DELL Technologies

Dell SafeGuard and Response

Secureworks® Taegis™ XDR

Gérez et traitez les menaces de cybersécurité grâce à l'automatisation, qui permet d'obtenir de meilleurs résultats en matière de sécurité et de réduction des risques

FONCTIONNALITÉS PRINCIPALES

- Couverture complète **de la surface d'attaque**, y compris les environnements de point de terminaison, de réseau et Cloud.
- **Analyse de la télémétrie et des événements basée sur l'apprentissage automatique et le Deep Learning** provenant de plusieurs vecteurs d'attaque, enrichis d'une intelligence complète sur les menaces.
- **Alertes haute fidélité** complétées par tout le contexte et toutes les données dont vous avez besoin, quand et où vous en avez besoin.
- **Actions de réponse en un seul clic** via la console avec des playbooks automatisés.
- **Une solution XDR ouverte** offre des intégrations personnalisées complètes, préconçues et faciles à créer, avec des outils de sécurité tiers.

La plateforme SaaS Cloud native Secureworks Taegis™ XDR permet d'améliorer l'efficacité de vos opérations de sécurité, en intégrant une connaissance approfondie de la sécurité du paysage des menaces.

- Bénéficiez d'une visibilité et d'un contrôle holistiques sur vos environnements de point de terminaison, de réseau et Cloud Windows, macOS et Linux, en agrégeant la télémétrie en temps réel à partir de l'ensemble des environnements IT de votre organisation.
- Détectez les menaces avancées et les TTP MITRE ATT&CK avec l'analytique optimisée par l'IA, des milliers de contre-mesures automatisées intégrées, une famille de détecteurs de menaces alimentés par l'apprentissage automatique et de puissants graphiques Tactic Graphs™ pour connecter les événements de bas niveau associés. Grâce à l'apprentissage automatique et à l'IA, Taegis reconnaît les schémas au sein d'événements de niveau inférieur et les connecte, là où il existe des points communs.
- Accélérez les investigations en vous concentrant sur les alertes stratégiques. Taegis XDR vous fournit des données de réponse aux incidents et des outils de chasse aux menaces, et met à votre disposition des playbooks automatisés dans une console Cloud facile à utiliser.

Toutes les fonctionnalités intégrées à Taegis sont constamment enrichies avec une intelligence complète sur les menaces, provenant de Secureworks Counter Threat Unit™, et avec des milliers d'engagements réels de réponse aux incidents réalisés par l'équipe de Secureworks.

Pour en savoir plus, consultez le site DellEMC.com/endpointsecurity

Secureworks®

DELL Technologies

OPTIMISER L'EFFICACITÉ DE LA SÉCURITÉ

Taegis XDR regroupe les signaux de votre réseau, du Cloud, des points de terminaison et d'autres outils de sécurité avec une intelligence sur les menaces, afin que vous puissiez bénéficier d'une visibilité et d'un contrôle centralisés sur votre surface d'attaque.

Les détecteurs alimentés par l'IA de Taegis utilisent des algorithmes d'apprentissage automatique et des techniques analytiques de pointe pour surveiller en permanence votre environnement, afin d'identifier les activités malveillantes et de reconnaître les comportements malveillants dès le début. Les playbooks automatiques Taegis XDR et les actions de réponse en un clic permettent de répondre rapidement. Ils sont conçus pour vous aider à détecter, comprendre et arrêter les attaques sophistiquées avant qu'elles ne puissent causer des dommages.

Une intelligence complète sur les menaces, produite en continu par Secureworks Counter Threat Unit, fournit une analyse approfondie des menaces émergentes, ainsi que de l'intention et du comportement des acteurs malveillants. Les contre-mesures Taegis XDR intègrent ces connaissances pour interrompre les attaques. De plus, vos équipes peuvent les utiliser pour comprendre qui est l'auteur de la menace, de quoi il s'agit, quand elle a eu lieu, pourquoi et comment.

OPTIMISER L'EFFICACITÉ DES OPÉRATIONS DE SÉCURITÉ

Enquêtez sur ce qui compte : Taegis met en corrélation l'intelligence sur les menaces, les journaux et les événements issus de différents outils de sécurité pour valider et hiérarchiser les alertes. Ainsi, vos analystes passent moins de temps à gérer les faux positifs et plus de temps à traiter les menaces réelles.

Résolvez plus rapidement l'énigme des attaques : Taegis met automatiquement en corrélation les événements connexes dans vos environnements de point de terminaison, de réseau et Cloud, afin que vous puissiez déterminer la cause première d'une attaque.

Effectuez des investigations à partir d'une seule plateforme : Taegis collecte les données depuis l'ensemble de votre environnement et intègre un kit d'outils complet de chasse aux menaces, y compris les TTP MITRE ATT&CK. Ainsi, vos analystes bénéficient d'une vue globale sur votre infrastructure de sécurité et peuvent mener des investigations au sein de la plateforme, sans avoir à relier manuellement les données ni à passer d'un outil à l'autre.

Travaillez ensemble plus intelligemment et plus rapidement : accélérez les investigations grâce à une collaboration améliorée et à une prise de décision plus rapide, avec des fonctionnalités flexibles de recherche et de création de rapports qui permettent à vos analystes d'assembler rapidement les informations pertinentes et de les partager avec d'autres personnes pour collaborer sur les investigations : insérez des commentaires, ajoutez ou supprimez des données connexes et modifiez l'état.

DELL PROSUPPORT POUR VOS LOGICIELS

Votre solution Dell Endpoint Security Software inclut le support de Dell. Avec Dell ProSupport for Software, des techniciens hautement qualifiés et certifiés sont disponibles 24x7 afin de vous apporter un support logiciel complet, pour une plus grande tranquillité d'esprit.

Contactez votre spécialiste Dell Endpoint Security dédié dès aujourd'hui à l'adresse endpointsecurity@dell.com, pour en savoir plus sur les produits SafeGuard and Response qui peuvent vous aider à améliorer votre posture de sécurité.

Configuration matérielle : Console Taegis XDR : s'agissant d'une application Cloud native, elle requiert un navigateur moderne, c'est-à-dire Chrome, Edge ou Firefox. Systèmes pris en charge pour l'agent Taegis XDR : Microsoft Windows - Windows 10, 11 ; Windows Server 2016 et 2019 ; macOS : macOS Catalina 10.15, Big Sur 11, Monterey 12 (+M1) ; autres : CentOS 7, Amazon Linux 2, Ubuntu 18.04

Pour en savoir plus, consultez le site DellEMC.com/endpointsecurity

Secureworks®