Votre guide pour la commercialisation rapide des services MDR

Tirez parti de WatchGuard MDR pour répondre à la demande croissante de détection et de réponse aux menaces sophistiquées

Ce guide fournit des étapes essentielles pour que nos partenaires commercialisent rapidement une offre de services MDR sous leur marque, répondant aux besoins de sécurité de leurs clients et leur offrant de nouvelles sources de revenus.

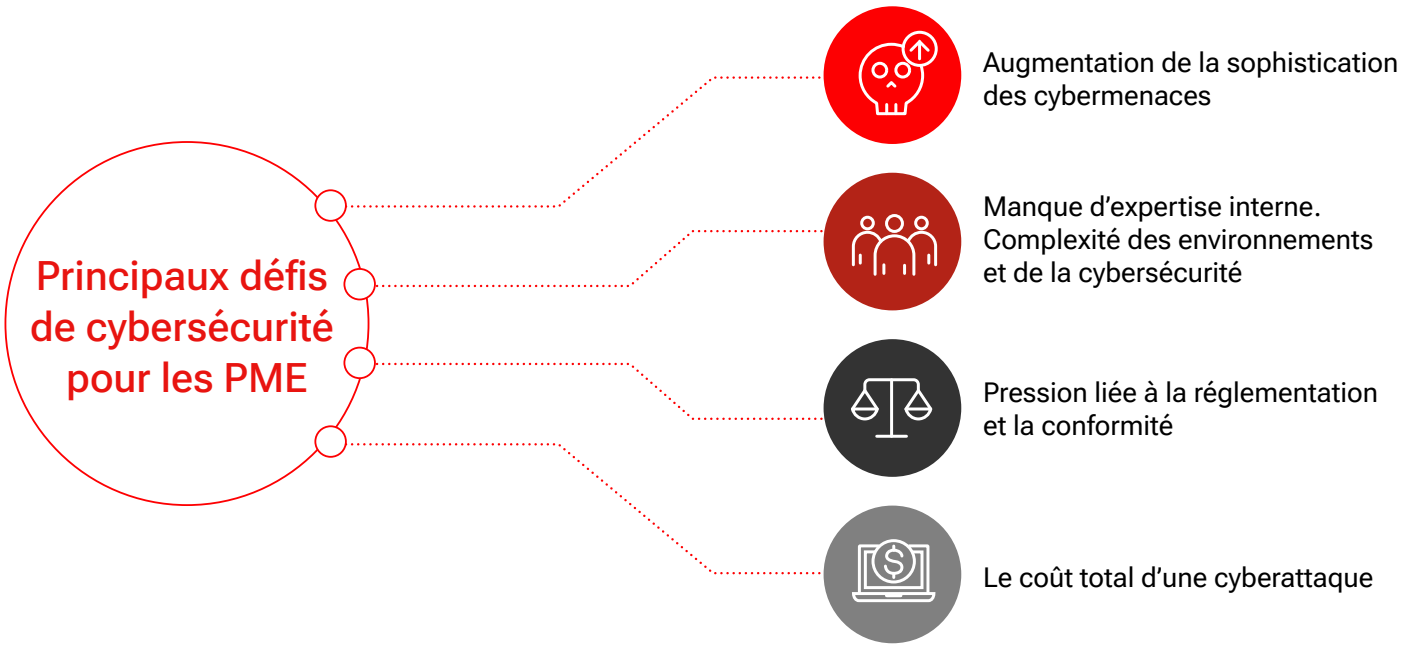
Sommaire

Introduction 2
Principaux défis de cybersécurité auxquels sont confrontées les PME 2
Augmentation de la sophistication des cybermenaces 2
Manque d'expertise interne et complexité de la cybersécurité 3
Pressions liées à la réglementation et la conformité 3
L'impact financier des cyberattaques 3
Les services MDR comme solution pour relever les défis liés à la cybersécurité des PME 4
6 avantages clés des services MDR 4
Comment les partenaires peuvent vendre des services MDR 4
Packaging des services MDR pour la rentabilité 5
Répondre aux objections des clients aux services MDR 7
Présentation de WatchGuard MDR 8
Conclusion 9

Introduction

Dans le paysage numérique actuel, les petites et moyennes entreprises (TPE, PME, ETI, Administrations) sont confrontées à des défis croissants en matière de cybersécurité. À mesure que les cybermenaces gagnent en sophistication, les PME, qui ne disposent souvent pas de l'infrastructure de sécurité nécessaire, deviennent des cibles de choix. Ce livre blanc explore comment les partenaires peuvent efficacement positionner et vendre des services managés de détection et de réponse (Managed Detection and Response, MDR) à leurs clients. Nous examinerons les principaux défis auxquels les PME sont confrontées, la manière dont les services MDR peuvent résoudre ces problèmes et proposerons des stratégies aux partenaires pour qu'ils présentent et packagent les services MDR de manière à maximiser la rentabilité.

Principaux défis de cybersécurité auxquels sont confrontées les PME



Augmentation de la sophistication des cybermenaces

Les cybermenaces sont de plus en plus sophistiquées et difficiles à détecter. Les attaques de type « Living off the Land » et les ransomwares sont particulièrement dangereux pour les PME, qui n'ont souvent pas les défenses sophistiquées des grandes entreprises.

Exemples : Fin 2022, des cybercriminels russes ont lancé une attaque contre le réseau électrique ukrainien, démontrant ainsi que la cyberguerre peut provoquer des perturbations à grande échelle. Cela montre que les cyberattaques peuvent cibler des infrastructures critiques, d'où la nécessité de mettre en place des mesures de sécurité robustes.

> « Au cours des quatre dernières années, le groupe de ransomware LockBit a mené une série d'attaques incessantes, ciblant des milliers d'entreprises, d'écoles, d'établissements de santé et de gouvernements à travers le monde, ce qui lui a permis de gagner des millions de dollars. Un hôpital pour enfants, Boeing, Royal Mail du Royaume-Uni et la chaîne de sandwiches Subway comptent parmi les victimes récentes ».
>
> REUTERS

> « Microsoft et OpenAI affirment que les pirates informatiques utilisent ChatGPT pour améliorer les cyberattaques. Un certain nombre de groupes soutenus par des nations commencent à utiliser de grands modèles de langage pour les aider dans la recherche, la rédaction de scripts et la création d'e-mail de phishing. »
>
> WIRED

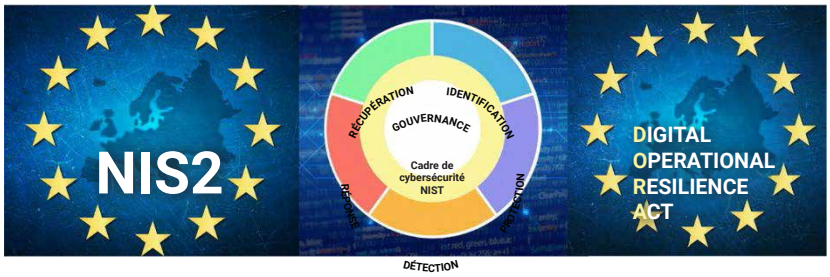
> « Des cyberespions russes sont à l'origine d'un piratage qui a perturbé une partie du réseau électrique ukrainien à la fin de 2022 dans le cadre d'une forme rare et sophistiquée de cyberguerre, a déclaré la société américaine de cybersécurité Mandiant, qui fait partie de Google, dans un rapport publié jeudi. »
>
> The Verge

Manque d'expertise interne et complexité de la cybersécurité

Selon l'étude 2024 (ISC)² Cybersecurity Workforce Study, la pénurie mondiale de professionnels de la cybersécurité s'élève à près de 5 millions. Les PME sont touchées de manière disproportionnée par ce déficit de compétences, ce qui les rend plus vulnérables aux cyberattaques en raison de leur manque d'expertise interne.

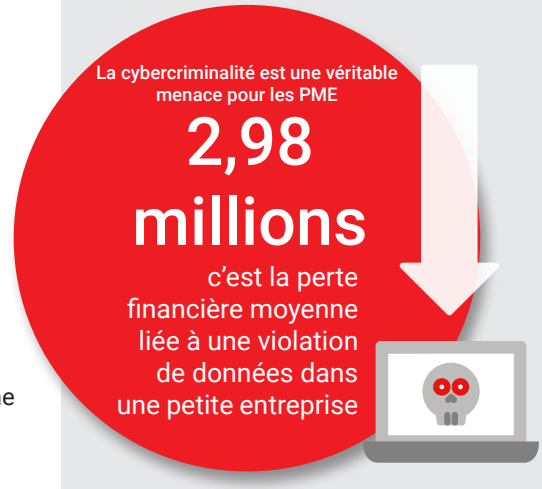
Pressions liées à la réglementation et la conformité

La conformité aux réglementations telles que NIST, NIS 2, DORA, HIPAA et PCI DSS devient de plus en plus obligatoire. Les amendes pour non-conformité peuvent atteindre jusqu'à 10 millions de dollars ou 2 % du chiffre d'affaires mondial. De nombreuses PME ont du mal à affecter les ressources nécessaires pour répondre à ces exigences, ce qui augmente leur risque.



L'impact financier des cyberattaques

Les cyberattaques sont financièrement dévastatrices pour les PME. Le Ponemon Institute indique qu'une seule violation de données peut coûter environ 2,98 millions de dollars à une petite entreprise. Ces coûts comprennent les dépenses directes, telles que les paiements de rançons et les frais juridiques, ainsi que les coûts indirects, tels que les dommages à la réputation et les interruptions.



Rapport Cost of a Data Breach 2023 d'IBM, qui comprend des recherches du Ponemon Institute

Les services MDR comme solution pour relever les défis liés à la cybersécurité des PME

Les services managés de détection et de réponse (MDR) fournissent une surveillance et une détection continues des menaces, ainsi qu'une réponse assurée par des experts. L'externalisation de la cybersécurité à des fournisseurs de services MDR permet aux PME d'accéder à une protection 24h/24 et 7j/7 sans avoir besoin de mettre en place un SOC interne.

Comment les partenaires peuvent vendre des services MDR

Pour vendre efficacement des services MDR, les partenaires doivent identifier leurs segments de clients cibles, adapter leurs offres et développer une proposition de valeur claire. Les étapes clés comprennent :

- **Comprendre le profil client idéal :** Les besoins en matière de cybersécurité et les pressions liées à la conformité varient d'un secteur à l'autre.
- **Définir des packages et des bundles de services MDR :** Offrir des services progressifs, tels que la surveillance, la gestion des correctifs et la conformité, permet de répondre aux divers besoins des clients.
- **Élaborer une stratégie marketing pour les services MDR :** Informer et éduquer leur public grâce à des campagnes ciblées mettant en évidence les avantages uniques des services MDR.

6 avantages clés des services MDR

1. Surveillance 24h/24 et 7j/7 et gestion proactive des menaces
2. Analyse d'experts et réponses personnalisées
3. Réponse rapide aux incidents
4. Assistance à la conformité
5. Solutions rentables
6. Tranquillité d'esprit

Packaging des services MDR pour la rentabilité

Les MSP comprennent parfaitement les environnements, les besoins et les risques de leurs clients. Cela leur permet d'offrir des packages de services qui combinent des technologies de pointe comme les services MDR avec leur expertise. Ils créent ainsi des solutions de sécurité qui répondent aux défis les plus urgents de leurs clients. Voici quelques stratégies pour aider les MSP à intégrer efficacement les services MDR dans leur portefeuille et à réussir :

1. ### Éviter de faire des services MDR un simple module complémentaire :

   Les services MDR ne sont désormais plus optionnels. Ils sont essentiels pour protéger les entreprises contre les menaces sophistiquées. Ils doivent être regroupés avec d'autres solutions, telles que des pratiques robustes de réduction de la surface d'attaque et de sécurité des endpoints pour créer un package complet.

2. ### Tenir compte des besoins de leurs clients :

   Ils connaissent les besoins et les budgets de sécurité de leurs clients. Proposez des packages qui répondent à leurs problèmes et offrent une réelle valeur ajoutée au juste prix.

3. ### Proposer un chemin de mise à niveau :

   Tous les clients ne souscriront pas au package le plus complet dès le départ. Montrez-leur les avantages dont ils pourraient bénéficier et encouragez les mises à niveau progressives au fil du temps.

4. ### Expliquer la valeur des services MDR :

   Ne présumez pas que les clients comprennent parfaitement ce en quoi consistent les services MDR. Mettez en évidence les avantages de leur bundle, tels que la réduction du temps de réponse aux menaces, la réduction des coûts d'incident et l'amélioration de la conformité.

5. ### Offrir une assistance et une génération de rapports supplémentaires :

   Certains clients peuvent avoir besoin d'une génération de rapports plus détaillés ou d'une assistance supplémentaire, en particulier pour la conformité réglementaire. C'est une excellente opportunité de vendre des services premium.

En regroupant les services MDR avec des services, des produits ou des fonctionnalités spécifiques complémentaires, les MSP fournissent une solution de sécurité robuste, de bout en bout.

Pour relever les défis croissants auxquels les clients sont confrontés, tels que les menaces sophistiquées, le manque d'expertise interne, les environnements complexes, les pressions liées à la conformité et les coûts élevés des cyberattaques, il est essentiel d'offrir une « échelle » de services dont les MDR sont un élément central. Ces services améliorent la posture en matière de sécurité des clients et offrent une tranquillité d'esprit. Vous trouverez ci-dessous une proposition d'échelle de services de sécurité managés conçus pour résoudre ces problèmes en intégrant les services MDR.

Les problèmes rencontrés par vos clients

Augmentation de la sophistication des cybermenaces

Manque d'expertise interne.

Complexité de la cybersécurité et des environnements

Pression liée à la réglementation et la conformité

Le coût total d'une cyberattaque

Cyber assurance

Packaging des services MDR

Niveau 1 : Gestion de la prévention, de la détection et du confinement des endpoints :

Ce service d'entrée de gamme offre une prévention et une détection des menaces sophistiquées, avec une surveillance 24h/24 et 7j/7. Il comprend des notifications automatisées en cas de violation, la détection des ransomwares et leur confinement, tout en assurant une perturbation minimale de l'environnement du client.

Niveau 2 : Sécurité des endpoints entièrement managée

Ce niveau s'appuie sur leprécédent en renforçant l'hygiène de la cybersécurité grâce à l'identification des vulnérabilités et à la gestion des correctifs.
Il assure également une récupération rapide en cas d'incident, permettant des interruptions minimales.

Niveau 3 : Sécurité des endpoints entièrement gérée + Défense de la chaîne d'approvisionnement

Ce package se concentre sur la défense contre les attaques de la chaîne d'approvisionnement en plus de la sécurité des endpoints. Il partage les renseignements sur les menaces avec les partenaires clés (par exemple, les indicateurs de compromission, les règles Yara), ce qui garantit que les opérations commerciales sont protégées contre les vulnérabilités externes.

Niveau 4 : Sécurité des endpoints entièrement managée + conformité réglementaire

Conçu pour les entreprises opérant dans des secteurs réglementés, ce package offre des services MDR 24h/24 et 7j/7 avec des politiques de conformité automatisées alignées sur des cadres tels que NIST, NIS 2 et DORA. La génération de rapports détaillés et une documentation d'audit sont incluses pour assurer la conformité lors des audits réglementaires.

Niveau 5 : Sécurité des endpoints entièrement managée + cyberassurance

Certains clients peuvent avoir besoin d'une génération de rapports plus détaillés ou d'une assistance supplémentaire, en particulier pour la conformité réglementaire. C'est une excellente opportunité de vendre des services premium.

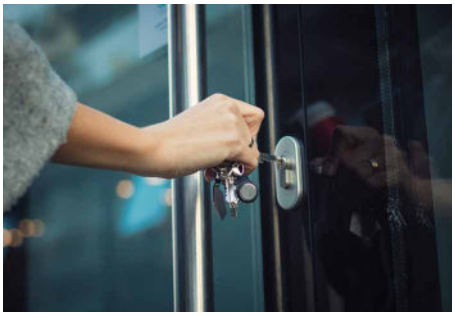
Répondre aux objections des clients aux services MDR

Une objection courante du client est : « Ai-je vraiment besoin de services MDR ? » La réponse est oui. Soulignez la sophistication croissante des cybermenaces et la nécessité d'une surveillance continue pour améliorer la détection et la réponse. Faites référence à des violations notoires pour mettre en évidence le risque pour les entreprises de toute taille.

Si les clients pensent que les services MDR semblent excessifs, rappelez-leur le coût d'une seule violation et comment les services MDR peut prévenir de tels incidents. Pour ceux qui se demandent pourquoi la sécurité existante ne suffit pas, expliquez-leur que la sécurité nécessite une approche en couches. Les services MDR viennent compléter les solutions existantes et permettent de lutter plus efficacement contre les menaces sophistiquées d'aujourd'hui.

Enfin, s'ils craignent que les services MDR ne soient qu'une mise à niveau inutile, soulignez qu'il ne s'agit pas seulement de technologie, elle est soutenue par l'expertise du SOC WatchGuard et de l'IA avancée, combinée à la connaissance de leur environnement par votre équipe. Les services MDR sont une mise à niveau essentielle pour aujourd'hui et pour demain.

L'analogie de la protection : verrous, capteurs et caméras de surveillance



Serrures = Antivirus

Alarmes de capteurs = EDR

Surveillance = MDR

Pour simplifier la valeur des services MDR, vous pouvez utiliser cette analogie :

Votre système de sécurité est comme votre maison. Les serrures de vos portes et fenêtres représentent les solutions de type antivirus et de protection des endpoints (Endpoint Protection, EPP) traditionnelles. Ils empêchent les menaces d'entrer, mais si un intrus habile trouve un moyen de crocheter la serrure, il peut toujours accéder à votre maison sans être détecté.

Maintenant, imaginez que vous avez installé des capteurs de mouvement à l'intérieur de votre maison. Ces capteurs correspondent aux outils de détection et de réponse au niveau des endpoints (Endpoint Detection and Response, EDR). Ils détectent les mouvements inhabituels à l'intérieur de la maison et déclenchent des alarmes lorsqu'un comportement suspect est détecté.

Cependant, même avec des capteurs de mouvement, vous avez parfois besoin d'un expert en sécurité pour analyser ce qui se passe. C'est là qu'interviennent les services MDR. Disposer de services MDR, c'est comme avoir une équipe de surveillance 24h/24 et 7j/7 qui surveille activement vos caméras de sécurité. Ces experts n'attendent pas qu'une alarme se déclenche ; ils sont en permanence à l'affût de toute activité suspecte, prêts à réagir instantanément. Si un intrus se présente, les services MDR répondent rapidement à la menace avant qu'elle ne cause des dommages importants, ce qui vous permet de dormir sur vos deux oreilles, sachant que votre maison est sécurisée.

Cette analogie souligne l'importance d'avoir plusieurs couches de sécurité en place. Les services MDR constituent une couche supplémentaire qui assure une réponse rapide et proactive, offrant aux entreprises une tranquillité d'esprit.

Présentation de WatchGuard MDR

La cybersécurité est très complexe et évolue si rapidement que les entreprises disposant de ressources limitées ont du mal à la gérer efficacement par elles-mêmes.

WatchGuard MDR est une extension de nos MSP, fournissant une surveillance 24h/24, 7j/7, une détection proactive, un confinement et des conseils d'experts pour aider à récupérer et à améliorer la posture en matière de sécurité globale de leurs clients.

Géré par des professionnels de la cybersécurité 24h/24, WatchGuard MDR offre une assistance flexible et adaptée à vos besoins opérationnels, que ce soit 24h/24 et 7j/7 ou 8h/j et 5j/7.

Ce qui différencie WatchGuard MDR :

1. WatchGuard MDR permet aux partenaires de créer leur propre offre de services MDR afin d'élargir leurs sources de revenus.
2. WatchGuard MDR offre une tranquillité d'esprit aux MSP et à leurs clients, car des experts en sécurité dédiés surveillent les environnements de leurs clients 24h/24 et 7j/7.
3. WatchGuard MDR accélère le délai de rentabilité, car c'est une solution simple et facile à déployer. Elle ne nécessite pas de déploiement supplémentaire lorsque le client est déjà protégé avec les solutions avancées de sécurité des endpoints WatchGuard.
4. WatchGuard MDR s'adapte au modèle opérationnel des MSP, offrant un service MDR de qualité professionnelle 24h/24 et 7j/7, que ceux-ci travaillent 24h/24 et 7j/7 ou 8h/j et 5j/7, leur permettant d'évoluer de manière flexible et de proposer des configurations sur mesure à leurs clients.

Pourquoi WatchGuard MDR

- Créez votre propre offre MDR à l'image de votre marque. Élargissez vos sources de revenus.
- MSS de qualité professionnelle. Tranquillité d'esprit.
- Simple à déployer. Délai de rentabilité rapide.
- Flexibilité opérationnelle. Évolue avec vous.

« Les services MDR sont devenus une lueur d'espoir, offrant un service managé attrayant, adapté à l'évolution des menaces et aux attentes des clients. Les DSI dont les ressources sont limitées ont désormais la possibilité d'améliorer leur programme de cybersécurité d'une manière abordable et personnalisée pour répondre à leurs besoins uniques en matière de sécurité et de risques. »

Craig Robinson
Vice-président de la recherche chez IDC

Les services MDR simplifiés

Le paysage des menaces de cybersécurité évolue constamment, et les PME ont besoin d'une solution robuste pour se protéger contre les attaques sophistiquées. Les services managés de détection et la réponse (MDR) offrent une solution de sécurité évolutive et rentable qui permet la continuité des activités et la conformité aux réglementations. Les partenaires qui positionnent efficacement les services MDR aideront leurs clients à atténuer les risques, à améliorer leur position sur le marché et à accroître leur rentabilité.

Ne manquez pas l'occasion d'améliorer vos services de sécurité managés en intégrant les services MDR à votre offre de base. Bénéficiez de l'accès privilégié que WatchGuard, un fournisseur de cybersécurité entièrement dédié aux MSP, offre à ses partenaires. Consultez WatchGuard MDR pour en savoir plus.

À propos de WatchGuard

WatchGuard® Technologies, Inc. est un leader mondial de la cybersécurité unifiée. Notre Unified Security Platform® est pensée pour les fournisseurs de services managés afin d'assurer une sécurité de pointe augmentant l'évolutivité et la vélocité de leur entreprise tout en améliorant leur efficacité opérationnelle. Recommandés par plus de 17 000 revendeurs et prestataires de services spécialisés dans la sécurité et adoptés par plus de 250 000 clients, les produits et services primés de WatchGuard mettent en lumière des solutions d'intelligence et de sécurité réseau, de protection avancée des endpoints, d'authentification multifacteur et de Wi-Fi sécurisé. Ensemble, ils offrent les cinq éléments essentiels d'une plateforme de sécurité : sécurité complète, intelligence collective, clarté et contrôle, alignement opérationnel et automatisation. L'entreprise a établi son siège social à Seattle, dans l'État de Washington, et possède des bureaux dans toute l'Amérique du Nord, en Europe, en Asie-Pacifique et en Amérique latine. Pour en savoir plus, rendez-vous sur le site WatchGuard.com/fr.

SERVICE COMMERCIAL FRANCE +33 97 755 4336 ADRESSE EMAIL france@watchguard.com SITE INTERNET https://www.watchguard.com/fr

WatchGuard Technologies, Inc.