Machine Translated by Google

CyberProof®
A UST Company

Le définitif Guide du MDR

Prestations de service

Faites évoluer la sécurité, réduisez les risques et atteignez les objectifs commerciaux critiques

Machine Translated by Google

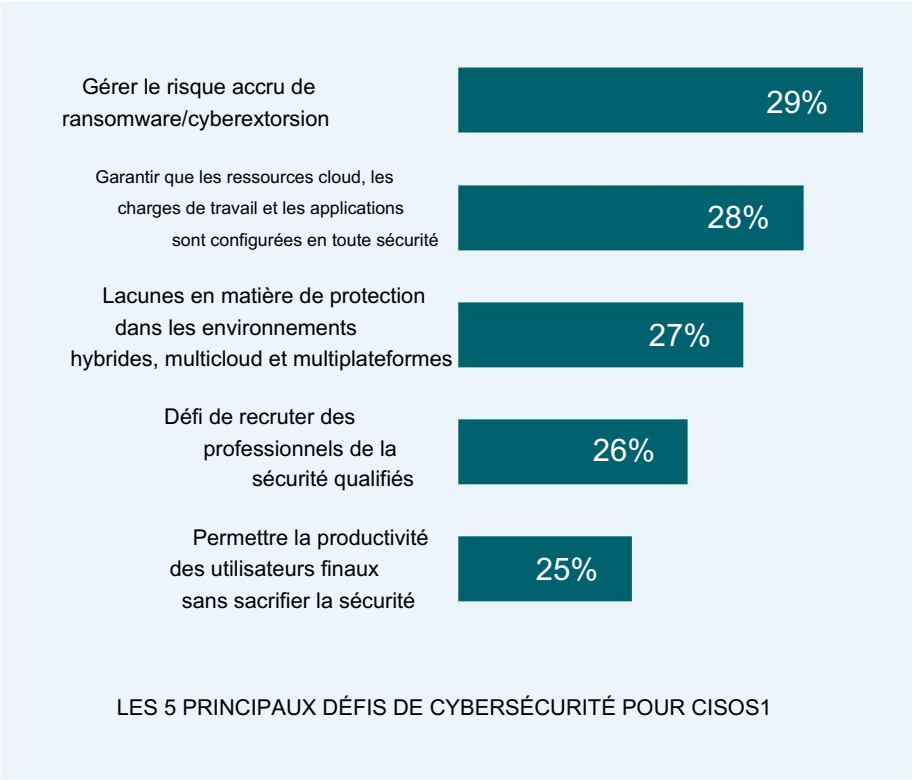
Contenu

Machine Translated by Google

Introduction : Le paysage changeant de la sécurité

La croissance de la transformation numérique et le passage à une infrastructure hybride et cloud native ont permis aux entreprises mondiales d'évoluer à une vitesse vertigineuse, en lançant de nouveaux produits et services, en augmentant les niveaux d'engagement des clients et en ajoutant de l'agilité et de l'automatisation à leur façon de travailler.

Mais il ne fait aucun doute que cette évolution a également ouvert des portes aux cybercriminels. Les entreprises ont du mal à visualiser et à gérer un volume croissant de données, à gagner en transparence sur l'endroit où les menaces surviennent et pourquoi, et à garder une longueur d'avance sur les acteurs des menaces et les réglementations de conformité de plus en plus sophistiquées.



LES 5 PRINCIPAUX DÉFIS DE CYBERSÉCURITÉ POUR CISOS1

65,9%

Le pourcentage des dépenses actuelles en logiciels d'application qui seront consacrés aux technologies cloud en 2025, en hausse par rapport à 57,7 % en 2022.2

1 article de blog Microsoft
2 Source : Impact sur le marché : transition vers le cloud 2022-2025, Gartner

Machine Translated by Google

L'émergence du Managed Détection et réponse

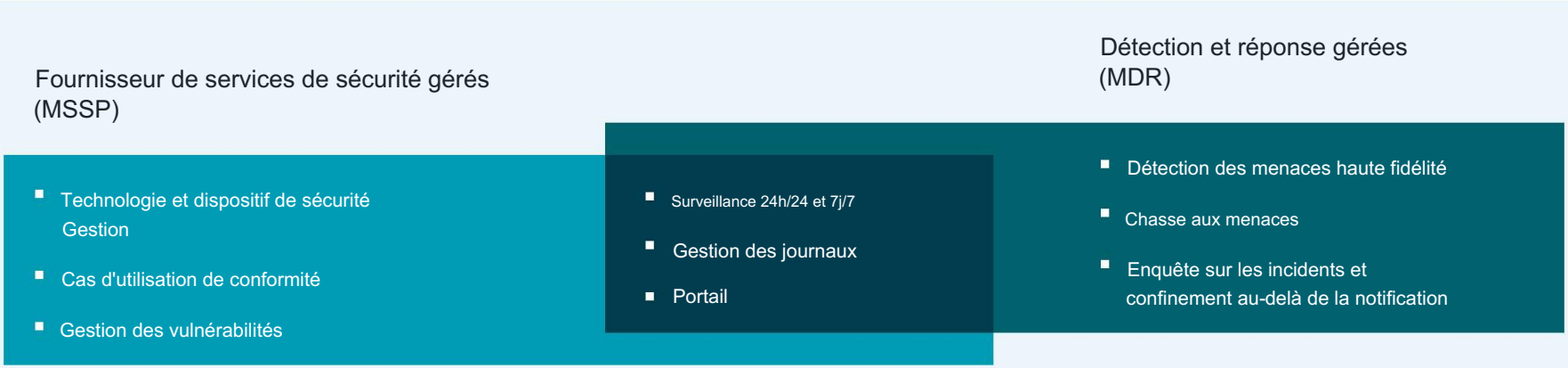
14

Le nombre de comptes divulgués par seconde au troisième trimestre 2022, avec des violations apparaissant dans le monde entier.

Les fournisseurs de services gérés ont tous un objectif commun : améliorer la résilience en matière de sécurité et atténuer bon nombre des défis auxquels les RSSI, les décideurs en matière de sécurité et les équipes SecOps sont confrontés chaque jour.

Jusqu'en 2016, les organisations s'appuyaient sur des fournisseurs de services de sécurité gérés (MSSP), qui les soutenaient avec des capacités informatiques et de sécurité gérées, souvent centrées sur les alertes et réactives.

En 2016, Gartner a inventé le terme Managed Detection and Response. (MDR) pour la première fois dans son Guide du marché, ouvrant une large catégorie incluant des mesures proactives telles que la chasse aux menaces et la réponse aux incidents.3



LE PASSAGE DE L'INDUSTRIE DU MSSP AU MDR

3 https://www.gartner.com/en/documents/3314023

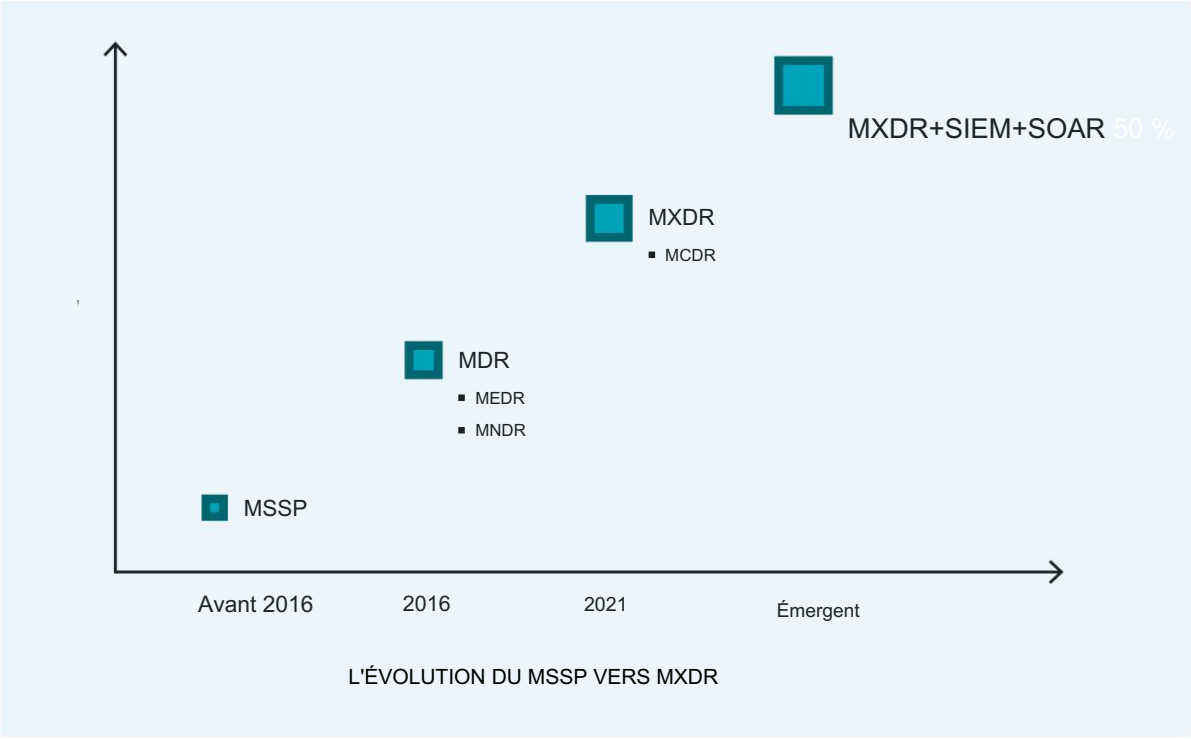
Machine Translated by Google

Évolution du MDR au XDR et au-delà

Peu de temps après, de nouvelles solutions ont émergé pour aborder le MDR sous différents angles et sous-catégories, notamment Managed Endpoint Detection and Response (MEDR), Managed Cloud Detection and Response (MCDR) et Managed Network Detection and Response (MNDR).

Plus récemment, les solutions Managed Extended Detection and Response (MXDR) sont devenues une super catégorie, qui a commencé à évoluer pour inclure un large éventail de fonctionnalités qui englobent également les plates-formes EDR et Security Orchestration Automation Response (SOAR).

Forrester explique comment l'enrichissement de XDR avec les fonctionnalités EDR, par exemple, peut ajouter des cas d'utilisation de gouvernance, de risque et de conformité (GRC), proposer des tableaux de bord et des rapports pour de meilleures analyses et bénéficier de sources de journaux et d'alertes plutôt que de s'appuyer uniquement sur la détection sur les points finaux.4



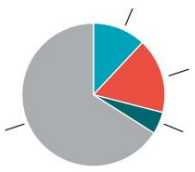
L'ÉVOLUTION DU MSSP VERS MXDR

Pourcentage d'organisations utilisant déjà les services MDR pour les fonctions de surveillance, de détection et de réponse aux menaces.5

4 https://www.forrester.com/blogs/xdr-faq-frequently-asked-questions-on-extended-detection-and-response/?ref_search=3293955_1668433988150

5 https://www.gartner.com/doc/reprints?id=1-27RKN2AN&ct=211029&st=sb

Machine Translated by Google



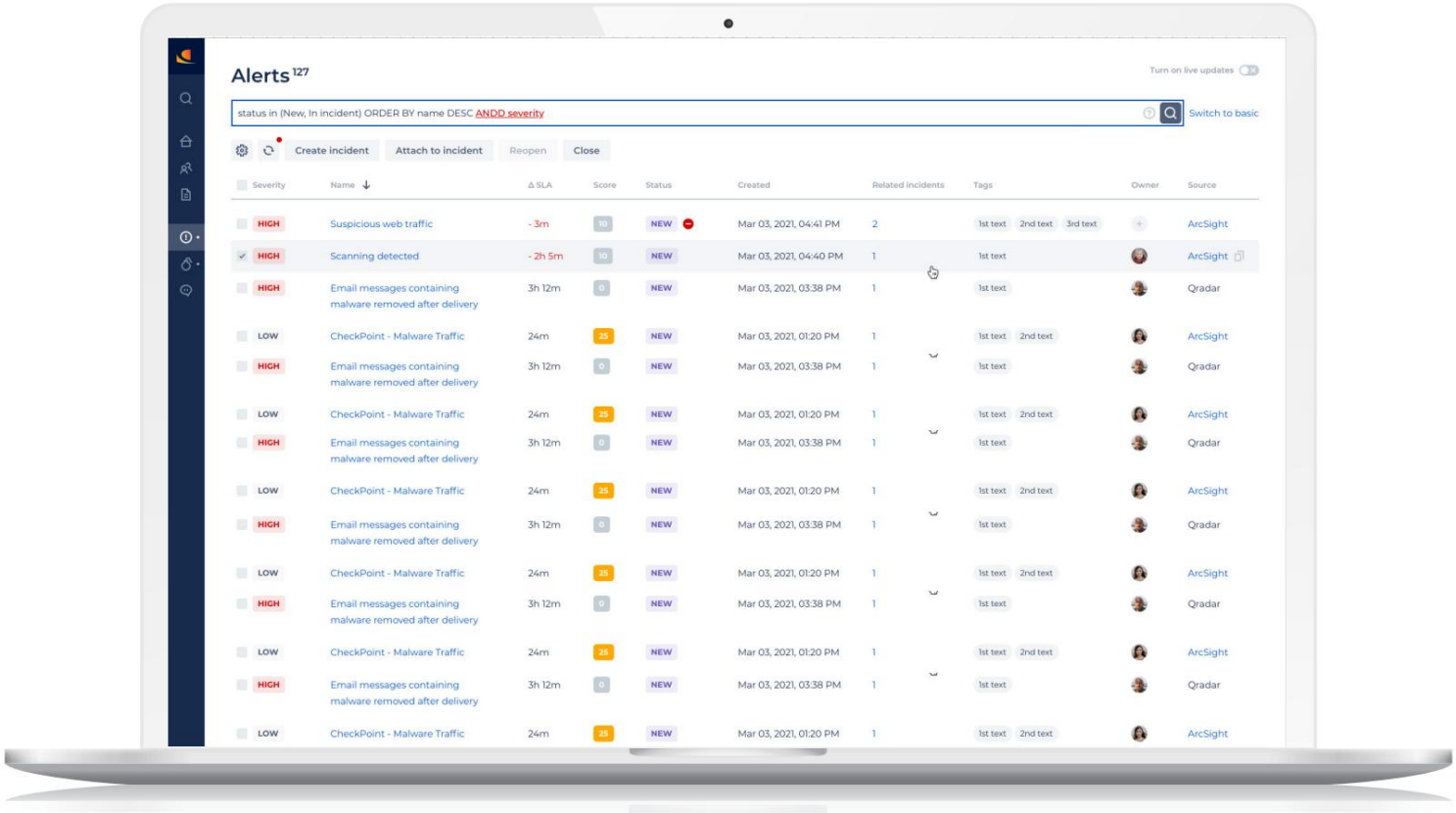
Machine Translated by Google

3. Le volume croissant de données à gérer et à sécuriser

63%

La quantité moyenne de volumes de données des organisations augmente chaque moi

Les organisations génèrent une grande quantité de données, avec des volumes de l'ordre de 5 à 9 To chaque jour, et en constante augmentation. Ces données sont stockées à la fois dans le cloud et sur site, et doivent être collectées, gérées, stockées et même supprimées de manière conforme et en gardant à l'esprit la gestion des risques. Le bon fournisseur MDR peut collecter des données en temps réel, en les acheminant de manière intelligente et contextuelle.



Machine Translated by Google

4. La lassitude face aux alertes est un défi de taille

30%

C'est le nombre d'alertes ignorées par les entreprises de taille moyenne, en raison d'une lassitude face aux alertes.

Avec la prolifération des technologies de sécurité, les équipes de sécurité ne savent plus où donner de la tête. Faux positifs, alertes en double ou suggestions d'atténuation concurrentes : ce ne sont là que quelques-uns des problèmes auxquels les équipes sont confrontées quotidiennement. Une plateforme MDR regroupera plusieurs alertes en un seul incident, puis découvrira la cause première afin que vous soyez uniquement alerté de ce qui compte.

Tout dans le cloud

Par sa définition même, disposer de fonctionnalités cloud natives et hybrides dans MDR est essentiel. Aujourd'hui, 80 % des entreprises ont adopté Microsoft Azure.9 10

Le cloud étant un élément essentiel de toute réalité d'entreprise, un service MDR doit naître dans le cloud, plutôt que d'être intégré au cloud après coup.

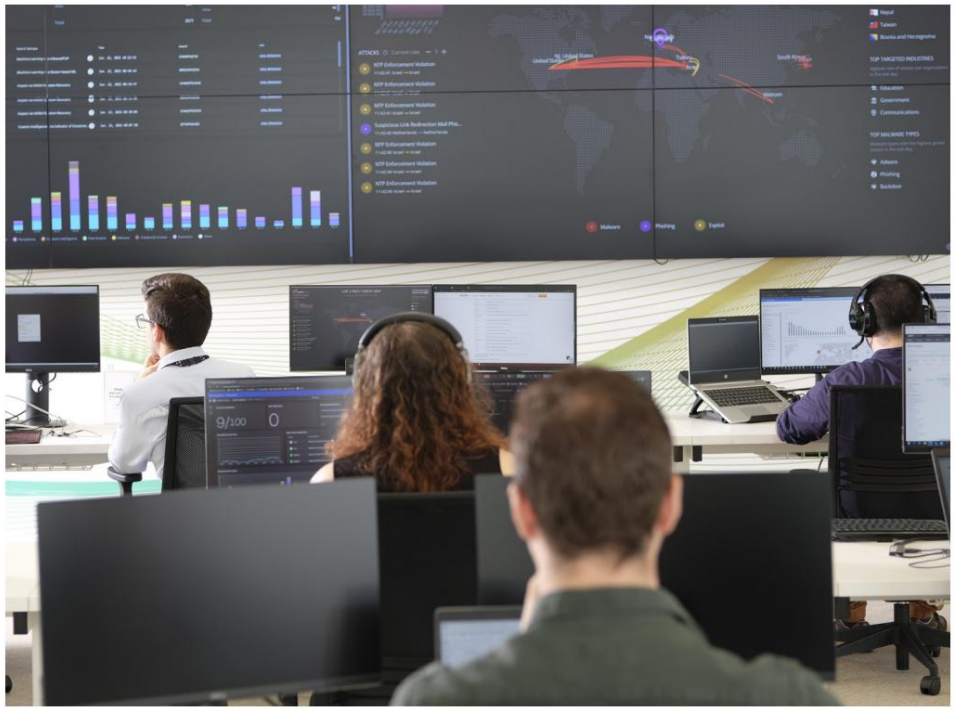
Cela inclut des fonctionnalités telles que :

Sécurité en tant que code : utilisation des environnements DevOps et des pipelines CI/CD pour mettre à jour le contenu en temps réel, déployer de nouvelles fonctionnalités de sécurité via des scripts et apporter des modifications en un seul clic.

Visibilité étendue : gestion des données et des renseignements à mesure qu'ils passent de l'environnement sur site au cloud et vice-versa, avec un aperçu des comportements anormaux dans un environnement hybride et multi-cloud.

Optimisation des données : navigation dans de gros volumes de données, y compris la gestion de la collecte de journaux, l'analyse, le marquage et le filtrage, la mise à l'échelle de la recherche et du reporting et l'accélération de la détection des menaces.

Automatisation : dans le cloud, il devient plus rapide et plus simple de mettre à jour et de tester les systèmes, de déployer des améliorations de l'infrastructure et d'utiliser l'IA et le ML pour ingérer des données et automatiser les réponses.



9 Rapport sur l'état du cloud de Flexera

10 Enquête de Statista : Adoption actuelle du cloud public d'entreprise dans le monde

Machine Translated by Google

Liste de contrôle MDR

S'associer à un fournisseur MDR avancé est une décision importante. Ce n'est pas comme intégrer un outil SaaS ou un nouveau matériel, où vous parlerez une fois par an lorsque la saison des renouvellements approche.

Choisir un fournisseur MDR, c'est choisir un véritable partenaire pour votre propre croissance et votre réussite, un fournisseur en qui vous aurez confiance pour être en première ligne pour protéger votre entreprise, vos données et vos collaborateurs.

Demandez-vous si votre service MDR comprend :

- [ ] Vaste expérience dans le déploiement de solutions SIEM et XDR cloud natives à grande échelle
- [ ] Utilisez des kits de cas qui permettent une intégration rapide et une visibilité sur les menaces cloud
- [ ] Alignement sur la matrice MITRE ATT&CK
- [ ] Suivi personnalisé de requêtes personnalisées, règles de détection, etc.
- [ ] Priorisation rapide des alertes et canaux de communication
- [ ] Approche DevOps automatisée pour déployer l'infrastructure de la pile de sécurité
- [ ] Processus transparents et reporting clair des KPI
- [ ] Modèle SOC hybride qui peut agir comme une extension de votre équipe
- [ ] Outils propriétaires et techniques de gestion des coûts
- [ ] Expertise dans la gestion des coûts de surveillance de la sécurité du cloud

Pourquoi choisir CyberProof ?

CyberProof, une société de l'UST, propose aux entreprises mondiales des opérations et des services de cybersécurité natifs du cloud rapides, transparents et entièrement gérés, garantissant ainsi la sécurité des entreprises lors de leur transition vers le cloud et au-delà.

En utilisant une combinaison innovante d'analystes humains experts, d'analystes virtuels et d'automatisations dans un service entièrement transparent basé sur une plateforme, CyberProof prend en charge, étend et optimise en permanence les opérations de cybersécurité, en collaborant avec les équipes de sécurité internes en temps réel. Nous fournissons:

- Détection et réponse gérées : surveillance de la sécurité, détection des menaces et réponse 24h/24 et 7j/7
- Gestion des plateformes de sécurité : concevoir, configurer et gérer des plateformes de sécurité
- Gestion des vulnérabilités : identifiez et sécurisez les points faibles avant les attaquants.
- Managed XDR pour Microsoft : cyberdéfense étendue dans toute votre entreprise
- Intelligence sur mesure sur les menaces : anticipez de manière proactive les menaces et l'exposition dans la nature
- Surveillance de la sécurité OT/IoT : maintenez une visibilité constante sur la sécurité sur tous vos réseaux
- Chasse avancée aux menaces : identifiez les menaces sérieuses qui se cachent dans vos réseaux
- Ingénierie de cas d'utilisation : Détection et réponse aux menaces à l'aide du Cadre MITRE ATT&CK

Sachant que l'entreprise, les données et les personnes sont protégées, CyberProof vous permet de repousser en toute confiance les limites de la transformation numérique.

Machine Translated by Google

CyberProof®
A UST Company

À propos de CyberProof

CyberProof, une société de l'UST, aide nos clients à transformer leur sécurité en une architecture technologique cloud native et rentable. Notre service Managed Detection & Response (MDR) de nouvelle génération est conçu pour prendre en charge les grandes entreprises complexes en combinant des analystes experts humains et virtuels. Nos services sont rendus possibles par notre plateforme spécialement conçue, le CyberProof Defense Center, qui nous permet d'être plus agiles, de mieux collaborer et de fournir des analyses puissantes. Nos services de sécurité intégrés comprennent la veille sur les menaces, la chasse aux menaces et la gestion des vulnérabilités. Nos experts innovent pour répondre aux besoins de nos clients avec des cas d'utilisation, des intégrations et des automatisations personnalisés.

Pour plus d'informations, visitez www.cyberproof.com.

Barcelone | Californie | Londres | Singapour | Tel-Aviv | Trivandrum

© 2023 CyberProof Inc. Tous droits réservés.