vise à identifier une utilisation irrégulière ou anormale. Ce type de chasse aux menaces avancées est généralement laissé aux membres les plus expérimentés de l'équipe qui utilisent des techniques comme le découpage et l'analyse des données pour obtenir des résultats. Une solution XDR simplifie ce processus en intégrant ces techniques avancées dans son interface, ce qui permet aux chasseurs, quel que soit leur niveau d'expérience, de tirer parti de ces techniques sans scripts, sans outils supplémentaires et sans avoir à apprendre un nouveau langage de requête.

- **Chasse basée sur les résultats :** dans cette approche, le chasseur examine les alertes passées mises en quarantaine, les enquêtes terminées ou toute autre menace résolue et les utilise pour identifier les variantes de la menace, les nouvelles menaces potentielles ou les vecteurs d'attaque ouverts. Une solution XDR de qualité peut intégrer automatiquement et en permanence la chasse aux menaces basée sur les résultats directement dans le flux de travail des alertes de sécurité et du traitement des incidents. Les enseignements tirés de chaque enquête sont appliqués pour éviter que vous ne soyez frappé par des attaques répétées.
- **Chasse basée sur la conformité :** cette approche de la chasse aux menaces vise à garantir la conformité aux exigences internes, sectorielles et gouvernementales en effectuant des recherches de routine qui indiquent une non-conformité, comme des données sensibles stockées sur des systèmes non autorisés ou une escalade des privilèges par des utilisateurs administrateurs. Une solution XDR peut être configurée pour alerter les analystes de sécurité de ce type d'activité et leur fournir un moyen d'enquêter rapidement sur la situation.
- **Chasse basée sur le Machine Learning :** les systèmes de Machine Learning établissent une base de référence des comportements typiques d'une organisation pour comprendre ce qui est normal et ce qui ne l'est pas. Grâce à des analyses à grande échelle, les solutions XDR utilisent le Machine Learning pour surveiller les comportements et identifier les anomalies qui s'écartent de ces lignes de base. Ces indicateurs comportementaux de compromission (BIOC) détectent de nombreuses menaces furtives qu'un analyste n'est pas toujours en mesure d'identifier manuellement et sont continuellement optimisés au fil du temps pour améliorer le modèle de Machine Learning. Cette forme de chasse aux menaces représente le gain de temps ultime pour les analystes et est essentielle pour optimiser les résultats en matière de sécurité.

RAPPEL

Avec XDR, les chasseurs de menaces disposent d'une capacité accrue pour :

- Tirer parti des données du réseau, des terminaux et du cloud pour les recherches et les analyses.
- Exploiter l'automatisation afin d'effectuer des recherches sur l'ensemble des activités du réseau, des terminaux et cloud.
- Utiliser des recherches et des assistants hautement configurables pour trouver les menaces internes et externes identifiées par les IOC traditionnels et les BIOC stockés dans votre bibliothèque de menaces.
- Remédier aux attaques par l'intégration de contrôles de sécurité.

IN THIS CHAPITRE

- Ensuring robust threat prevention and complete visibility
- Simplifying investigations with analytics, machine learning, coordinated response, and orchestration features
- Maximizing flexibility with a full protection suite
- Looking at third-party validation, innovative road maps, and total value

Chapitre 5
Dix fonctionnalités clés de XDR

La détection et la réponse étendues (XDR) permettent aux organisations de prévenir les cyberattaques réussies et de simplifier et renforcer leurs processus de sécurité en utilisant une approche proactive de la détection et de la réponse aux menaces. XDR bloque les attaques modernes en rassemblant et en analysant les données provenant de n'importe quelle source. Cette solution unifie la prévention, la détection, l'investigation et la réponse afin d'offrir une sécurité et une efficacité opérationnelle inégalées.

Ce chapitre présente les dix éléments essentiels à rechercher dans une solution XDR pour votre organisation. Il explique également comment Cortex XDR, première plateforme de détection et de réponse étendues du secteur, offre ces fonctionnalités essentielles.

Meilleure prévention des menaces sur les terminaux

La protection de votre entreprise commence par la prévention optimale des menaces sur les terminaux, qui bloque les logiciels et codes malveillants, les ransomwares et les attaques sans fichier, connus et inconnus.

RAPPEL

Cortex XDR fournit tout ce dont vous avez besoin pour la prévention, la détection et la réponse aux menaces avec un agent unique géré depuis le cloud. Cette plateforme protège vos terminaux grâce à une analyse locale et une protection basée sur le comportement (voir la figure 5-1), fondées sur l'intelligence artificielle (IA) et les meilleures pratiques du secteur.

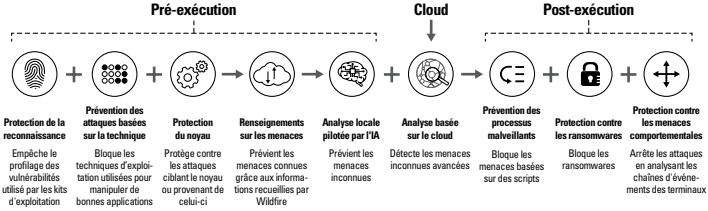

FIGURE 5-1 : Cortex XDR offre une prévention complète des menaces sur les terminaux.

Recherchez un antivirus de nouvelle génération qui fournit :

- Une protection contre les logiciels malveillants, les ransomwares et les menaces sans fichier
- Des renseignements sur les menaces mondiales en temps réel basés sur le cloud
- Une analyse locale via Machine Learning
- Une protection contre les menaces comportementales
- Une protection granulaire des processus enfants
- Une prévention des attaques en amont basée sur des techniques
- Une prévention des attaques du noyau
- Une protection contre le vol d'informations d'identification

Suite flexible de fonctionnalités de protection des terminaux

Vous avez besoin d'un moyen simple d'identifier et de hiérarchiser les risques liés aux terminaux, de réduire votre surface d'attaque et de mettre fin aux pertes de données. Recherchez des fonctionnalités de protection des terminaux, notamment les suivantes :

- **Évaluation des vulnérabilités :** profitez de l'évaluation des vulnérabilités, de la visibilité des applications sur les terminaux gérés et non gérés, et plus encore pour obtenir une vue d'ensemble de vos actifs numériques.
- **Pare-feu hôte :** gérez de manière centralisée les communications entrantes et sortantes sur vos terminaux à partir de la console de gestion Cortex XDR.
- **Chiffrement du disque :** appliquez des politiques de chiffrement ou de déchiffrement sur vos terminaux et consultez les listes de tous les lecteurs chiffrés.
- **Contrôle des appareils :** surveillez et contrôlez de manière granulaire l'accès au bus série universel (USB) pour protéger vos terminaux.

Visibilité étendue à toutes les sources de données

Pour réduire le risque d'une attaque réussie, vous avez besoin d'une approche globale de la détection et de la réponse qui élimine les angles morts, augmente la précision et rationalise les investigations dans tous les environnements, y compris le réseau, le cloud et les terminaux.

CONSEIL

Cortex XDR est la première plateforme XDR du secteur qui intègre nativement les données des terminaux, du réseau et du cloud pour stopper les attaques sophistiquées. Cortex XDR offre toutes les fonctionnalités de détection et de réponse sur le réseau (NDR), de détection et de réponse sur les terminaux (EDR), de protection des terminaux (EPP), de détection et de réponse dans le cloud (CDR) et d'analyse du comportement des utilisateurs et des entités (UEBA), comme le montre la figure 5-2.

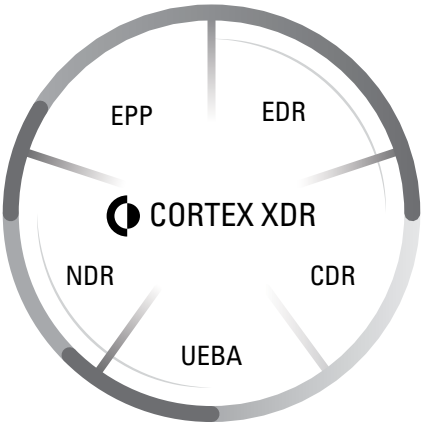

FIGURE 5-2 : Cortex XDR recueille et analyse des données enrichies pour offrir les capacités traditionnellement fournies par les outils EPP, EDR, NDR, CDR et UEBA.

Investigations *simplifiées*

Les outils de sécurité actuels, cloisonnés, génèrent des alertes sans fin avec un contexte limité. Selon le *rapport* 2020 *Cost of a Data Breach* du Ponemon Institute, le délai moyen pour identifier et contenir une violation est de 280 jours. Pour réduire les temps de réponse, les outils de sécurité doivent fournir une image complète des incidents avec des détails d'investigation enrichis.

CONSEIL

Cortex XDR simplifie les enquêtes en révélant automatiquement la cause profonde, la séquence des événements et les détails des alertes en matière de renseignements sur les menaces. Cette plateforme réduit le temps d'investigation de 88 % en révélant la cause profonde et le contexte enrichi des alertes concernant le réseau, les terminaux et le cloud, et réduit les alertes de 98 % grâce au regroupement et à la déduplication intelligents des alertes.

Analyses et Machine Learning

Les cybercriminels s'appuient sur le cloud et les technologies de Machine Learning pour augmenter l'échelle et l'efficacité de leurs attaques. Vous avez besoin d'un ensemble complet de techniques de Machine Learning et d'analyse pour anticiper les menaces qui évoluent rapidement et contrer les attaques sophistiquées.

RAPPEL

Cortex XDR fournit :

- Une analyse locale pilotée par l'IA pour bloquer les logiciels malveillants
- Une analyse comportementale pour détecter les intrusions et les attaques actives
- Une analyse globale pour améliorer la précision et la couverture de la détection

Réponse coordonnée

Après avoir identifié les menaces dans votre environnement, vous devez les contenir rapidement. Votre équipe a besoin d'options de réponse intégrées et flexibles pour mettre fin aux attaques rapidement et efficacement avant qu'elles ne fassent plus de dégâts. Une solution XDR doit permettre à votre équipe d'arrêter à distance la propagation des logiciels malveillants, de restreindre l'activité du réseau en provenance et à destination des appareils, et de mettre à jour les listes de prévention des menaces, comme les domaines risqués, grâce à une intégration étroite avec les points d'application.

CONSEIL

Cortex XDR permet à votre équipe de sécurité d'éliminer instantanément les menaces liées au réseau, aux terminaux et au cloud à partir d'une seule console.

Automatisation des tâches de sécurité

Les tâches et processus manuels ralentissent la réponse aux incidents et augmentent le coût des opérations de sécurité. En exécutant une série d'actions de réponse nativement sur le terminal et sur d'autres points d'application clés, les solutions XDR peuvent rapidement contenir les menaces. Les SOC avancés peuvent nécessiter des processus comprenant une logique de décision et une orchestration du flux de travail contrôlées par des manuels et comprenant une série d'actions sur un large éventail d'outils de sécurité et informatiques provenant de différents fournisseurs. Une solution complète d'automatisation et d'orchestration de la sécurité, qui fournit une logique d'orchestration et dispose d'intégrations étendues avec des partenaires, ainsi que de contenus et manuels préétablis, peut répondre à ces exigences. Par conséquent, recherchez une solution XDR qui s'intègre étroitement à une plateforme SOAR de pointe.

RAPPEL

Cortex XDR s'intègre étroitement à Cortex XSOAR pour une gestion complète des renseignements sur les menaces et offre plus de 750 intégrations de partenaires et 680 packs de contenu pour vous permettre de faire passer vos opérations de sécurité au niveau supérieur.

Tests et validation indépendants

Lorsque vous choisissez une solution XDR, vous devez toujours examiner les tests effectués par des tiers, la validation des analystes et les témoignages des clients pour obtenir une perspective indépendante et objective.

CONSEIL

Cortex XDR a obtenu des résultats exceptionnels lors de tests, notamment la meilleure combinaison de détection et de protection lors de l'évaluation ATT&CK de MITRE Round 3, et un classement « Strategic Leader » lors du test AV-Comparatives Endpoint Prevention and Response (EPR). Encensée par les clients et les critiques, la plateforme Cortex XDR est un outil fiable pour protéger vos terminaux et vos données.

Rapidité de l'innovation

Pour devancer des adversaires qui évoluent rapidement, recherchez des fournisseurs qui renforcent ou étendent continuellement les capacités de leurs produits.

CONSEIL

Cortex XDR continue de redéfinir la manière dont les équipes chargées des opérations de sécurité traitent les menaces modernes complexes et gagnent en efficacité. En s'attaquant au problème de l'intégration des systèmes de collecte, d'intégration et d'analyse des données et en le couplant à la capacité de lancer des flux de travail hautement optimisés et automatisés, XDR permet de relever les défis de la détection, de l'investigation et de la réponse à grande échelle de manière consolidée.

Un retour sur investissement inégalé

Lorsque vous sélectionnez un élément clé de votre infrastructure de sécurité, vous devez vous assurer qu'il fournira une valeur réelle qui peut être facilement démontrée à vos parties prenantes.

RAPPEL

Cortex XDR réduit le coût total de possession (TCO) de 44 %, en moyenne, par rapport aux outils traditionnels :

- En tirant parti de vos outils de sécurité existants comme capteurs pour la détection et la réponse
- En éliminant les serveurs de logs sur site grâce au déploiement cloud
- En simplifiant les opérations grâce à l'assemblage des données, au regroupement des alertes et à l'analyse des causes profondes

CORTEX® XDR™

Testé.
Revu.
Approuvé.

Testé au combat face à l'attaque SolarWind

100% des menaces bloquées et un taux de 97% de visibilité en détection lors du troisième tour d'évaluation MITRE ATT&CK

MITRE ENGENUITY

Un leader du logiciel Forrester Wave Endpoint Security en tant que service, T2 2021

FORRESTER®
WAVE LEADER 2021
Endpoint Security Software As A Service

En savoir plus sur la première plate-forme XDR du secteur

Cortex XDR:
http://go.paloaltonetworks.com/xdrpdpfr

Guide essentiel de MITRE Round 3:
http://go.paloaltonetworks.com/mitrewileyfr

Forrester ESS Wave:
http://go.paloaltonetworks.com/esswileyfr

Contactez-nous aujourd'hui:
08 05 54 25 75

paloalto® NETWORKS

Améliorez l'efficacité de vos opérations de sécurité avec la détection et la réponse étendues (XDR)

Les équipes de sécurité sont confrontées à un éventail vertigineux de menaces, des ransomwares aux attaques sans fichier, en passant par les exfiltrations de données. Toutefois, le plus gros casse-tête pour de nombreux analystes de sécurité n'est pas le nombre incessant d'attaques qui font la une des journaux, mais plutôt les tâches répétitives qu'ils doivent accomplir chaque jour pour trier les événements et tenter de réduire un arriéré sans fin d'alertes. La détection et la réponse étendues (XDR) constituent une nouvelle approche de la détection, de l'investigation et de la réponse aux menaces qui intègre et analyse des données provenant de n'importe quelle source.

À l'intérieur…

- Reconnaître les limites des approches actuelles
- Remédier à la pénurie de personnel dans le domaine de la cybersécurité
- Assurer une prévention robuste des menaces
- Obtenir une visibilité totale
- Automatiser la détection et la réponse
- Améliorer l'efficacité de la sécurité
- Protéger les ressources du réseau, des terminaux et du cloud

paloalto NETWORKS

Depuis plus de 25 ans, **Lawrence Miller** travaille dans le domaine de la technologie de l'information dans différentes industries. Il a co-écrit *« CISSP For Dummies »* et plus de 200 autres ouvrages *pour les nuls* portant sur diverses questions de sécurité et de technologie.

ISBN: 978-1-119-87903-9

pour les nuls®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.