DELL Technologies

Dell SafeGuard and Response

Secureworks® Taegis™ XDR

Gestione e risposta alle minacce alla sicurezza informatica con l'automazione, per ottenere risultati migliori in termini di sicurezza e riduzione del rischio

CARATTERISTICHE PRINCIPALI

- Copertura completa della **superficie di attacco** inclusi gli ambienti endpoint, di rete e cloud.
- **Analisi basate su apprendimento automatico e apprendimento approfondito della telemetria e degli eventi** dovuti a più vettori di attacco, ottimizzate con funzionalità complete di Threat Intelligence.
- **Avvisi ad alta fedeltà** ottimizzati con tutto il contesto e i dati necessari, dove e quando servono.
- **Azioni di risposta con un solo clic** dalla console con playbook automatizzati.
- **Una soluzione XDR aperta** offre ampie integrazioni personalizzate predefinite e facili da creare con strumenti per la sicurezza di terze parti.

La piattaforma SaaS nativa per il cloud Secureworks Taegis™ XDR contribuisce a migliorare l'efficacia e l'efficienza delle operazioni di sicurezza incorporando conoscenze approfondite sul panorama delle minacce.

- Visibilità olistica e controllo sugli ambienti endpoint, di rete e cloud Windows, macOS e Linux grazie all'aggregazione della telemetria in tempo reale proveniente dagli ambienti IT dell'organizzazione.
- Rilevamento delle minacce avanzate e dei TTP MITRE ATT&CK con analisi basate sull'intelligenza artificiale, migliaia di contromisure automatizzate integrate, una serie di sensori delle minacce con apprendimento automatico e una potente grafica Tactic™ per collegare gli eventi secondari correlati. Attraverso l'apprendimento automatico e l'intelligenza artificiale, Taegis riconosce schermi ricorrenti negli eventi secondari e li connette, se individua caratteristiche comuni.
- Accelerazione delle indagini con particolare attenzione agli avvisi critici. Taegis XDR fornisce dati sulla risposta agli incidenti e strumenti di ricerca delle minacce, oltre a rendere disponibili playbook automatizzati in un'unica console cloud di facile utilizzo.

Tutte le funzionalità integrate in Taegis sono costantemente ottimizzate in base a input completi di Threat Intelligence di Secureworks Counter Threat Unit™ e a migliaia di interventi di risposta agli incidenti completati dal team Secureworks.

Ulteriori informazioni sono disponibili sul sito DellEMC.com/endpointsecurity

Secureworks®

DELL Technologies

MASSIMA EFFICACIA DELLA SICUREZZA

Taegis XDR aggrega i segnali dalla rete, dal cloud, dagli endpoint e da altri strumenti per la sicurezza con Threat Intelligence, in modo da poter ottenere visibilità e controllo centralizzati sulla superficie di attacco.

I sensori basati sull'intelligenza artificiale Taegis sfruttano algoritmi di apprendimento automatico e tecniche di analisi all'avanguardia per monitorare continuamente l'ambiente alla ricerca di attività malevole, individuando fin dalle prime fasi comportamenti pericolosi. I playbook automatici e le azioni di risposta con un solo clic di Taegis XDR consentono di reagire rapidamente e sono progettati per rilevare, comprendere e bloccare gli attacchi sofisticati prima che possano causare danni.

La Threat Intelligence completa alimentata continuamente da Secureworks Counter Threat Unit fornisce un'analisi approfondita delle minacce emergenti, nonché delle intenzioni e dei comportamenti degli autori delle minacce. Le contromisure di Taegis XDR si avvalgono di queste conoscenze per bloccare gli attacchi. Inoltre, i team possono utilizzarlo per capire ogni aspetto di una minaccia: chi, cosa, quando, perché e come.

MAGGIORE EFFICIENZA DELLE OPERAZIONI DI SICUREZZA

Indagini sugli aspetti rilevanti: Taegis mette in correlazione Threat Intelligence, log ed eventi di diversi strumenti per la sicurezza per convalidare e assegnare priorità agli avvisi. In questo modo, gli analisti devono dedicare meno tempo a elaborare i falsi positivi e possono concentrarsi sulle minacce reali.

Risoluzione più rapida dell'attacco: Taegis mette automaticamente in correlazione gli eventi nell'endpoint, nella rete e negli ambienti cloud, al fine di determinare la root cause di un attacco.

Tutte le indagini in un'unica piattaforma: Taegis raccoglie i dati in tutto l'ambiente e integra un toolkit completo per la ricerca delle minacce, che include anche i TTP MITRE ATT&CK. Con questi strumenti, gli analisti possono avere una visione olistica dell'infrastruttura di sicurezza e possono eseguire indagini dall'interno della piattaforma, senza dover unire manualmente i dati o passare da uno strumento all'altro.

Collaborazione più veloce e intelligente: Le funzionalità flessibili di ricerca e reporting consentono una collaborazione ottimale e processi decisionali più rapidi che si traducono in indagini più veloci. Tutto ciò consente agli analisti di collegare rapidamente le informazioni rilevanti e di condividerle con altri per migliorare la collaborazione sulle indagini con commenti, aggiunta o rimozione di dati correlati e modifica dello stato.

DELL PROSUPPORT FOR SOFTWARE

La soluzione Dell Endpoint Security Software include il supporto di Dell. Con Dell ProSupport for Software, tecnici altamente qualificati e certificati sono disponibili 24x7 per fornire un supporto per software completo, garantendo la massima tranquillità ai clienti.

Contattare gli esperti per la sicurezza degli endpoint Dell dedicati all'indirizzo endpointsecurity@dell.com per saperne di più sui prodotti Dell SafeGuard and Response che possono migliorare il profilo di sicurezza dell'azienda

Requisiti di sistema: Console Taegis XDR: essendo un'applicazione nativa per il cloud, richiede un browser moderno come Chrome, Edge o Firefox. Sistemi supportati per l'agent Taegis XDR: Windows 10, 11; Windows Server 2016 e 2019 (Microsoft Windows), MacOS Catalina 10.15, Big Sur 11, Monterey 12 (+M1) (macOS), CentOS 7, Amazon Linux 2, Ubuntu 18.04 (altri).

Ulteriori informazioni sono disponibili sul sito DellEMC.com/endpointsecurity

Secureworks®