

VARS

**OPTIMISER
LA PRÉVENTION,
LA DÉTECTION ET
LA RÉPONSE AUX
INCIDENTS AVEC
LA SURVEILLANCE
DES POINTS
DE TERMINAISON
(XDR)**

Propulsée par  **Cynet**

Voir la forêt à travers les arbres : Réduire la complexité de la cybersécurité

Augmentation des budgets $\neq$ Augmentation de la performance

Les professionnels de la sécurité sont submergés par des milliers d'alertes par jour provenant d'un nombre croissant de solutions de sécurité. Examiner différentes alertes et faire le rapprochement entre elles peut prendre des jours. Le dicton « voir la forêt à travers les arbres » est un combat permanent. Et, une fois les menaces découvertes, le temps nécessaire pour comprendre l'ampleur de l'attaque et éventuellement y remédier se mesure désormais en mois. Selon le rapport d'IBM sur le coût d'une intrusion (Data Breach Report 2019), le temps moyen pour identifier une attaque malveillante est de 230 jours, puis le temps moyen pour contenir l'attaque est de 84 jours. C'est la raison pour laquelle les incidents de cyber-intrusions continuent d'augmenter malgré l'accroissement des investissements en cybersécurité.

Les petites entreprises sont celles qui souffrent le plus

Les petites entreprises souffrent également de la complexité croissante de la cybersécurité, mais nombre d'entre elles n'ont tout simplement pas les moyens de se procurer le large éventail de solutions de sécurité nécessaires pour assurer la visibilité des menaces imminentes dans l'ensemble de leurs environnements. De plus, l'univers de la cybersécurité est devenu si complexe que les compétences requises pour maintenir et exploiter les solutions sont hors de portée des entreprises, à l'exception des plus grandes organisations internationales.

Voir la forêt

Une nouvelle catégorie d'outils de sécurité émerge et promet d'améliorer considérablement l'efficacité et l'efficience de la détection et des interventions en cas de menace. Gartner a défini une nouvelle catégorie de solutions qui agrègent et mettent en corrélation la télémétrie de plusieurs contrôles de détection, puis synthétisent et automatisent les mesures d'intervention : les solutions XDR (Extended Detection and Response).

Le défi de la protection contre les menaces : Utiliser davantage de solutions ponctuelles n'est pas la solution

Les entreprises déploient généralement plusieurs technologies de prévention et de détection pour protéger les points d'entrée et détecter les mouvements latéraux, tels que les points d'accès, les réseaux, les utilisateurs et les données. Si ces outils font généralement un excellent travail de prévention et de détection pour la grande majorité des cyberattaques, ils continuent de passer à côté des cas particuliers, c'est-à-dire des attaques sournoises qui passent à travers les mailles des solutions ponctuelles. La visibilité sur l'ensemble de l'environnement et la compréhension du contexte des données et des alertes de sécurité constituent la première étape de la résolution du problème de la complexité.

La protection des points d'accès n'est pas suffisante

De nombreuses organisations se sont tournées vers les solutions EDR (Endpoint Detection and Response), EPP (Endpoint Protection Platform) et NGAV (Next Generation Anti-Virus) pour améliorer leur protection au-delà des plateformes antivirus couramment utilisées. Les solutions EDR/EPP/NGAV se sont avérées très utiles pour prévenir et détecter de nombreuses formes d'attaques sur les points d'accès. Cependant, les cybercriminels trouvent des moyens de contourner ces approches par des attaques de plus en plus furtives. Les niveaux d'intrusions confirmées ont continué d'augmenter malgré les investissements massifs dans les ressources et les solutions de cybersécurité.

La nécessité d'une détection unifiée

Sur la base de la « durée » citée dans l'étude d'IBM mentionnée précédemment, le véritable défi en matière de sécurité consiste à découvrir le plus rapidement

possible les menaces qui ont contourné les défenses de première ligne. Parfois, un élément qui peut sembler inoffensif à une solution de sécurité devient soudain préoccupant lorsqu'il est intelligemment associé aux informations provenant d'autres solutions de sécurité. La consolidation des technologies de prévention et de détection en une seule solution permet de coordonner les signes de menace afin de dresser un tableau plus précis des attaques.

La nécessité d'une intervention automatisée

Une autre étape importante de la simplification de la sécurité réside dans l'automatisation des mesures d'intervention pour traiter les réelles menaces identifiées grâce à une meilleure visibilité et un meilleur contexte. De nos jours, les équipes de sécurité passent beaucoup de temps à examiner les fausses alertes. Les menaces confirmées nécessitent alors l'accès à de multiples contrôles par le biais de plusieurs consoles et interfaces pour comprendre toute l'ampleur de l'attaque. L'élimination des menaces exige également beaucoup trop d'efforts pour planifier et coordonner les mesures correctives à travers de multiples systèmes de sécurité. Les équipes de sécurité sont tout simplement submergées par l'exploitation et la maintenance de trop nombreuses solutions individuelles.

RÉSEAU : mouvement latéral, usurpation d'identité, exfiltration, balayage

POINT D'ACCÈS : menaces sans fichier, rançongiciels, exploits, logiciels malveillants

UTILISATEUR : ressource interne malveillante, exploits par vol d'authentifiant, compte compromis, comportement anormal

SIMULATION : leurres au niveau des ressources partagées, des fichiers, des hôtes et des utilisateurs

XDR : une nouvelle approche de détection et réponse en cas de menace

Les plateformes XDR aident les équipes de sécurité en consolidant et en rationalisant les alertes en incidents traitables et en automatisant les mesures d'investigation et d'intervention. Les principales exigences d'une plateforme XDR sont la visibilité des menaces, l'orientation des incidents et l'automatisation des interventions.

Visibilité et protection étendues des menaces

Une visibilité étendue sur les principales composantes de prévention et de détection qui fournissent la télémétrie des menaces la plus pertinente constitue la base du XDR. La combinaison des signaux provenant de ces composantes fournit le contexte nécessaire à la détection des attaques furtives (qui seraient autrement indétectables) tout en offrant une plus grande précision de détection (et donc une réduction des faux positifs). Comme les composantes incluses font partie d'une plateforme unique, les données et les informations d'alerte peuvent être facilement normalisées et combinées, ce qui peut s'avérer très difficile lorsqu'on essaie de coordonner les solutions ponctuelles de plusieurs fournisseurs.

Décider quelles composantes de prévention et de détection devraient être incluses dans la plateforme XDR est essentiel. Bien que certains suggèrent d'inclure une très large gamme d'outils de détection et de sécurité, la priorité devrait être donnée aux outils qui couvrent les principaux vecteurs d'attaque. Au minimum, les outils XDR devraient inclure des signaux provenant des composantes clés suivantes :



NGAV

Antivirus de nouvelle génération pour une prévention et une détection de base des logiciels malveillants sur les points d'accès.



EPP/EDR

Plateforme de protection des points d'accès / détection et intervention au niveau des points d'accès pour une protection, une détection et une intervention plus avancées au niveau des points d'accès.



UEBA

Analyse du comportement des utilisateurs et des entités (pour détecter les comportements anormaux des utilisateurs).



NTA

Analyse du trafic réseau pour détecter les activités malveillantes sur votre réseau.

Combinés, les signaux de ces catégories de solutions offrent la visibilité étendue requise pour détecter la grande majorité des attaques tout au long de la chaîne de la cyber attaque. D'autres données peuvent compléter cet assortiment de base, mais il a été démontré que ces composantes offrent la meilleure valeur. Par exemple, les signaux émis par les technologies de simulation, qui trompent les intrus et les incitent à révéler leur présence avant que des dommages ne soient causés, peuvent fournir des signaux très précieux à une plateforme XDR.

Il est également recommandé que le plus grand nombre possible de composantes soient incluses de façon native dans la plateforme. Cela fait en sorte que tous les signaux soient correctement normalisés et pondérés et que toutes les fonctions et politiques puissent être gérées à partir d'une seule interface. Cela élimine également le temps et les efforts nécessaires à l'intégration et à la maintenance continue d'outils provenant de plusieurs fournisseurs.

XDR : une nouvelle approche de détection et réponse en cas de menace *(suite)*



Orientation des incidents

La centralisation des signaux provenant de plusieurs outils de détection permet aux plateformes XDR de combiner les alertes et les données en incidents. Les plateformes XDR peuvent intelligemment combiner des signaux apparemment bénins provenant de plusieurs sources pour découvrir des menaces qui ne seraient pas détectées par une source unique. La plateforme peut également déterminer si les alertes doivent être combinées et transformées en incidents holistiques ou rejetées comme faux positifs.

La formation d'incidents holistiques fournit beaucoup plus de contexte aux mesures d'intervention que les alertes individuelles. Les incidents comprennent toutes les alertes et renseignements pertinents liés à une attaque afin d'accélérer les mesures d'investigation, de décision et d'intervention. Il est beaucoup plus efficace de présenter les menaces sous la forme d'incidents que de passer d'un système à un autre pour recueillir (si tout va bien) les mêmes renseignements. En ce sens, les plateformes XDR ressemblent aux outils SIEM, mais les données et les capacités sont incluses de façon native dans la plateforme XDR.



Automatisation des interventions

Après avoir formulé un incident de sécurité, avec le contexte et tous les détails associés, les plateformes XDR fournissent également des fonctions d'intervention pour rapidement et automatiquement prévenir ou minimiser les dommages. Les mesures d'intervention débutent par l'investigation, avec la possibilité de recueillir automatiquement des informations associées

à l'incident, de déterminer la cause originale et d'analyser l'impact de la menace. Par exemple, certains outils XDR peuvent dresser automatiquement la liste des processus en cours d'exécution associés à une alerte, effectuer des recherches dans le registre de Windows, recueillir des variables environnementales ou exécuter un script automatisé, entre autres.

Bien que beaucoup d'attention ait été accordée à la partie détection du XDR, les capacités d'intervention de la plateforme peuvent permettre aux organisations d'intervenir instantanément dans des situations de menaces réelles tout en minimisant la charge de travail de leurs équipes de sécurité. La plupart des outils XDR offrent un certain niveau d'interventions automatisées, comme la suppression des fichiers malveillants, la mise en quarantaine des points d'accès infectés ou l'arrêt des processus malveillants. Des plateformes XDR plus avancées étendent la remédiation à l'ensemble de l'environnement et automatisent des mesures d'intervention plus complexes qui enchaînent diverses mesures de remédiation en un seul flux qui s'exécute automatiquement lorsqu'une alerte prédéfinie est déclenchée.

De nombreuses grandes entreprises se tournent vers la technologie SOAR (Security Orchestration, Automation and Response) pour recueillir des données relatives aux menaces à partir de sources multiples, puis automatiser les interventions contre les menaces réelles à travers plusieurs contrôles de sécurité. Toutefois, la mise en œuvre réussie de la technologie SOAR est très complexe et exige un effort de gestion important, ce qui la destine uniquement aux grandes entreprises. Les plateformes XDR, qui intègrent de multiples contrôles de sécurité présents de façon native, ont la possibilité d'offrir des capacités similaires à celles de la technologie SOAR, sans les efforts importants requis par une solution SOAR complète.

Les avantages du XDR

Les plateformes XDR fournissent une plateforme holistique qui unifie plusieurs points de contrôle pour coordonner la prévention, la détection et les réponses contre les menaces. Cette approche améliore la précision de la détection tout en réduisant considérablement la complexité et les frais nécessaires à une protection complète contre les menaces.



Précision

Les plateformes XDR offrent une vision plus globale des menaces entrantes en combinant de façon native les contrôles de prévention et de détection des vecteurs d'attaque significatifs. Cette vision globale permet aux plateformes XDR d'extraire automatiquement les alertes réelles des informations non pertinentes, ainsi que de déceler des indices de menaces subtiles qui auraient pu passer inaperçus avec des outils de détection cloisonnés. La visibilité et les renseignements fournis par les plateformes XDR permettent de détecter les menaces avec une précision sans précédent.



Efficiency

Les équipes de sécurité passent beaucoup moins de temps à traquer les fausses alertes positives avec les plateformes XDR. De nombreuses menaces réelles sont automatiquement éliminées, sans intervention manuelle. Les incidents confirmés sont soit examinés et traités automatiquement, soit accompagnés du contexte et de données pertinentes permettant de raccourcir les mesures manuelles d'investigation et de réponse. Le temps nécessaire à l'intégration, la maintenance et l'exploitation de systèmes de fournisseurs disparates est éliminé. Avec l'automatisation d'une grande partie de la détection et réponses face aux menaces contre l'entreprise, le personnel de sécurité peut se concentrer sur d'autres problèmes urgents plutôt que de traquer continuellement des alertes.



Réduction des coûts

La consolidation de plusieurs produits de sécurité en une seule plateforme XDR permet de réaliser d'importantes économies, tant en termes de coûts directs provenant des fournisseurs que des coûts de soutien interne. Les petites entreprises qui ne disposent pas d'une gamme complète de contrôles de prévention et de détection bénéficient automatiquement d'une couverture étendue et approfondie des menaces grâce à l'achat d'une seule solution XDR. La réduction d'un grand volume d'alertes en un nombre réduit d'incidents significatifs et l'automatisation des réponses réduisent le temps que les équipes de sécurité consacraient autrement à ces tâches.

Cynet 360 : Une plateforme complète de XDR et d'automatisation des réponses, complétée par des services MDR 24/7

Les solutions XDR offrent une plateforme holistique qui unifie plusieurs points de contrôle pour coordonner la prévention, la détection et les réponses aux menaces. Cette approche améliore la précision de la détection tout en réduisant considérablement la complexité et les frais nécessaires à une protection complète contre les menaces.

AUTOMATISATION DES INTERVENTIONS

Investigation automatisée

Mesures correctives automatisées

Plans de match personnalisés

Incident Engine

XDR

Antivirus de nouvelle génération (NGAV)

Détection et réponse au niveau des points d'accès (EDR)

Analyse du comportement des utilisateurs et des entités (UEBA)

Analyse du trafic réseau (NTA)

Simulation

MDR 24/7

Protection autonome contre les intrusions

Rapports d'attaque

Surveillance des alertes

Intervention à distance en cas d'incident

Traque de menaces

Cynet établit la norme pour les plateformes XDR



Visibilité complète des menaces

En combinant les signaux provenant des contrôles des points d'accès, du réseau et des utilisateurs, Cynet XDR offre une visibilité complète sur l'ensemble de votre environnement. La puissance de détection obtenue en combinant de façon native les signaux et les données provenant de sources multiples ne peut tout simplement pas être égalée par des solutions de protection ponctuelle cloisonnées. Même les attaques les plus furtives sont exposées avec une précision extrême par Cynet XDR.



Prévention et détection complètes

Cynet XDR offre plusieurs technologies de prévention intégrées pour bloquer les attaques standard et avancées dans l'ensemble de votre environnement. La technologie de simulation est également intégrée à Cynet XDR pour tromper les cybercriminels qui ont réussi à pénétrer votre réseau et les inciter à s'exposer avant que des dommages ne soient causés.



Incident Engine

Le Incident Engine de Cynet automatise l'ensemble du processus d'intervention, y compris l'automatisation de l'investigation pour révéler la cause et l'impact complet de la menace identifiée, ainsi qu'un large éventail de mesures correctives sur les hôtes, les processus, les fichiers, les utilisateurs et le trafic réseau. L'automatisation complète des interventions soulage les équipes de sécurité surchargées qui ne disposent pas des ressources ou de l'expertise nécessaires pour investiguer et intervenir sur chaque alerte.



Automatisation des réponses

Cynet XDR offre des outils de réponse entièrement automatisés pour l'investigation et l'application de mesures correctives inter-environnements. Les investigations sont entièrement automatisées : elles déterminent d'abord la cause première, puis elles analysent l'ampleur et l'impact de la menace. Grâce à l'utilisation de mesures correctives préétablies et personnalisées, Cynet XDR accélère et optimise la réponse en cas d'incident, en outillant les équipes de sécurité d'un arsenal complet de mesures correctives sans jamais avoir à quitter la console Cynet.



Détection et réponses gérées (MDR)

Cynet XDR bonifie et améliore vos ressources de sécurité avec une équipe d'experts en cybersécurité de classe mondiale : CyOps. L'équipe CyOps surveille en permanence votre environnement, 24 heures sur 24 et 7 jours sur 7, pour s'assurer que toutes les attaques soient découvertes, elle fournit des investigations ad hoc sur les menaces ainsi que des analyses scientifiques, et vous guide dans toutes les étapes de mesures correctives nécessaires. De plus, les fonctions de détection et réponse gérées par CyOps sont automatiquement incluses dans la plateforme Cynet XDR, sans frais supplémentaires. Alors que d'autres fournisseurs facturent des frais exorbitants pour ce type de service, vous ne paierez pas un sou de plus avec VARS.