Secureworks®

LIVRE BLANC

XDR VS SIEM :
UN GUIDE POUR LES DÉCIDEURS DE LA CYBERSÉCURITÉ

Alors que les menaces s'intensifient et que les équipes SecOps sont appelées à défendre des environnements numériques qui ne cessent de croître en taille et en complexité, avec un périmètre de défense qui a pratiquement disparu, les fournisseurs de cybersécurité répondent avec une nouvelle génération de solutions logicielles et de services.

En particulier en 2022, l'industrie voit l'émergence d'une nouvelle classe de solutions appelée Extended Detection and Response, communément appelée XDR.

Étant donné que XDR agrège des données de sécurité provenant de l'ensemble de l'entreprise, certains responsables cybersécurité pourraient penser qu'il s'agit simplement d'une version évoluée de la Gestion des Informations et des Evénements de Sécurité (SIEM). Mais la réalité est que XDR va bien au-delà des caractéristiques d'un SIEM traditionnel, offrant une valeur tangible qui améliore la visibilité de la sécurité, les capacités d'enquête opérationnelle et collaborative, et les actions de réponse au sein de l'entreprise.

Les équipes SecOps étant confrontées à des pressions croissantes en termes de charge de travail et d'alertes de faible qualité, associées à une pénurie préoccupante de talents SecOps disponibles pour répondre à ces demandes, les responsables cybersécurité devraient examiner et comprendre les différences non négligeables entre XDR et SIEM.

Ce guide fournit un aperçu de ces différences.

QU'EST-CE QU'UN SIEM ?

Bien que l'acronyme "SIEM" ait été créé pour la première fois par Gartner en 2005[1], les fondamentaux fonctionnels de SIEM existent depuis encore plus longtemps. Dès les années 1990, des organisations prévoyantes ont réalisé qu'elles devaient consolider leurs journaux de sécurité disparates en un seul système pour faciliter l'analyse et répondre aux exigences de conformité.

[1]Gartner Research: Innovation Insight for Extended Detection and Response

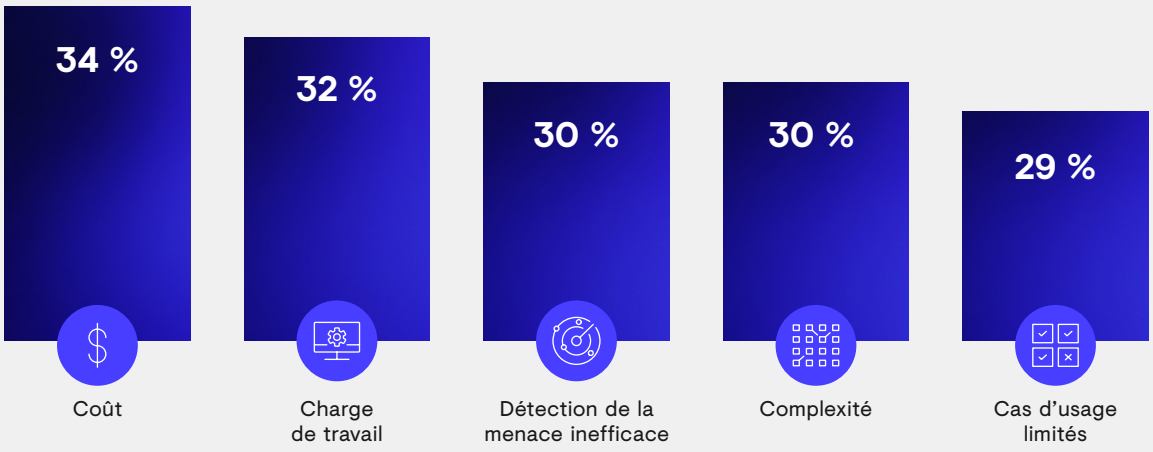
Toutes les solutions SIEM ne sont pas équivalentes. Cependant, elles partagent généralement les caractéristiques suivantes :

- **Agrégation de données de journalisation** qui fournit aux équipes SecOps une source consolidée de télémétrie provenant de toute l'entreprise.
- **Rétention centralisée des données** qui maintient un historique à des fins de conformité et d'enquête avec une période de rétention commune, tout en permettant à des journaux dispersés de vider leur cache aussi fréquemment que nécessaire.
- **Requêtage des données** à travers les systèmes qui aide les équipes SecOps à enquêter sur les journaux et les alertes de sécurité afin de rechercher des menaces actives non découvertes dans l'environnement.
- **Les tableaux de bord et les rapports** permettent aux SecOps de surveiller leurs environnements à la demande, de se conformer aux exigences d'audit et de fournir aux tiers tels que les MSSP les données dont ils ont besoin.

Certaines solutions SIEM offrent également des outils d'analyse et de manipulation des données qui aident les équipes SecOps à corréler les événements connexes, à appliquer des filtres qui améliorent le rapport signal / bruit, et à supporter les enquêtes forensiques.

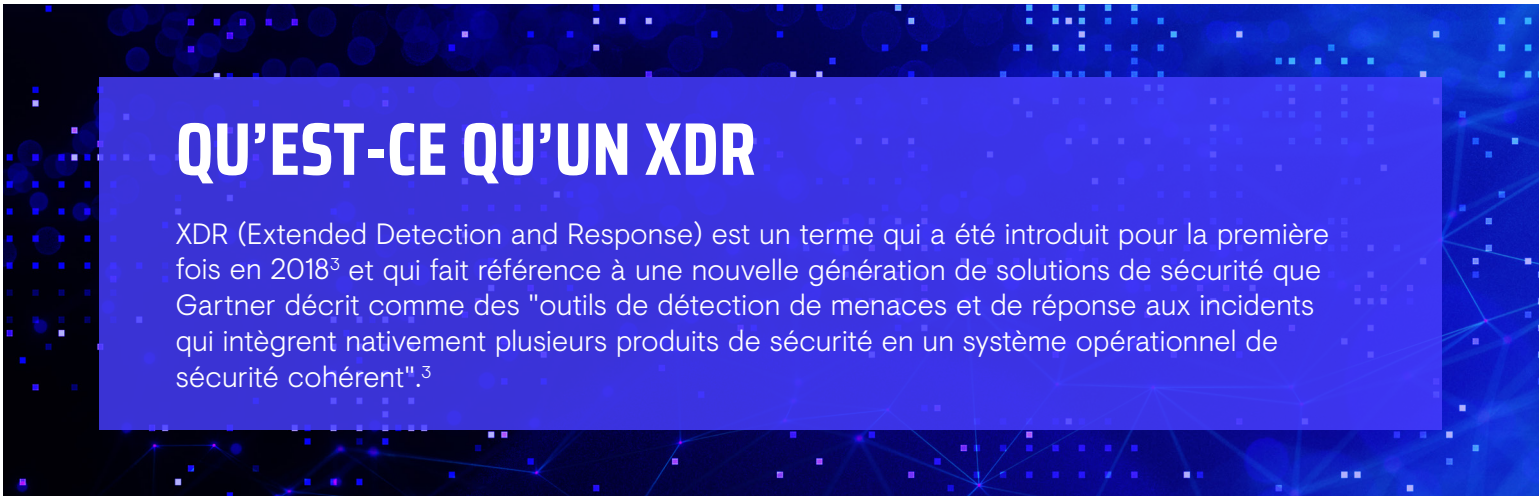
Ce que la technologie SIEM n'a historiquement jamais fourni, c'est une capacité intégrée à corréler les données d'alerte/télémétrie actuelles d'une organisation avec vis-à-vis lde comportements connus des acteurs de la menace, basés sur l'intelligence du renseignement actualisée sur les menaces. Sans cette intégration native de l'intelligence sur la menace, la technologie SIEM conventionnelle ne sait pas guider, et manque également de flux de travail de sécurité intégrés pour guider le personnel SecOps dans l'identification, la réponse et la remédiation des menaces actives.

LES POINTS LES PLUS DIFFICILES POUR LES ORGANISATIONS EN MATIÈRE DE SIEM, SELON UNE ENQUÊTE DE ESG[2]



[2]ESG: The Impact of XDR in the Modern SOC

Une gestion de bout en bout de la kill-chain est essentielle pour une atténuation efficace des risques, mais cette capacité est diluée, voire inefficace et peut être perdue au sein d'une organisation qui ne compte que sur un SIEM pour faire office de portail unique. Aucune combinaison d'outils de sécurité ne peut offrir une couverture à 100% contre un incident de cyber sécurité. Nos adversaires peuvent générer d'énormes dégâts s'ils arrivent à se maintenir clandestinement pendant longtemps au sein d'un eco-système IT; un SIEM est un avantage pour eux car il laisse les capacités de détection complexe à la charge du personnel SecOps , certes compétent mais compétences de leurs équipes SecOps, qui sont le plus souvent surchargées. Quelque part, la bonne recette pour un désastre.



QU'EST-CE QU'UN XDR

XDR (Extended Detection and Response) est un terme qui a été introduit pour la première fois en 2018[3] et qui fait référence à une nouvelle génération de solutions de sécurité que Gartner décrit comme des "outils de détection de menaces et de réponse aux incidents qui intègrent nativement plusieurs produits de sécurité en un système opérationnel de sécurité cohérent".[3]

Les caractéristiques distinctives des solutions de classe XDR comprennent :

- **L'agrégation de données de télémétrie sélective** sur les endpoints, serveurs, réseaux, clouds, e-mails et applications. Cette agrégation de données doit également toucher les pares-feux, la détection et la prévention des intrusions et autres contrôles de sécurité au sein de l'environnement.
- **L'analyse et la corrélation des données par rapport aux renseignements sur les menaces** qui exposent et identifient les activités potentiellement malveillantes dans l'environnement en fonction d'indices comportementaux.
- **L'utilisation continue de machine learning et d'intelligence humaine** pour améliorer en permanence la sensibilité et l'exactitude de la détection des menaces.
- **Le support natif pour une investigation et une réponse aux incidents** efficaces, collaborative, avec des workflows intégrés d'investigation de sécurité.
- **L'accès intégré à des directives spécifiques aux menaces** pour la remédiation, la restauration et l'amélioration des cyberdéfenses préventives.
- **L'automatisation complète et/ou l'assistance automatisée** pour les actions correctives, ainsi que les "playbooks" de remédiations spécifiques aux menaces basés sur les recherches et les meilleures pratiques actuelles.

[3]Forrester: XDR Defined: Giving Meaning to Extended Detection and Response

XDR améliore ainsi la solution EDR (Détection et réponse sur les points d'extrémité) traditionnelle de deux manières critiques :

1. Elle va au-delà de la télémétrie des points d'extrémité équipés d'un EDR pour inclure des systèmes tels que le réseau, le cloud, les système de gestion d'identités et de SSO, les passerelles e-mails et d'autres systèmes qui jusqu'à présent ne pouvaient être agrégés que via SIEM.
2. Elle complète la prévention contre les logiciels malveillants et la lutte contre les menaces connues, typiquement le module antivirus de l'EDR, avec une détection proactive et une réponse accélérée contre les menaces avancées, évolutives voire inconnues - y compris et surtout celles qui ont contourné les défenses classiques (NGFW, NGAV) du périmètre ou du poste de travail au sein d'une organisation.

XDR vs. SIEM

Munies des descriptions ci-dessus, nous pouvons observer que SIEM et XDR ont des fonctions distinctes et sont adaptés à des objectifs très différents. Étant donné l'émergence du concept de XDR, il est clair que le SIEM a atteint certaines limites et que, même s'il subsiste des situations spécifiques où il devrait être utilisé, il ne constitue pas LA solution de choix, bien au contraire. Le tableau ci-dessous offre une comparaison opportune :

Description	XDR	SIEM
Plateforme ouverte pour agréger la télémétrie et les données de sécurité pertinentes provenant de sources diverses	✓	Varie
Stockage de journaux complexes ou cas d'usage tels que gouvernance, gestion des risques et de conformité (GRC)	✗	✓
Rétention à long terme des données pour la conformité et l'audit	Varie	✓
Corrèle les indicateurs comportementaux avec de l'intelligence sur la menace pour détecter et identifier les menaces avancées	✓	✗
Utilise à la fois et continuellement du machine learning et l'intelligence humaine pour améliorer et mettre à jour en permanence la détection et l'identification de menaces	✓	✗
Facilite les enquêtes collaboratives afin que les équipes SecOps et leurs partenaires externes puissent accélérer les processus urgents de kill-chain et rémédiation	✓	✗
Aide les équipes SecOps à répondre et remédier aux problèmes de sécurité plus rapidement et de manière plus efficace grâce à des actions automatisées et à des playbooks éprouvés	✓	Add-on Requis
Licensing	Assets couverts	Volume de données

Sur la base de cette comparaison, les organisations qui ont investi considérablement dans un SIEM peuvent toujours choisir de l'utiliser à des fins de conformité et d'audit - en particulier dans des secteurs tels que la finance et la santé qui font l'objet d'un examen réglementaire important en matière de protection des données.

En revanche, XDR est la plateforme la plus pertinente pour atténuer les risques de cybersécurité dans une nouvelle ère où la surface d'attaque s'est élargie et les périmètres de sécurité réduits voire absents, en particulier pour les organisations qui ont des ressources internes SecOps limitées et se doivent donc d'exploiter de manière forte des supports externes d'intelligence sur la menace et de services de soutien en cybersécurité (MDR).

Pour les organisations qui n'ont pas investi de manière significative dans un SIEM - ou qui sont prêtes à abandonner ces investissements dans le cadre de leur stratégie de réalignement / optimisation de l'allocation de leurs budgets de cybersécurité - XDR peut potentiellement servir à la fois de plateforme opérationnelle centrale pour SecOps et de référentiel de données central pour la conformité / les rapports d'audit sans l'investissement continu de la maintenance d'une plateforme SIEM héritée.

Trois autres points sont à noter concernant toute comparaison entre XDR et SIEM :

1. En raison de sa tarification généralement basée sur le volume de données, le SIEM sanctionne paradoxalement les bonnes pratiques de cybersécurité, comme la défense en profondeur, avec une pénalité financière. Cette pénalité est susceptible de croître considérablement dans les années à venir à mesure que nos environnements deviennent plus vastes et plus diversifiés - et que nous capturons de plus en plus de données. Il y a également des coûts d'implémentation élevés, un réglage et une maintenance continus requis, ainsi que des coûts de licence supplémentaire. Les décideurs technologiques doivent prendre en compte ces coûts de licence à long terme lorsqu'ils déterminent la meilleure façon d'allouer leur budget pour obtenir des résultats optimaux.
2. Alors que nous considérons la cybersécurité comme quelque chose que nous pratiquons principalement au sein de nos propres organisations, l'inverse est vrai également. La cybersécurité est intrinsèquement une activité collective. Nous rendons chaque autre organisation que nous touchons plus vulnérable lorsque nous échouons - et nous protégeons chaque autre organisation que nous touchons lorsque nous réussissons. L'intelligence des menaces est également une entreprise intrinsèquement collective, car la qualité de cette intelligence dépend fortement de la mesure dans laquelle nous partageons ce que nous savons.
3. D'un point de vue global en matière de sécurité, le SIEM représente un écosystème totalement différent de celui d'un XDR. Les SIEM peuvent avoir pour effet d'être isolés, tels une île, avec de nombreux problèmes de sécurité existant juste à l'extérieur de la sphère d'influence des SIEM. En revanche, XDR agit comme un système interconnecté, avec l'intelligence sur la menace bénéficiant à chaque angle de l'environnement, sans introduire de risques partagés ni de coûts supplémentaires.

XDR, par sa nature même, facilite cette défense collective en tirant parti de notre intelligence des menaces partagées et en permettant une enquête et une réponse véritablement collaboratives. XDR facilite également la défense collective en réduisant l'exposition de chaque organisation touchée par les organisations individuelles qui l'utilisent.

En revanche, un SIEM est par nature auto-suffisant et privé, conçu pour la gestion des journaux et non pour l'investigation et la réponse en matière de sécurité. Un SIEM contribue donc beaucoup moins à notre défense collective.

POURQUOI CELA EST DESORMAIS IMPORTANT

Une compréhension claire de la différence entre XDR et SIEM est nécessaire non seulement en raison de toute l'attention que XDR reçoit actuellement sur le marché, mais également en raison de la nouvelle réalité à laquelle sont confrontées les organisations, notamment :

- Escalade continue de l'**intensité et de la sophistication des cyberattaques**
- L'expansion continue de la taille et **de la complexité des environnements** que les équipes SecOps sont chargées de protéger - en particulier en ce qui concerne l'utilisation de plusieurs clouds IaaS et d'un nombre croissant d'applications SaaS (pour lesquelles, qu'on le veuille ou non, les équipes de SecOps restent finalement responsables)
- Une pénurie chronique de talents professionnels en cybersécurité, résultant en des **périodes d'emploi plus courtes et un roulement continu**
- La pression associée à la **nécessité de conserver en permanence le personnel SecOps** déjà en place (en créant une expérience de travail positive, en évitant l'épuisement professionnel, etc.)
- La pression continue d'assurer des défenses solides pour maintenir les données et les systèmes sécurisés va **au-delà d'une simple case de conformité à cocher**
- Une utilisation accrue de l'**accès distant** comme conséquence à long terme de la pandémie et des politiques de travail à distance.
- **Des demandes accrues des cadres dirigeants** qui sont plus préoccupés que jamais par les conséquences négatives des violations sur les opérations commerciales, les relations avec les clients, la valeur de la marque, le prix des actions, etc., mais qui ne signeront absolument pas un chèque en blanc pour les opérations de sécurité des systèmes d'information (SecOps)

La disparité entre les besoins en matière de cybersécurité et les ressources en cybersécurité a atteint un point de basculement au-delà duquel le statu quo n'est plus suffisant

Les responsables cybersécurité vont donc devoir prendre des décisions difficiles. Une compréhension claire de ce que XDR et SIEM peuvent et ne peuvent pas faire, ainsi que de leur impact sur l'efficacité des ressources des équipes SecOps, est essentielle pour quiconque doit prendre la bonne décision pour le bien-être à long terme de l'organisation qu'il sert.

« Alors que la technologie de gestion des informations et des événements de sécurité (SIEM) devient obsolète et moins efficace, les plates-formes d'analyse de sécurité délivrées dans le cloud qui fournissent des détections personnalisées dicteront quels fournisseurs orienteront le marché.[4] »

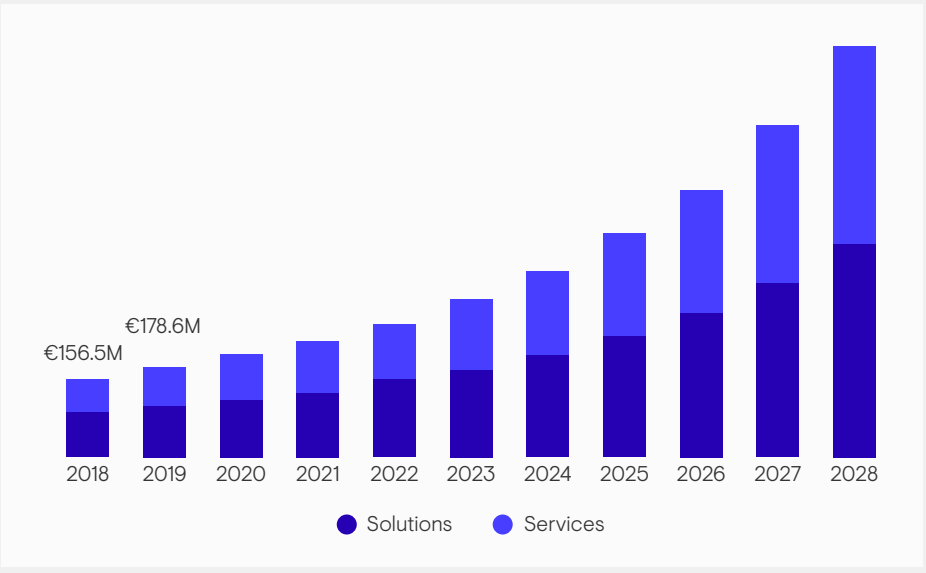
FORRESTER

« En réponse à l'écart croissant des compétences en matière de sécurité et aux tendances des attaquants, des outils de détection et de réponse étendues (XDR), de l'apprentissage automatique (Machine Learning) et des capacités d'automatisation émergent pour améliorer la productivité des opérations de sécurité et la précision des détections [5]. »

GARTNER

LES PRESSIONS CROISSANTES EN CYBERSÉCURITÉ ENCOURAGENT L'ADOPTION DE XDR

Le marché XDR devrait croître à un taux de 19,6 % TCAC[6]



[4]The Forrester Wave: Security Analytics Platforms, Q4 2020 report
[5]Top Security and Risk Management Trends June 2020
[6]XDR Market Size, Share & Trends Analysis, Grand View Research, April 2021

Secureworks®

Secureworks® (NASDAQ: SCWX) est un leader mondial de la cybersécurité qui assure le progrès humain en devançant et en déjouant les menaces Cyber avec Secureworks® Taegis™, une plateforme d'analyse de sécurité native du cloud construite sur plus de 20 ans d'intelligence et de recherche sur les menaces du monde réel, améliorant la capacité des clients à détecter les menaces avancées, rationaliser et collaborer sur les enquêtes, et automatiser les actions appropriées

SIEGE SOCIAL

Etats-Unis
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

EUROPE & MOYEN ORIENT

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Allemagne
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

Royaume-Uni
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

Emirats Arabes Unis
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

ASIE PACIFIQUE

Australie
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japon
Otemachi One Tower 17F
2-1 Otemachi 1-chome, Chiyoda-ku
Tokyo 100-8159, Japan
81-3-4400-9373
www.secureworks.jp