PRÉSENTATION DE SOLUTION

Secureworks®

Évaluation d'un fournisseur de détection et réponse étendue managée

Les équipes de sécurité de toutes les tailles et de tous les niveaux de maturité ont du mal à gérer les surfaces d'attaque étendues, les outils disparates et la pénurie de personnel et de compétences. Secureworks® Taegis™ ManagedXDR résout ces problématiques, mais tous les fournisseurs de XDR gérée ne sont pas égaux sur le marché d'aujourd'hui. Lisez cette présentation pour connaître les exigences à rechercher dans une solution de XDR managée et savoir comment Secureworks se distingue sur un marché chargé et évolutif.

Problématique de la détection et réponse

76 %

des professionnels de la cybersécurité lors d'une enquête récente d'ESG[1] ont indiqué que la détection des menaces était plus difficile qu'il y a deux ans. Notre expérience auprès des clients indique que c'est le résultat d'un volume de menaces amplifié, de pénuries de personnel, d'un excès de tâches manuelles et de l'élargissement de la surface d'attaque.

89 %

des personnes interrogées dans le cadre de l'enquête ESG[1] indiquent qu'ils ont l'intention d'augmenter le financement de leurs activités de détection des menaces et de réponse. Toutefois, il n'est pas facile de choisir un fournisseur avec lequel établir un partenariat. En effet, le nombre de fournisseurs sur le marché qui essaient de traiter la détection et réponse a considérablement augmenté. Toutefois, ces fournisseurs ratent leur coup pour la plupart.

Ce que vous y trouverez

Cette présentation détaille les principales exigences à prendre en compte lors de l'évaluation de services managés de détection et réponse. Elle indique ensuite comment ManagedXDR fait appel à une combinaison de logiciel analytique, d'intelligence approfondie sur les menaces et d'expertise de pointe en sécurité pour améliorer considérablement les délais de détection et de réponse. Des liens vers des ressources utiles telles que des rapports, des documents et des webinaires sont fournis tout au long de la présentation si vous souhaitez rapidement obtenir des réponses à vos questions ou consulter des données de tiers.

[1]Source : ESG Master Survey Results, The Threat Detection and Response Landscape, avril 2019

Les disponibilités varient selon les zones géographiques. © 2021 SecureWorks Inc. Tous droits réservés.

Tableau des exigences de l'acheteur

Le tableau suivant indique en quoi la solution de XDR managée que vous évaluez doit répondre à certaines conditions minimum pour résoudre les problématiques ci-dessus.

Composant	Description	Questions d'évaluation d'un fournisseur
	La vitesse d'analyse constitue une arme puissante pour les opérations de sécurité. Toute solution proposée doit être conçue à partir de la dernière technologie d'analytique, même si vous n'y faites pas appel directement. Recherchez les véritables architectures Cloud natives qui intègrent des méthodes de science des données telles que l'apprentissage automatique et le Deep Learning.	1. Indiquez votre rapidité de détection de <insérer menace ici> et pouvez-vous nous montrer comment vous allez y répondre en notre nom ? 2. Expliquez comment votre technologie d'analytique Cloud native fonctionne. L'avez-vous conçue en interne ou êtes vous simplement partenaire d'un autre fournisseur ? 3. Indiquez-nous comment vous avez incorporé la science des données dans votre processus de développement logiciel.
	La détection rapide d'une fausse alarme n'est pas très efficace. Les détections précises favorisent les réponses précises. Les détecteurs reposant sur l'IA doivent être dédiés et utilisés lors des opérations quotidiennes du fournisseur. Ces détecteurs sont utilisés pour identifier les anomalies de comportement, telles que les attaques de type commande et contrôle ou par force brute, ou encore les informations d'identification volées.	1. Indiquez la précision avec laquelle vous pouvez détecter <insérer menace ici> et pouvez-vous nous montrer comment vous allez y répondre en notre nom ? 2. Parlez-nous de votre expérience en matière de réponse et d'élimination des menaces pesant sur les organisations. 3. Pouvez-vous me présenter une démo de la manière dont votre solution va appliquer cette expérience pour maintenir notre sécurité ? 4. Votre logiciel est-il propriétaire ou est-il fourni par un tiers ? Notre équipe peut-elle accéder à votre logiciel dans le cadre de la solution ?
	Lorsqu'un cybercriminel a infiltré votre environnement, il utilise souvent des outils légitimes pour échapper à la détection par les contrôles de sécurité traditionnels. En fait, notre recherche démontre que la durée de présence moyenne des attaquants est de 111 jours. Détecter et éliminer ces menaces nécessite de vastes quantités de données sur les menaces, combinées à une compréhension approfondie du comportement des menaces.	1. De combien de professionnels disposez-vous pour tenir le rythme du paysage des menaces ? 2. Montrez-nous comment votre logiciel intègre une diversité de données sur les menaces historiques, actuelles et potentielles. 3. La solution s'adapte-t-elle aux nouveaux schémas d'attaques ou s'agit-il d'un ensemble statique de règles faciles à déterminer et à déjouer ? 4. Décrivez comment vous procédez pour découvrir des menaces dans les environnements d'autres clients et intégrer celles-ci à notre posture de défense.
	La collaboration et la transparence entre le fournisseur et votre équipe est un facteur de réussite clé. Il doit nécessairement exister des fonctionnalités d'investigation collaborative et des canaux de communication ouverts. Les menaces ne dorment jamais, et il doit en être de même pour la capacité de votre fournisseur à vous tenir informé d'un risque sur votre entreprise.	1. Veuillez nous montrer une démo de l'interface utilisateur que vous fournissez pour prendre en charge la recherche et les investigations en collaboration. 2. Décrivez ce qui se produit lorsque nous avons des questions. Pouvons-nous vous appeler ou discuter en direct par chat à tout moment ? 3. Indiquez comment vous savez quoi rechercher dans notre environnement et ce qui déclencherait une recherche de menace avec nous. Pouvons-nous lancer une demande d'aide dans ce domaine ?
	Votre équipe doit être en mesure de compter sur des professionnels expérimentés de la sécurité pour apporter son aide lors des événements critiques. Un fournisseur doit pouvoir prouver exactement que les heures de réponse aux incidents à distance font partie de sa solution XDR managée sans frais ou coûts cachés.	1. Les heures de réponse aux incidents sont-elles incluses dans la solution managée ? 2. Quelle sera votre rapidité de réponse en cas d'incident validé ? 3. Dites-nous en plus sur l'expérience de votre équipe de réponse. Ses membres sont-ils reconnus par des analystes du secteur d'activité ?
Suivi continu de la connexion entre les ressources Web et machines	Manuel	Automatisé

Les disponibilités varient selon les zones géographiques. © 2021 SecureWorks Inc. Tous droits réservés.

Cliquez ici pour demander une démo de notre logiciel d'analytique de sécurité

OU

Cliquez ici pour regarder un webcast et en savoir plus

« Donnez la priorité aux fournisseurs qui détiennent leur propre propriété intellectuelle de MDR »

Forrester Research Inc. Now Tech : Managed Detection And Response (MDR) Services, 2e trimestre 2018, Jeff Pollard

Consulter le rapport

Lire le livre blanc IDC Analyst Connection sur la MDR suivant

de Martha Vazquez

Lire le livre blanc

Pour télécharger une fiche technique sur ManagedXDR, **cliquez ici.**

Les réponses à ces questions indiqueront si la solution XDR managée proposée peut améliorer votre posture de défense ou si elle va gaspiller votre temps et vos ressources limités. Bien entendu, chaque environnement a des variables uniques à prendre en compte, notamment la taille de l'effectif, les investissements technologiques existants, le secteur d'activité ou les nuances géographiques. Mais cette liste de base de considérations vous aidera à éviter de prendre une décision regrettable.

Taegis ManagedXDR

La vitesse et la précision de détection nécessitent une formule optimisée par logiciel. Notre solution ManagedXDR repose sur une plate-forme d'analytique de sécurité extrêmement puissante nommée Taegis. Celle-ci a été conçue à partir de techniques avancées de science des données qui permettent de détecter de manière fiable les adversaires qui échapperaient autrement à votre vigilance.

Notre analytique comportementale des menaces repose sur une combinaison d'apprentissage automatique et de deep learning, entraînés par nos fonctionnalités propriétaires d'intelligence sur les menaces et nos données client. Le logiciel intègre des cas d'usage de la détection, des workflows d'investigation simple et des actions automatisées d'isolement couvrant vos environnements de points de terminaison, de réseau et Cloud (voir Figure 1).

Secureworks fusionne l'intelligence humaine et machine pour améliorer la sécurité des organisations de toutes tailles. Cliquez sur l'un des liens suivants pour en savoir plus sur nos capacités.

- La cartographie MITRE ATT&CK
- Expertise en réponse aux incidents et en recherche de menaces
- Intelligence sur les menaces et recherche
- Plus de 20 ans d'excellence des services
- Voir comment nos experts comprennent l'état d'esprit d'un pirate

ManagedXDR permet à votre équipe, quel que soit son niveau, de traiter un volume de charges applicatives et de menaces en augmentation constante. Nous apportons notre expertise à vos opérations quotidiennes. Votre équipe peut collaborer avec nous lors des recherches, peut discuter avec nos analystes et évaluer régulièrement votre posture de sécurité.

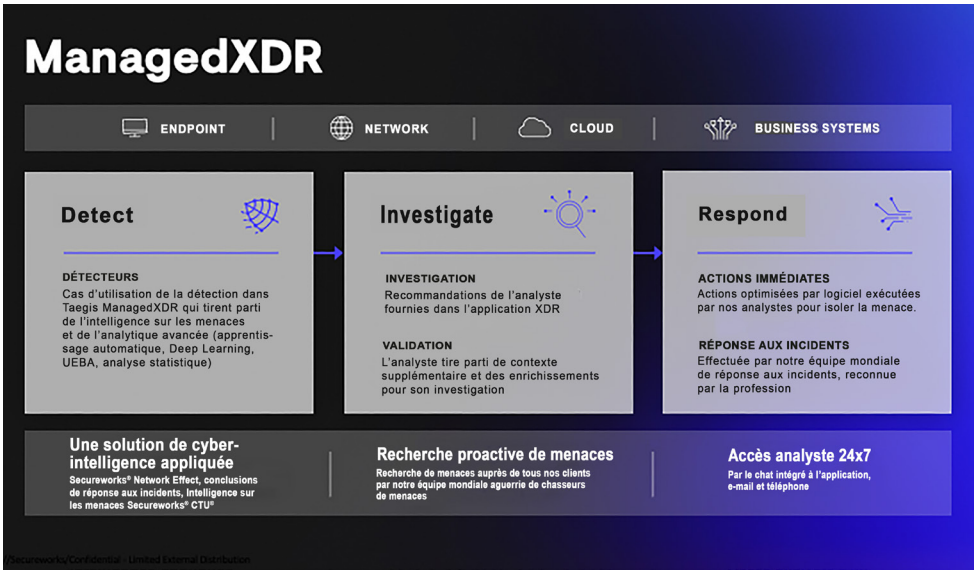

Figure 1. ManagedXDR

Les disponibilités varient selon les zones géographiques. © 2021 SecureWorks Inc. Tous droits réservés.

Secureworks®

10 raisons d'envisager Secureworks pour vos besoins en ManagedXDR

Vous subissez un incident ?

Si votre entreprise nécessite une aide immédiate face à un incident potentiel ou à une faille de sécurité, contactez directement notre assistance téléphonique de réponse aux incidents.

États-Unis et Canada :
1-877-884-1110

Royaume-Uni :
+33-0800-91-57-18

Pour plus d'informations, composez le **1-877-838-7947** pour parler à un spécialiste en sécurité Secureworks secureworks.com

1 **Profitez de plus de 20 années d'expertise**
Établissez un partenariat avec une entreprise de sécurité qui utilise ses 20 années d'expertise en opérations de sécurité pour détecter, isoler et résoudre les menaces avancées.

2 **Participez aux investigations**
Augmentez le niveau de compétences de votre équipe en participant aux investigations avec nos experts.

3 **Chat en direct avec nos analystes de sécurité**
Ouvrez instantanément une fenêtre de chat pour recevoir l'assistance d'un expert dès que vous en avez besoin.

4 **Renforcez votre posture de sécurité par des revues régulières**
Améliorations continues de votre posture de sécurité grâce à des examens et des rapports réguliers.

5 **Détectez plus de menaces grâce à une diversité unique des données**
Basez-vous sur une connaissance des menaces issue de plus de 1 400 interventions de réponse aux incidents, d'une équipe de 80 chercheurs en menaces et de notre expérience de la protection de plus de 4 000 clients dans le monde.

6 **Agissez en toute assurance, avec le soutien de l'intelligence humaine et machine**
Gagnez du temps et augmentez votre efficacité grâce à l'automatisation des tâches de routine et aux investigations collaboratives.

7 **Détectez les menaces inconnues et répondez-y**
Détectez les menaces évasives, telles que les logiciels malveillants sans fichier et sachez exactement comment y répondre.

8 **Recherchez les menaces proactivement pour vérifier les anomalies**
Nos experts vous aident à rechercher les mécanismes de persistance, les tactiques des pirates, les communications réseau anormales et une utilisation anormale des applications.

9 **Réponse aux incidents incluse**
Les heures de réponse aux incidents sont incluses pour renforcer votre tranquillité d'esprit.

10 **Protégez vos déploiements Cloud**
Utilisez notre architecture Cloud native pour détecter et répondre aux événements de vos environnements AWS, Office 365 et Azure.

À propos de Secureworks
Secureworks® (NASDAQ : SCWX) est un leader mondial en cybersécurité qui protège l'évolution des clients à l'aide de Secureworks® Taegis™, une plate-forme d'analytique de sécurité native Cloud reposant sur plus de 20 ans d'intelligence sur les menaces et de recherche dans le monde réel. Les clients peuvent ainsi mieux détecter les menaces avancées, rationaliser et collaborer sur les investigations, et automatiser les mesures appropriées.

Les disponibilités varient selon les zones géographiques. © 2021 SecureWorks Inc. Tous droits réservés.