

Elimina l'esposizione dell'OT grazie alla soluzione di sicurezza unificata per gli ambienti OT/IT convergenti



Panoramica del prodotto

La convergenza dei sistemi di tecnologia operativa (OT) e IT, insieme alla rapida adozione delle tecnologie dell'IoT, sta trasformando i settori. Questa convergenza ottimizza i processi di produzione, promuove l'innovazione e aumenta l'efficienza attraverso analisi dei dati in tempo reale e comunicazione tra sistemi. Tuttavia, aumenta anche la superficie di attacco introducendo nuove vulnerabilità e vettori di attacco. Con l'aumento dell'interconnessione tra le reti OT e quelle IT, il potenziale per le minacce informatiche cresce, richiedendo misure di sicurezza solide per proteggersi dagli attacchi informatici e garantire l'integrità e l'affidabilità delle operazioni più importanti.

Tenable OT Security offre visibilità, sicurezza e controllo degli ambienti industriali, delle infrastrutture critiche, dei sistemi di gestione degli edifici e molto altro. Riduce i rischi aziendali e protegge le aziende dagli attacchi su tutto l'ambiente OT/IT che oggi sta rapidamente convergendo. Grazie a un approccio di indagine ibrido brevettato che consente di ottenere in modo sicuro visibilità sui dispositivi OT, IT e IoT, e sui sistemi cyber-fisici, Tenable OT Security fornisce un Asset Inventory completo in un'unica interfaccia, con una profonda consapevolezza situazionale di tutti i siti a livello globale. Dalla gestione delle vulnerabilità e dal rilevamento delle minacce al controllo della configurazione e al reporting, Tenable OT Security permette alle aziende di dare priorità alle azioni e consente ai loro team di sicurezza OT e IT di collaborare al meglio per fermare l'esposizione.

Il nostro campo d'azione

- Produzione discreta
- Energia ed elettricità
- Petrolio e gas
- Settore aerospaziale
- Settore chimico e petrolchimico
- Automazione degli edifici
- Servizi idrici
- Prodotti alimentari e bevande
- Settore farmaceutico
- Trasporti

Vantaggi principali

Conosci ogni asset OT/IT nel tuo ambiente unificato

- **Ottieni una visibilità unificata** negli ambienti OT/IT convergenti. Rimuovi i punti ciechi e chiudi i silos dove le minacce laterali possono colpire OT, IT e IoT.
- **Scopri le vulnerabilità degli asset OT e IT** e organizza per urgenza le potenziali minacce prima che vengano sfruttate. Dai priorità alla correzione e riduci l'esposizione secondo la gravità e l'impatto della vulnerabilità.

Esponi le pericolose lacune che mettono a repentaglio la tua azienda

- **Sfrutta al massimo le informazioni** combinando il monitoraggio della rete con le funzionalità avanzate di individuazione per scoprire le violazioni dei criteri, individuare comportamenti anomali e tracciare le firme ad alto rischio sulla tua superficie di attacco.
- **Controlla le modifiche alla configurazione** con un percorso di verifica completo per determinare chi ha effettuato modifiche, cosa è stato cambiato, per quale motivo e quale sia il risultato.

Ferma le esposizioni prioritarie con sicurezza

- **Metti fine alle esposizioni** con valutazioni della priorità su tutti gli asset, correzioni guidate e gestione avanzata delle configurazioni.
- **Prendi il controllo** del tuo ambiente unificato e implementa difese strategiche per prevenire lo spostamento di minacce laterali nei domini OT e IT.



Funzionalità chiave

Visibilità completa degli asset

Tenable OT Security automatizza la scoperta degli asset e crea mappe visuali degli asset per una vista unificata degli asset di rete, comprese le stazioni di lavoro, i server, HMI, storici, PLC, RTU, IED e i dispositivi IoT. I motori di connessione si concentrano sulle applicazioni che gestiscono i dispositivi IoT e assicurano un inventario completo. Gestisci i tuoi asset tracciando le versioni del firmware e del sistema operativo, le configurazioni interne, le applicazioni e gli utenti, i numeri seriali e la configurazione backplane per l'attrezzatura basata sia sull'OT che sull'IT.

Rilevamento avanzato di minacce e anomalie

Tenable OT Security sfrutta un motore avanzato di individuazione multipla in grado di identificare le anomalie di rete, applicare i criteri di sicurezza e tracciare i cambiamenti locali sui dispositivi con eventi ad alto rischio; il tutto con la massima precisione. Con l'individuazione delle minacce basate sul dispositivo, le aziende possono identificare i problemi sui dispositivi inattivi per individuare e mitigare gli eventi di rischio negli ambienti OT/IT. Grazie alla flessibilità, gli utenti possono personalizzare e regolare i metodi di individuazione per adattarli ai bisogni specifici dei loro ambienti. Le funzionalità di risposta alle minacce sono migliorate con avvisi contestualizzati e un percorso di verifica completo per la risposta agli incidenti e un'indagine delle minacce.

Tracciamento delle modifiche di configurazione

Con il Controllo della configurazione di Tenable OT è possibile tener traccia delle modifiche eseguite dal malware e dagli utenti attraverso la rete o direttamente su un dispositivo. Tenable fornisce una cronologia delle modifiche apportate alle configurazioni dei dispositivi, fra cui specifici segmenti di diagramma a contatti (ladder logic), i buffer diagnostici e le tabelle di tag. Crea un'istantanea di backup identificando "l'ultimo stato valido conosciuto" per un ripristino più rapido e per assicurare la conformità con le normative di settore.

Gestione delle vulnerabilità OT/IT basata sul rischio

Tenable OT Security utilizza un modello di punteggio VPR (Vulnerability Priority Rating) sofisticato per valutare le vulnerabilità in base al contesto e all'impatto potenziale, permettendo azioni di correzione prioritarie. Ogni asset viene valutato con dati completi che includono le versioni firmware, le ricerche proprietarie e le informazioni sulle relazioni degli asset, le esposizioni e i percorsi di attacco. Questo offre ai team tutta l'intelligenza sfruttabile di cui hanno bisogno per prendere decisioni informate e accelerare le misure di mitigazione.

Gestione degli asset automatizzati

Tenable OT Security semplifica la gestione degli asset con visibilità migliorata e informazioni sul contesto. Le scoperte ibride con query in lingua naturale offrono una gestione dell'inventario senza interruzione, permettendo un'identificazione rapida degli asset e delle esposizioni critiche degli stessi. La mappatura degli asset mostra relazioni intricate tra i dispositivi connessi fisicamente e quelli comunicanti per aiutare nella costruzione di strategie di difesa solide.

Massimizza gli investimenti attuali sulla sicurezza

Tenable OT Security è progettato per adattarsi e lavorare facilmente in diverse infrastrutture, integrandosi con gli altri prodotti Tenable oltre a strumenti per la sicurezza leader di settore come SIEM, SOAR e firewall next-gen. Tenable condivide le informazioni anche con il database di gestione della configurazione, con le piattaforme di inventario delle risorse, gli strumenti di gestione dei cambiamenti e altri ancora. La nostra API RESTful è stata progettata per agevolare l'estrazione dei dati su strumenti proprietari, offrendo una vista più coerente degli ambienti IT e OT in un'unica interfaccia.



Informazioni su Tenable

Tenable® è l'azienda della Exposure Management, che si occupa di esporre e colmare le lacune della sicurezza informatica che erodono il valore aziendale, la reputazione e la fiducia dei clienti. La sua piattaforma di gestione, basata sull'intelligenza artificiale, le informazioni e le azioni relative della sicurezza su tutta la superficie di attacco, dotando le organizzazioni di protezione contro gli attacchi alle infrastrutture IT e agli ambienti cloud, compresi gli asset più critici. Proteggendo le aziende dall'esposizione ai rischi per la sicurezza, Tenable riduce i rischi aziendali per oltre 44.000 clienti in tutto il mondo. Scopri di più su it.tenable.com.

Contatti

Invia un'email a sales@tenable.com o visita it.tenable.com/contact.