ExtraHop

Rise Above the Noise.

Modernisez votre sécurité, adoptez l'IDS de nouvelle génération (NG-IDS)

RÉSUMÉ

Après plus de vingt ans de résultats décevants, de nombreux responsables de la sécurité se sont résignés à ce que leurs systèmes de détection d'intrusion (IDS) se limitent à remplir les obligations de conformité. Ce n'est un secret pour personne que le recours aux signatures bimodales fait de l'IDS un outil instable et facile à contourner, générant un volume d'alertes impossible à gérer. Il est souvent difficile d'obtenir de nouveaux budgets pour la sécurité : dès lors, ne devriez-vous pas attendre de meilleurs résultats de la part de vos outils ?

Pour offrir une protection plus efficace, l'IDS de nouvelle génération (NG-IDS) s'appuie sur une analyse comportementale dans le cloud, optimisée par Machine Learning, et sur la détection de vulnérabilités critiques reposant sur des règles. Il assure la visibilité sur le trafic chiffré et latéral (est-ouest) pour étendre la détection à l'ensemble du cycle de vie des attaques.

Outre des budgets serrés, les responsables informatiques sont également confrontés à une pénurie d'experts en sécurité. Une solution NG-IDS offre aux analystes un outil unique qui intègre la détection, l'investigation et la réponse, optimisant ainsi la gestion des processus.

Dans ce livre blanc, nous examinerons comment vous pouvez moderniser votre dispositif de détection des intrusions pour renforcer votre sécurité et élargir votre couverture de conformité. Nous aborderons en détail les points suivants :

- Le déclin de l'efficacité des systèmes IDS au fil du temps et les failles de sécurité qui en découlent
- La défense en profondeur contre tous les types d'attaques qu'offre le NG-IDS
- Les stratégies permettant de combler les failles liées au chiffrement et de corriger les violations de conformité de l'environnement cloud, tout en renforçant la sécurité

SOMMAIRE

OBSOLESCENCE DES SYSTÈMES IDS

Les systèmes IDS ont gagné en popularité dans les années 90 suite à l'apparition de SNORT, Bro et ISS RealSecure. Leur utilisation a explosé lorsque des frameworks de sécurité tels que la liste SANS 20 Critical Security Controls, ou des normes telles que PCI DSS, ont spécifiquement recommandé l'implémentation d'un système IDS. Pourtant, même après un quart de siècle d'innovation et d'adoption de cette technologie dans de nombreuses entreprises, les mêmes défis persistent.

Si l'on se réfère à la norme NIST 800-94 de 2007, la définition de l'IDS ressemble davantage à une liste de souhaits qu'à une description de ses fonctionnalités réelles, même aujourd'hui.

La publication du NIST décrivait les problèmes liés aux systèmes IDS de l'époque :

- Précision de détection : « taux élevés de faux positifs et de faux négatifs » (pp. 4 à 10)
- Configuration : « d'importants efforts de personnalisation et d'optimisation de la configuration sont nécessaires* » (pp. 4 à 11)
- Angles morts : « ne peuvent pas détecter les attaques au sein du trafic réseau chiffré » (pp. 4 à 11)
- Limites de performances : « incapables d'effectuer une analyse complète en cas de charges élevées » (pp. 4 à 12)

**Dans de nombreux cas, les « efforts de personnalisation et d'optimisation de la configuration » entraînent l'abandon de signatures, si bien que les signaux réels disparaissent en même temps que les données parasites.*

> “Certains clients, souvent avec raison, voient cette technologie comme une source continue d'alertes, où les informations pertinentes pour la sécurité sont présentes mais noyées dans la masse des messages générés.
>
> **2019 Market Guide for Intrusion Detection and Prevention Systems, Craig Larson, Gartner**

Même dans la perspective monolithique qui a inspiré la conception de l'IDS, à savoir un environnement défini par un périmètre fermé, ces défauts limitaient la convivialité et l'efficacité. Si l'on ajoute à cela l'évolution profonde des réseaux d'entreprise actuels, il semble peu judicieux de poursuivre dans la voie des IDS traditionnels.

La profonde mutation du périmètre

Le mot *périmètre* évoque des images de bases militaires bordées de hautes clôtures en fil de fer, ou du moins des lignes pleines tracées sur la carte d'un réseau. Aucun de ces concepts ne constitue une représentation réaliste des réseaux actuels, car il n'est plus aussi simple de séparer les actifs de confiance des actifs non approuvés. Le périmètre réseau actuel est poreux, élastique et abstrait. D'innombrables équipements et workloads non gérés le traversent sans que l'on ait une vue sur leur niveau de sécurité.

Défis liés au périmètre :

- Équipements personnels (BYOD)
- Collaborateurs distants
- Internet des objets (IoT)
- Services et actifs de tiers
- Toutes les fonctions informatiques fournies sous forme de service (XaaS)

L'interdiction de ces outils de productivité n'est plus envisageable, car ils font partie intégrante de la chaîne de création de valeur. Cependant, des compromissions de grande ampleur telles que SolarWinds SUNBURST nous montrent que la confiance que nous leur accordons peut les transformer en vecteurs d'attaque. Ils peuvent être infectés tandis qu'ils se trouvent hors du champ d'action du dispositif de sécurité, ou par le biais de canaux de communication alternatifs tels que les VPN tiers, les canaux secondaires mobiles ou les réseaux de partenaires réputés de confiance. Toutes ces méthodes échappent aux systèmes IDS, tournés vers l'extérieur.

Les menaces telles que les attaques perpétrées par des utilisateurs internes obligent les responsables de la sécurité à étendre les mesures de détection à l'intérieur du réseau, afin d'empêcher de graves dommages.

Le chiffrement et la tunnellisation dans l'angle mort de la sécurité

Dans les années 90, la majorité du trafic réseau circulait en clair. À l'époque, le chiffrement nécessitait un matériel coûteux et des algorithmes complexes à intégrer, et on le réservait à la protection d'informations secrètes ou confidentielles. Aujourd'hui, nous chiffrons à peu près tout ; c'est par exemple le cas de 95 % du trafic Google. En conséquence, les outils de sécurité traditionnels ne sont pas en mesure de faire la distinction entre trafic important, banal ou dangereux qui traverse le périmètre ou se déplace latéralement dans les datacenters et/ou les infrastructures cloud.

Certains éditeurs de solutions IDS ont ajouté des fonctionnalités de déchiffrement-inspection-chiffrement de type intercepteur (man-in-the-middle) à leur offre IDS. Malheureusement, ces fonctionnalités se sont révélées difficiles à mettre en œuvre et augmentent les risques en raison de la faiblesse du transcodage cryptographique, comme le souligne un avis de la NSA.

Même les éléments en clair du trafic réseau présentent de nouveaux défis pour les systèmes IDS du fait de l'utilisation quotidienne de la tunnellisation. Selon l'implémentation de l'IDS, ces workloads sont inobservables ou nécessitent un prétraitement, ajoutant une charge importante à un moteur d'inspection déjà mis à rude épreuve.

Protocoles de tunnellisation courants :
ICMP, IP/IP, GRE, VPN, SSH, GTP, tout le trafic HTTP

Les nouvelles stratégies d'attaque

Les systèmes IDS reposent sur un principe de prévention des incidents consistant à chercher les correspondances entre les signatures de trafic et les vulnérabilités logicielles répertoriées dans des référentiels de sécurité (comme la NVD). À cet égard, même s'il génère un volume d'alertes élevé et résiste mal au contournement, l'IDS offre des performantes satisfaisantes — pour autant que les attaquants respectent les règles.

Lors de l'émergence de la technologie IDS, les vulnérabilités logicielles constituaient la principale menace, et représentent d'ailleurs toujours un problème de sécurité important. Cependant, les attaquants préfèrent désormais d'autres stratégies, estimant qu'il est plus efficace d'utiliser l'ingénierie sociale pour manipuler les utilisateurs, d'acheter des identifiants volés ou d'exploiter des erreurs humaines de configuration que de se plonger dans du code assembleur pour développer acquérir de coûteuses exploitations de failles Zero Day.

Principales techniques d'attaque initiales

#1 Phishing
#2 Utilisation d'identifiants volés
#3 Erreur de destinataire
#4 Erreur de configuration
#5 Abus de privilèges (intentionnel ou involontaire par un utilisateur interne)
#6 Collecte de mots de passe

Source : Verizon 2020 Data Breach and Incident Response (DBIR)

La tactique cybercriminelle pour laquelle les systèmes IDS sont conçus, à savoir l'exploitation des vulnérabilités, arrive en neuvième position. Le rapport DBIR souligne que cette stratégie d'attaque a connu son apogée en 2017, avec 5 % des compromissions étudiées, puis a progressivement baissé pour se stabiliser à 2,5 %.

L'IDS PEU EFFICACE EN TERMES DE DÉFENSE EN PROFONDEUR

Dans la mesure où les attaquants privilégient la faiblesse humaine à l'exploitation des vulnérabilités logicielles, une question existentielle se pose : l'impact de l'IDS sur votre dispositif de sécurité justifie-t-il la charge administrative qu'il engendre ?

L'importance de la défense en profondeur

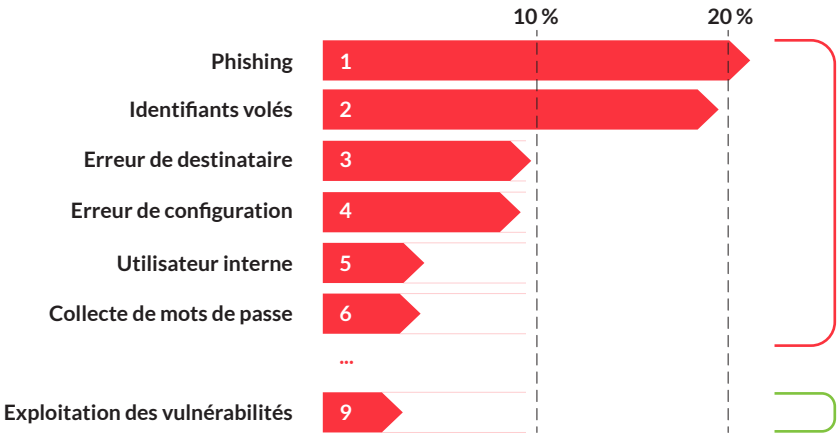
La défense en profondeur est un principe de sécurité éprouvé qui favorise les mesures défensives multiniveaux et décourage une dépendance excessive vis-à-vis d'une seule ligne de défense prétendument « impénétrable ». En principe, c'est bien ce que les systèmes IDS tentent d'offrir : une détection en profondeur. Les systèmes IDS résident derrière les pare-feux de la zone démilitarisée (DMZ) et entrent en action après que les outils de prévention tels que les filtres de messagerie, les contrôles d'accès et le pare-feu WAF ont rempli leur tâche. Le système IDS applique alors l'inspection approfondie des paquets pour réexaminer le trafic, à la recherche d'infractions aux stratégies et de signaux d'exploitation d'une faille.

Lorsqu'une attaque cherche à exploiter une vulnérabilité logicielle connue sur une machine exposée à l'accès public, le système IDS a de bonnes chances de créer une alerte. Tant que l'entreprise suit des pratiques raisonnables en matière de sécurité, vos actifs les plus précieux tels que les contrôleurs de domaine, les bases de données clients et les données de propriété intellectuelle, sont protégés contre les attaques frontales. Malheureusement, toutes les attaques n'exploitent pas les vulnérabilités connues, comme nous l'explique la section suivante.

Les grandes manœuvres des attaquants

Les attaquants recherchent plutôt des points d'accès faciles leur permettant de traverser ou de contourner le périmètre pour établir une tête de pont. À partir de là, ils peuvent utiliser des outils et des méthodes disponibles sur l'hôte pour effectuer une reconnaissance, élever leurs privilèges ou désactiver la journalisation afin d'échapper aux solutions EDR et SIEM. Une fois établi, le pirate se déplace latéralement à l'intérieur du réseau pour se tourner vers des actifs plus précieux à voler, bloquer ou détruire — que ses motivations soient le profit, la vengeance ou l'espionnage.
Les systèmes IDS traditionnels ne peuvent pas distinguer ces activités de celles des utilisateurs légitimes. En effet, la seule différence réside dans l'intention.

Verizon DBIR 2020



Le rapport *DBIR* de Verizon et d'autres rapports rétrospectifs sur la sécurité (par exemple, le rapport *Digital Defense Report 2020* de Microsoft) mettent en lumière les tactiques actuellement utilisées par les attaquants pour s'implanter à l'intérieur du périmètre.

Selon le rapport *DBIR* de Verizon, seuls 2,5 % des quelque 3 000 compromissions étudiées avaient pour origine l'exploitation d'une vulnérabilité identifiable par IDS. Qu'en est-il des 97,5 % d'attaques qui échappent à vos dispositifs de prévention des attaques ? Malheureusement, les systèmes IDS axés sur l'exploitation des vulnérabilités sont hors du coup lorsqu'il s'agit d'assurer une protection en profondeur contre les tactiques les plus répandues.

L'IDS DE NOUVELLE GÉNÉRATION (NG-IDS)

Comme les IDS traditionnels, les IDS de nouvelle génération (NG-IDS) reposent sur le principe que la sécurité réseau est invisible et inévitable pour les attaquants. S'appuyant sur la technologie NDR, les NG-IDS ajoutent des fonctions d'analyse assistée par Machine Learning et la détection de l'exploitation des CVE (Common Vulnerabilities and Exposures) basée sur des règles. Gartner considère la technologie NDR comme un élément essentiel de la triade de visibilité du SOC. Anton Chuvakin, expert en sécurité chez Gartner, explique que cette triade « cherche à réduire fortement la probabilité que l'attaquant opère sur votre réseau suffisamment longtemps pour atteindre ses objectifs. »

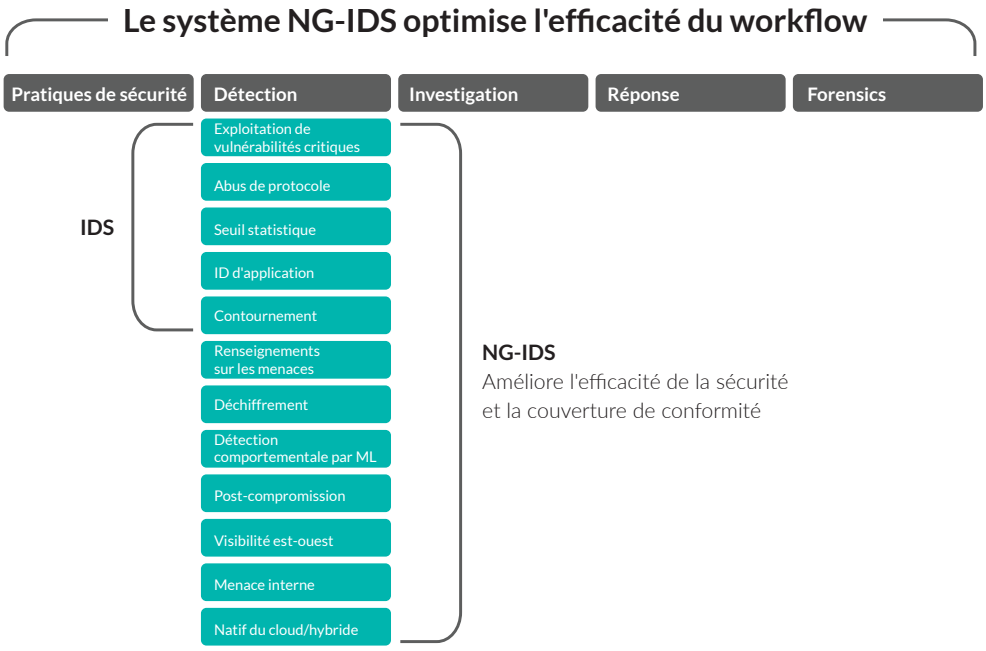
Les systèmes NG-IDS atteignent les objectifs de la triade en ajoutant une couche de détection réseau au point d'intrusion et dans le corridor est-ouest pour les situations où un attaquant atteint une tête de pont en tirant parti de défenses poreuses ou au moyen de techniques avancées.

Tout aussi important, les NG-IDS améliorent l'efficacité des analystes en intégrant la détection, l'investigation et la réponse au sein d'un outil unique offrant un workflow de sécurité optimisé.

Les NG-IDS comblent les lacunes des IDS traditionnels :

- Détection des déplacements de l'attaquant tout au long de la chaîne d'attaque avant qu'il ne cause de réels dégâts
- Correction des violations de conformité causées par les angles morts cryptographiques, sans affaiblir le chiffrement
- Mise en conformité des services cloud sans entraver les activités
- Gain de temps et d'argent grâce à un outil unique pour la détection, l'investigation et la réponse

Fonctionnalités des systèmes IDS et NG-IDS



Détection des menaces tout au long de la chaîne d'attaque

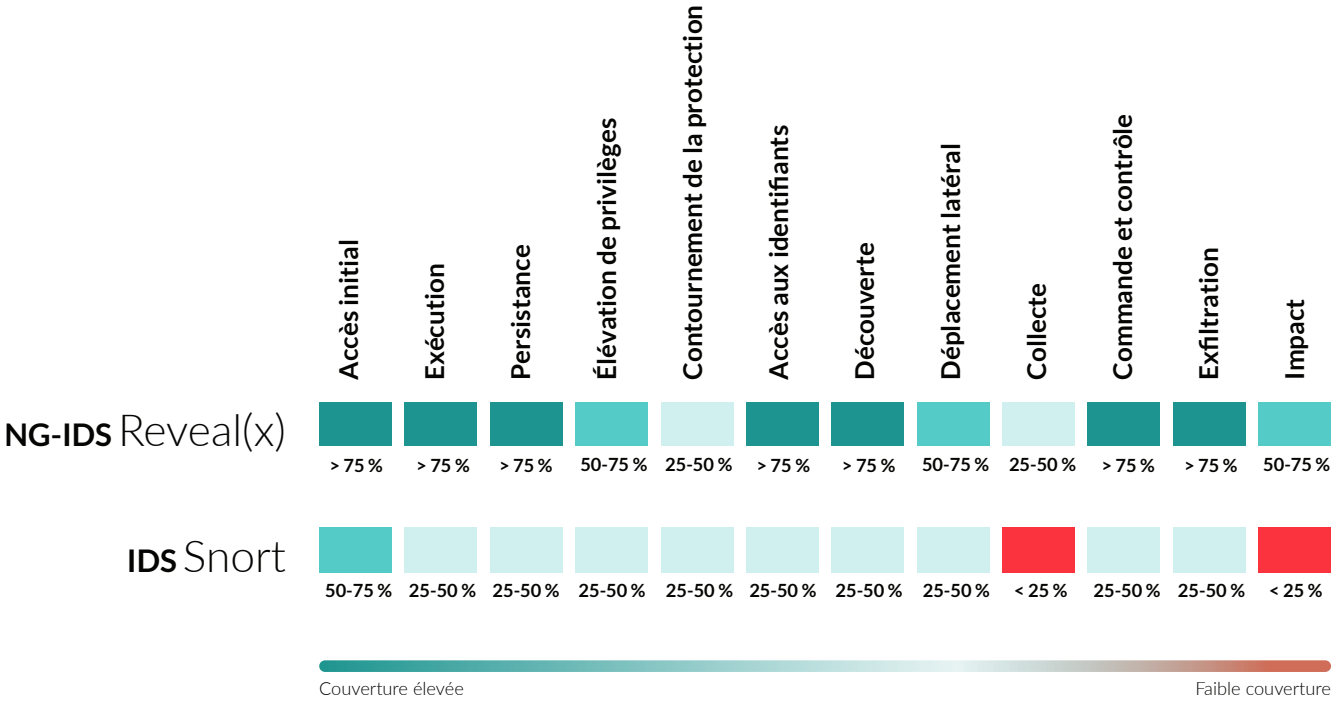
Les cybercriminels motivés sont déterminés et trouveront inévitablement une faiblesse aux frontières du réseau. C'est ce que l'on appelle souvent le dilemme du défenseur : les attaquants disposent d'une infinité de choix et de tentatives pour arriver à leurs fins, tandis que les défenseurs n'ont aucun droit à l'erreur. La protection parfaite du périmètre réseau est une chimère, et l'agresseur a l'avantage.

Vous ne pourrez sans doute pas bloquer toutes les tentatives d'intrusion au niveau du périmètre, mais les stratégies en plusieurs phases des attaquants (intrusion suivie d'une recherche de la cible réelle) vous permettent de neutraliser les menaces avant que les dommages réels ne surviennent, du moins si vous êtes aux aguets à l'intérieur du réseau. Les analyses optimisées par Machine Learning et la visibilité est-ouest offertes par les NG-IDS renversent les rôles, en obligeant les attaquants à rester continuellement sur leurs gardes une fois dans l'environnement pour éviter la détection. Un faux pas inévitable, comme un téléphone IP tentant de synchroniser l'annuaire d'un contrôleur de domaine, ou des pics de transferts de données via le DNS, et la campagne du cybercriminel est terminée.

Par exemple, la détection par FireEye d'un intrus se faisant passer pour le deuxième smartphone d'un collaborateur a mis fin à une infiltration sophistiquée, commanditée par un État, qui durait depuis environ un an. Ce seul faux pas a mis fin à la progression de l'attaquant et a alerté les 18 000 autres entreprises infectées qui avaient téléchargé la mise à jour de Solarwinds Orion.

Les fonctionnalités de détection post-compromission ajoutent une couche critique de défense en profondeur contre les 97,5 % de tactiques de compromission initiales décrites dans le rapport *DBIR* de Verizon, contre lesquelles les IDS traditionnels sont inefficaces.

Le framework MITRE ATT&CK énumère les options dont dispose l'attaquant une fois la compromission effectuée. Le système NG-IDS mesure l'efficacité de la sécurité en prenant ce framework comme point de référence, et non le nombre de signatures.

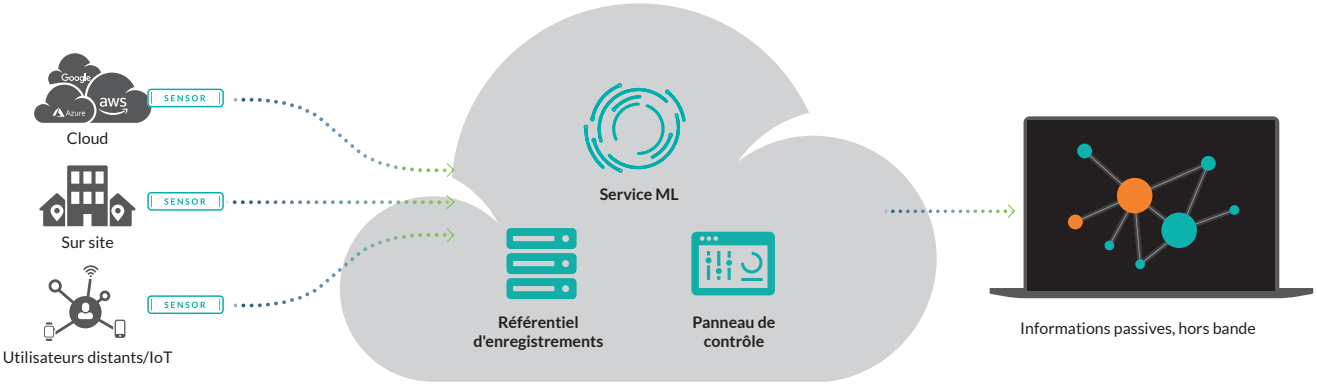


Efficacité contre les techniques de compromission du réseau — Comparaison basée sur le framework MITRE ATT&CK

Mise en conformité et renforcement de la sécurité

La conformité réglementaire constitue la principale motivation de nombreuses entreprises qui maintiennent ou étendent leurs dispositifs de détection des intrusions. Pourtant, la transformation numérique, les initiatives cloud et les attaques dissimulées au sein de canaux chiffrés augmentent le risque de violations de conformité, que les systèmes IDS ne permettent pas de résoudre facilement.

Les systèmes NG-IDS assurent le déchiffrement SSL/TLS hors bande pour vous offrir une analyse approfondie et pertinente du trafic réseau sans risque pour les données sensibles ou régies par diverses réglementations telles que le RGPD, la loi HIPAA, la norme PCI, etc.



Sécurité d'entreprise hybride native du cloud

La sécurité ne peut pas ralentir les activités. Les systèmes NG-IDS assurent une sécurité unifiée sans agent pour les environnements sur site et cloud, sans points de friction pour le pipeline d'innovation DevOps.

Un outil unique pour la détection, l'investigation et la réponse

De nombreux administrateurs IT considèrent la technologie IDS comme un générateur d'alertes. Malheureusement, l'IDS se borne à émettre des alertes, laissant aux analystes déjà débordés le soin d'en rechercher la cause à l'aide d'autres outils d'investigation et, dans certains cas, d'interoger un référentiel PCAP supplémentaire afin d'y trouver des indices.

Les systèmes NG-IDS améliorent l'efficacité de la sécurité et offrent un outil unique qui évalue les pratiques en matière de sécurité avant les attaques, puis assure la détection, l'investigation et la réponse pour permettre aux analystes d'être plus efficaces. Ceux-ci peuvent passer rapidement de la détection, à l'investigation et à la réponse à l'aide de workflows optimisés. Ils ont en outre accès à la demande aux métadonnées, voire aux paquets bruts, pendant au moins 90 jours.
Tout cela à l'aide d'un seul outil.

Les systèmes NG-IDS ne se contentent pas de générer des alertes :

- Ils offrent une visibilité sur les pratiques de sécurité afin de réduire les surfaces d'attaque potentielles.
- Ils contextualisent l'information en explicitant les événements survenus avant et après l'incident.
- Ils montrent les relations entre l'hôte compromis et les autres systèmes.
- Ils identifient et classent automatiquement les systèmes critiques.
- Ils stockent les métadonnées pour une investigation rétroactive, même si aucune alerte n'a été déclenchée.

CONCLUSION

Il est habituel d'utiliser l'IDS pour répondre aux exigences de conformité en matière de conformité de la sécurité réseau, malgré des résultats opérationnels décevants. Cependant, dans la mesure où les pare-feux de nouvelle génération (NGFW) exécutent désormais des fonctions IDS au niveau du périmètre, il paraît judicieux de réorienter les investissements vers des couches plus profondes du réseau et d'implémenter un système NG-IDS. Reposant sur les principes fondamentaux de la détection des intrusions, ExtraHop Reveal(x) est une solution NG-IDS qui détecte également les menaces se déplaçant latéralement, neutralise les intrus après la compromission et corrige les violations de conformité que causent les projets cloud et les angles morts liés au chiffrement.

Passez à l'offensive et optimisez votre budget IDS grâce à Reveal(x) et à sa technologie cloud optimisée par Machine Learning, qui simplifie l'investigation et la réponse.

À PROPOS D'EXTRAHOP

ExtraHop s'est donné pour mission d'offrir aux équipes de sécurité les outils nécessaires pour neutraliser les menaces actives et bloquer les compromissions. Notre plateforme Reveal(x) 360, solution cloud optimisée par l'intelligence artificielle, déchiffre et analyse tout le trafic cloud et réseau, en temps réel et en toute transparence. Objectif : éliminer les angles morts et détecter les menaces qui échappent aux autres outils. Des modèles de Machine Learning sophistiqués sont appliqués à plusieurs pétaoctets de données télémétriques collectées en continu, afin d'aider les clients d'ExtraHop à identifier les comportements suspects et à sécuriser leur environnement — protégeant plus de 15 millions d'actifs IT, 2 millions de systèmes de point de vente et 50 millions de dossiers médicaux. L'un des leaders du marché NDR, ExtraHop a remporté 30 récompenses décernées récemment par le secteur, notamment les prix Forbes AI 50, CybercrimeRansomware 25 et SC Media Security Innovator.

ExtraHop

info@extrahop.com
www.extrahop.com

Neutralisez les compromissions 84 % plus rapidement. **Découvrez notre solution sur www.extrahop.com/freetrial**