Secureworks®

PRÉSENTATION DE SOLUTION

Guide de l'acheteur Secureworks® Taegis™ XDR

La solution

La solution a initialement été créée suite aux demandes d'opérations simplifiées et de détection des menaces avancées émises par les clients. Étant donné que les organisations ont du mal à identifier efficacement les cybercriminels et leurs activités, l'importance d'une identification rapide des menaces émergentes est devenue une nécessité.

Introduction au guide de l'acheteur

La détection et réponse étendues (XDR) a été qualifiée de prochaine avancée déterminante en cybersécurité. Le cabinet de recherche et de conseil Gartner a classé XDR comme sa première « tendance sécurité et risques » en 2020 et parmi les 10 premiers « projets de sécurité » pour 2021[1]. De très nombreux blogs du secteur d'activité ont qualifié XDR de « prochaine évolution ». Alors que la rumeur continue à enfler au sein du secteur d'activité, les professionnels de l'IT et les responsables sécurité ont rapidement reconnu l'impact potentiel de XDR dans la transformation de la détection des menaces et de la réponse.

La demande de détection des menaces avancées explose.

83 % des professionnels de l'IT augmentent leur budget consacré aux technologies de détection des menaces et de réponse.[2]

Bien que la solution en soit toujours à ses balbutiements, elle a rapidement suscité l'intérêt de la clientèle. XDR fournit des fonctionnalités centralisées de réponse aux incidents qui détectent les attaques complexes souvent inaperçues par les solutions ad-hoc et SIEM existantes.

Les informaticiens considèrent que XDR constitue une approche viable pour améliorer la protection contre les menaces.
Les capacités supérieures de détection de XDR ont fait l'objet de toutes les attentions[2].

42 %

de visualisation des attaques complexes

38 %

d'analytique qui détecte les attaques modernes

31 %

d'amélioration du délai moyen de détection

[1] Gartner, Smarter with Gartner, 2020
[2] ESG, The Impact of the Modern SOC, 2020

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

Face à divers obstacles en matière de simplification des opérations de sécurité, la promesse d'une productivité accrue est un autre avantage attrayant de XDR.

Alors que la concurrence fait rage pour assurer le bon positionnement des solutions de chacun sur le marché très concurrentiel de XDR, les dirigeants IT se devront d'aller au-delà du battage pour évaluer les fournisseurs de XDR en s'appuyant sur les critères suivants :

- Comparaison entre les fonctionnalités de sécurité existantes et les avantages fournis par une solution XDR
- Besoins de l'entreprise actuels et futurs, et mesures prises par XDR pour maintenir votre posture de sécurité
- Principaux critères de différenciation des solutions XDR

Ce guide met en évidence quinze questions auxquelles chaque équipe de sécurité doit répondre avant de commencer à se renseigner sur un produit XDR.

XDR renforce l'efficacité des SecOps

58 %

des informaticiens estiment que XDR peut améliorer les capacités des analystes en sécurité.[2]

Comprendre le paysage des menaces

À mesure que la transformation de l'entreprise redéfinit les lieux et les modes de travail des entreprises, le paysage des menaces continue également à évoluer. Avec les millions de collaborateurs qui sont passés d'un immeuble de bureaux central à un bureau à domicile, la surface d'attaque a considérablement augmenté. Les adversaires malveillants se sont rapidement adaptés. Les attaques sur les domiciles ont augmenté de 210 % en 2020 pour atteindre pratiquement 2,9 milliards, soit 15,5 % de tous les foyers[3]. Par ailleurs, les cybercriminels font usage d'attaques complexes de plus en plus difficiles à détecter. Une étude récente du Ponemon Institute montre l'impact de ces attaques sophistiquées :

- En moyenne, 80 % des violations réussies sont le fruit d'attaques « zero-day » nouvelles ou inconnues
- Les attaques zero-day nouvelles ou inconnues devraient plus que doubler au cours de l'année à venir

Dans cette nouvelle réalité, les entreprises qui ne sont pas préparées à s'adapter à ce paysage en évolution constante peuvent en ressentir les conséquences pendant des années.

Conséquences d'une protection réactive contre les menaces

Les mesures de sécurité réactives constituent une protection inefficace contre les menaces émergentes et les attaques ciblées d'aujourd'hui. Les équipes de sécurité sont souvent dans l'impossibilité de devancer les adversaires en raison du temps et des efforts exigés par la gestion du grand nombre d'outils de sécurité en silo utilisés pour protéger leur infrastructure. Comme l'intégration entre ces solutions est absente, les analystes de sécurité sont souvent forcés de consacrer plus de temps aux tâches de gestion de la plate-forme et d'administration qu'à la détection des menaces complexes. Ce plus haut niveau de complexité oblige souvent les équipes chargées des opérations de sécurité à combler les manques d'effectifs et de compétences en recrutant des analystes junior. Ces défauts, ainsi que l'incapacité à identifier les menaces complexes et masquées sont caractéristiques des solutions SIEM et des systèmes ponctuels existants. Sans solution unifiée de détection des incidents et de réponse, la plupart des entreprises ont du mal à garder le contrôle des tendances avec une posture de sécurité médiocre.

[3] Trend Micro, rapport annuel sur la cybersécurité, 2020

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

Secureworks®

XDR : une nouvelle approche pour une nouvelle réalité

XDR (Détection et réponse étendues) constitue une nouvelle évolution de la détection des menaces et réponse. Fondamentalement, elle continue là ou l'EDR s'est arrêtée en étendant la détection et la réponse au-delà des points de terminaison pour inclure les environnements réseau et Cloud. Le cabinet d'analyse Gartner définit XDR :

Le terme détection et réponse étendues « désigne une plate-forme de détection des incidents de sécurité et de réponse unifiée qui collecte et met en corrélation automatiquement les données de plusieurs composants de sécurité propriétaires. »[4]

Plus de 90 % des informaticiens déclarent que l'intégration des outils fait partie de leurs cinq premières priorités lorsqu'ils développent l'architecture d'outils de leur centre d'opérations de sécurité. 37 % d'entre eux citent l'intégration comme première priorité[2]. Unifier la détection et la réponse entre des produits en silo accroît la visibilité des menaces et permet aux organisations d'identifier celles qui échappent généralement aux solutions ad-hoc. L'exécution sous-jacente à la détection unifiée commence par la centralisation de données d'événement historiques et en temps réel en des formats de données communs au sein d'un référentiel central. Avec une représentation complète de l'activité des menaces, XDR met en corrélation les données de sécurité pour identifier les relations et les tendances qui indiquent une activité malveillante. Les équipes de sécurité en tirent parti en assurant une détection et une réponse plus rapides, avec un contexte plus vaste et une précision accrue.

Entre trier les alertes et suivre le rythme d'une nouvelle vague de hackers malveillants, les opérations de sécurité n'ont jamais été aussi difficiles. L'exploitation de chaque solution ad-hoc nécessite une gestion et une expertise spécifique. Cette complexité a eu de lourdes conséquences sur la productivité des équipes de sécurité. XDR regroupe plusieurs composants de sécurité en une solution de détection et de réponse unique qui élimine la saisie d'informations identiques dans des systèmes disparates et renforce l'efficacité des analystes. Elle permet également d'élever les capacités des analystes débutants. XDR prend en charge la transformation de l'entreprise grâce à une productivité opérationnelle améliorée et à une détection des menaces renforcée.

Principaux critères d'évaluation des fournisseurs de XDR

Amélioration de l'efficacité de la sécurité et des opérations

L'une des principales exigences liées à XDR consiste à fournir des fonctionnalités centralisées de réponse aux incidents en vue d'améliorer la détection et la réponse face aux menaces sophistiquées inconnues, ainsi qu'à stimuler la productivité opérationnelle. Les XDR doivent également offrir des fonctionnalités de corrélation automatisée afin d'éliminer la désensibilisation aux alertes et de permettre aux équipes chargées de la sécurité de mieux se concentrer sur les menaces significatives.

[4] Gartner, Innovation Insight for Extended Detection and Response, 2020

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

Pour mieux comprendre les fonctionnalités de protection contre les menaces, il est nécessaire de procéder à une évaluation de la capacité du fournisseur à actualiser en permanence ses solutions XDR au moyen d'informations sur les activités de cybercriminels.

5 questions à poser au fournisseur

- Quels sont les types de menaces et d'activités malveillantes détectés par les solutions ? Couvrent-elles les menaces connues aussi bien qu'inconnues ?
- Quelles sont les sources d'intelligence sur les menaces utilisées par le fournisseur ?
- Le fournisseur établit-il une correspondance entre les alertes et le cadre Mitre ATT&CK ? Où les données les plus précieuses résident-elles ?
- Quelle est l'efficacité de la solution XDR pour arrêter les attaques avant que des dommages ne surviennent ?
- Quelles sont les technologies utilisées par le fournisseur pour identifier les anomalies et trouver les indicateurs de compromission ?

Architecture ouverte

On distingue deux principaux types de solutions XDR : XDR fermée ou propriétaire et XDR ouverte. XDR propriétaire est caractérisée par les fournisseurs qui ont unifié leur propre suite de solutions réseau sur une plate-forme de gestion XDR centralisée. Cette approche exige des clients qu'ils retirent et remplacent leurs contrôles de sécurité existants et sacrifient l'efficacité là où la gamme des fournisseurs présente des lacunes.

Contrairement aux solutions proposées par un fournisseur unique, XDR ouverte consolide des produits de sécurité de pointe en un hub de gestion centralisée. Lors de votre recherche de fournisseurs de XDR, assurez-vous que leur solution interopère avec vos outils de sécurité existants et qu'elle est suffisamment souple pour prendre en charge des solutions des vendeurs externes dont votre organisation pourrait avoir besoin à l'avenir.

Faciliter la gestion des données

40 % des informaticiens estiment qu'une amélioration de l'ingestion des données pour tenir le rythme des sources de données en temps réel pourra faciliter l'efficacité de la sécurité et de leur organisation[2]. Avec l'accélération de la transformation numérique, les XDR doivent être en mesure de centraliser, d'établir la corrélation et d'analyser des téra-octets de données batch et en temps réel. Une sécurité cloisonnée crée des angles morts qui occasionnent des lacunes de données sur l'ensemble de votre écosystème. La capacité de centraliser et de normaliser les données dans un référentiel centralisé à des fins d'analyse est l'une des principales exigences associées à XDR.[2]

Les fournisseurs qui développent leurs solutions XDR sur des plates-formes Cloud natives facilitent l'intégration de données issues de produits multifournisseur, et fournissent l'évolutivité requise pour répondre aux demandes d'augmentation du volume de données de l'entreprise. Les entreprises doivent également comprendre

5 questions à poser au fournisseur

- Devrez-vous modifier votre infrastructure ou déployer de nouvelles technologies ? Avez-vous besoin de vous adapter au package technologique du fournisseur ?
- Combien d'environnements votre solution couvre-t-elle (Cloud/point de terminaison/réseau/tous) ? Les considérez-vous séparément ou comme un ensemble ?

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

- Pouvez-vous centraliser et analyser les données à partir de ma technologie de sécurité existante ?
- Quelles sont les sources de journalisation collectées et conservées par le fournisseur ? Pouvez-vous effectuer directement des recherches dans vos informations de journalisation ?
- Comment se déroulent la collecte, le stockage, le traitement et l'analyse des énormes quantités de données que vous exploitez ?

Sélectionnez votre niveau de support

En matière de cybersécurité, il n'existe pas de solution universelle. Il en est de même pour la XDR. Lorsqu'ils sont interrogés sur la gestion de XDR, 50 % des informaticiens préfèrent une XDR entièrement gérée. Parmi ceux qui veulent une XDR gérée, 57 % préfèrent acheter à la fois une solution XDR et un service MDR auprès d'un fournisseur unique[2]. Les clients doivent envisager de se tourner vers un MSSP si votre organisation n'a pas le personnel ou les compétences nécessaires pour fonctionner en 7x24.

Lorsque vous recherchez des fournisseurs, il est important de comprendre la reconnaissance des analystes, ainsi que le niveau de support et de collaboration proposé aux clients qui n'ont pas besoin d'un service managé.

5 questions à poser au fournisseur

- Proposez-vous une solution SDR entièrement gérée ?
- Quel est le niveau d'autonomie fourni par votre solution ?
- Quel est le délai moyen de déploiement complet de votre solution XDR ?
- Lorsque j'ai une question ou un problème, comment puis-je prendre contact avec votre équipe ?
- Si vous êtes sélectionné, pouvez-vous proposer une validation technique gratuite de 30 jours pour démontrer que vous pouvez fournir les résultats que vous indiquez ?

Pourquoi choisir Secureworks

Présentation historique de Secureworks

Fondé en 1999, Secureworks est un fournisseur mondial de solutions de cybersécurité reposant sur l'intelligence. Au titre de leader du marché en services de sécurité managés (MSS), la société met son expertise approfondie de la sécurité au service d'un plus grand nombre de clients avec sa plate-forme d'analytique de sécurité Cloud native Taegis. Reposant sur plus de 20 ans d'informations sur les cybercriminels et de recherche en sécurité, Secureworks fait avancer la force collective de la communauté agissant dans le domaine de la sécurité grâce à la collaboration.

Présentation de Secureworks Taegis XDR

Taegis XDR est une solution de détection et réponse étendue qui regroupe des composants de sécurité de pointe en une approche globale de protection proactive contre les cyberattaques complexes. XDR utilise la plate-forme d'analytique de sécurité Cloud native de Taegis pour assurer une puissante détection de sécurité et fournir des informations optimisées par l'analytique sur un hub de gestion centralisée couvrant les points de terminaison, le réseau et les environnements Cloud. Cette solution dynamise l'expérience de l'analyste au moyen de fonctionnalités opérationalisées d'intelligence sur les menaces et d'automatisation qui améliorent la visibilité et accélèrent les investigations et les réponses. XDR transforme la détection des menaces et la réponse en permettant aux entreprises de :

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

- Détecter les menaces avancées
- Faire confiance aux alertes de sécurité
- Rationaliser les informations et collaborer avec des experts en sécurité
- Automatiser l'action appropriée

L'approche Taegis de la protection contre les menaces

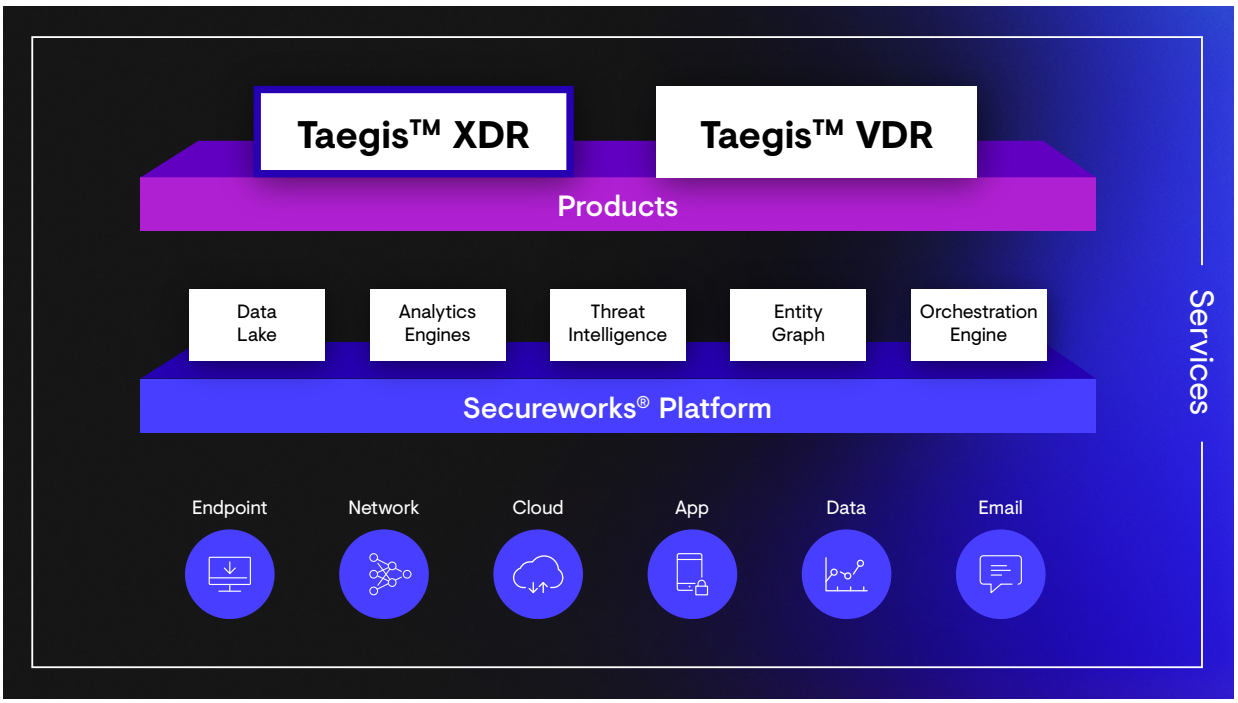
XDR combine la puissance de l'intellect humain avec des informations issues de l'analytique de sécurité afin d'unifier la détection et la réponse pour assurer de meilleurs résultats et simplifier les opérations de sécurité. La solution offre une approche de la cybersécurité globale et ouverte à différents fournisseurs :

Plate-forme XDR ouverte

XDR unifie la détection et la réponse par la collecte, la centralisation et la corrélation d'un volume croissant de données de sécurité issues de plusieurs solutions et sources. XDR procure une vaste visibilité sur les attaques complexes en assurant le suivi des menaces sur l'intégralité de l'écosystème.

Analytique avancée

Repose sur des algorithmes d'intelligence sur les menaces, d'apprentissage automatique et de deep learning pour réduire le nombre d'alertes inutiles et identifier les menaces émergentes et les attaques ciblées qui déjouent les systèmes ponctuels et les outils de sécurité existants.



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

Secureworks®

Intelligence appliquée par la communauté

La connaissance des menaces fournie par tous les clients de Secureworks contribue à notre intelligence sur les menaces intégrée et permet aux clients de tirer parti les uns des autres

Les fonctionnalités clés de Taegis XDR sont les suivantes :

- **Intelligence sur les menaces intégrée** recueillie via l'équipe de recherche Secureworks Counter Threat UnitTM qui suit en continu plus de 150 groupes de cybercriminels actifs
- **Détections reposant sur l'IA** pour réduire le nombre d'alertes et potentiellement détecter les menaces que les outils actuels ignorent.
- **Réponse optimisée par logiciel,** qui automatise les actions d'isolement et de prévention prédéterminées par les 20 années d'expérience de l'investigation de Secureworks.
- **Corrélation automatisée** pour présenter les relations entre les événements à l'échelle de l'environnement de sécurité et ainsi confirmer un danger.
- **Visibilité sur les points de terminaison** pour aider à détecter les adversaires par leur comportement seul avec une technologie de détection des points de terminaison et de réponse reposant sur l'analytique comportementale.
- **« Demandez à un spécialiste »**. Cette fonctionnalité de chat met en place une collaboration en temps réel avec nos propres experts en sécurité Secureworks, qui pourront recommander une réponse ou contribuer aux investigations si nécessaire.
- **Mappage Mitre ATT&CK,** qui couvre plus de 90 % des tactiques et techniques du cadre
- **Enrichissement des alertes** pour fournir du contexte en vue d'assurer des investigations plus informées.
- **Workflows intuitifs d'investigation,** que Secureworks a conçus pour sa propre équipe d'enquêteurs.

Fonctionnalités de la plate-forme Taegis :

Catégorie	Plate-forme Taegis
Commercials	• Licences par abonnement pour les points de terminaison • Abonnement TI inclus • Facturation simplifiée et coûts prévisibles (frais supplémentaires pour les clients qui dépassent le plafond de données)

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

Onboarding	• Simplification de l'intégration, de l'auto-déploiement et de la documentation • Option d'intégration premium
SOC Communication	• Investigations, appels, chat intégré « Demandez à un spécialiste » 24x7x365 • Collaboration en temps réel, remontée simplifiée (jusqu'à 3 contacts)
SOC Analysis	• Axée investigation • Ensemble réduit de remontées ciblées par le centre d'opérations de sécurité • Recherche proactive (mensuelle) • Coordination de la réponse aux incidents
Service Reviews	• Animées une fois par trimestre par TEM avec remise formelle de rapport, responsable de la réussite client
Log ingestion	• Couverture complète des points de terminaison (RC, CS, CB, MSFT) • + de 40 intégrations axées sécurité • Intégrations Cloud natives • Fonctionnalités d'intégration de journal syslog*
Integrations	• API GraphQL pour intégrations approfondies (Alertes, Actifs, Collecte, Investigation), intégration de ServiceNow*, TI intégré
Visibility & Search	• Accès de SCWX et des utilisateurs aux mêmes applications et données afin de renforcer le pouvoir des utilisateurs, options de recherche avancées et personnalisées/guidées*
Detection & Response	• Combinaison d'apprentissage automatique, d'analytique et de moteur de règles. • Actions de réponse intégrées (par ex. isolement de l'hôte) pour les technologies prises en charge.
Reporting & Log retention	• Rétention de données native sur 1 an / Exportation de données pour rapports/API • Tibco LMS (Expérience de double plate-forme) / Module complémentaire de rétention (jusqu'à 3 ans)

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

Extended SOC support	• Lx personnalisée avec ManagedXDR
Health Monitoring	• Intégrité collecteur et agent disponible via application XDR / API
iSensor™ integration	• Intégration native et support pour ManagedXDR (pas TDR)
Device Management	• Géré par le client ou un tiers (pas une option Taegis)
Vulnerability Mgmt.	• Qualys VMS (Expérience de double plate-forme), VDR

Témoignages : Ce que les clients et les cabinets d'analyse déclarent à propos de Taegis XDR

« XDR allie une solution d'analytique à des outils avancés inaccessibles jusqu'à présent. Il détecte des menaces que seuls nous aurions manquées. XDR n'est pas simplement l'outil SIEM de nouvelle génération, c'est une évolution. »

David Levine
VP sécurité de l'entreprise et des informations, RSSI
Ricoh USA, Inc.

« Notre principal défi en matière de sécurité était la possibilité d'identifier un événement et d'y répondre rapidement. Secureworks Taegis nous a averti de l'existence d'une activité suspecte et nous a fourni des recommandations exploitables spécifiques dès notre première nuit de mise en ligne. Nous n'avions jamais été alertés si rapidement et ceci a constitué une première étape critique de la mise en place d'une posture de sécurité renforcée pour notre équipe. »

Dr. Faisal Jaffri
Directeur IT mondial
GKN Wheels and Structures

« Outre analyser, mettre en corrélation et visualiser la télémétrie à partir de plusieurs contrôles de sécurité au moyen d'outils éprouvés que les équipes internes de Secureworks utilisent depuis des années, Secureworks Taegis XDR ajoute une intelligence sur les menaces enrichie et des contre-mesures éprouvées développées par leurs équipes expertes de recherche de menaces et de réponse. »

David Gruber
Analyste de sécurité senior
ESG

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

Démarrez votre propre évaluation gratuite de 30 jours dès aujourd'hui

Cliquez sur le lien ci-dessus pour accéder à la puissance de Taegis XDR. L'évaluation gratuite offre les avantages suivants :

- Aucune carte de crédit ou appel commercial requis : Inscription à l'évaluation en libre-service
- Démarrage en quelques minutes : Accès immédiat à la plate-forme après l'inscription
- Utilisation de vos propres données : Configurez l'évaluation avec vos propres données pour détecter les menaces connues et inconnues dans votre environnement
- 30 jours d'accès : Explorez à votre guise et évaluez XDR via des missions à votre propre rythme
- Utilisez les données de démo préchargées : comprenez comment XDR vous aide à détecter, à enquêter et à répondre à une démo d'attaque de type « living off the land »

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.

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

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