tenable | Scheda informativa

Tenable One Exposure Management Platform

L'unica piattaforma di gestione dell'esposizione con IA

Mettiti in vantaggio rispetto ai malintenzionati

Chi minaccia le organizzazioni non rispetta i silos di sicurezza. Cerca qualsiasi punto debole da sfruttare e si muove lateralmente. Tuttavia, gli strumenti a cui ci affidiamo per proteggere la superficie di attacco si concentrano sulle tecnologie in modo individuale (cloud, identità, IT, OT, IoT e applicazioni) e creano molto rumore. Manca il punto di vista di chi effettua l'attacco, che è fondamentale: una visione degli asset, delle identità e delle relazioni di rischio che permettono le violazioni in tutti i domini; ancor più importante, l'impatto sull'organizzazione, che sia sui profitti, sulla sovranità dei dati, sulla conformità o altri fattori cruciali.

Poiché è l'unica piattaforma di gestione dell'esposizione end-to-end, Tenable One unifica radicalmente la visibilità, le informazioni e le azioni di sicurezza su tutta la superficie di attacco. Aiuta le organizzazioni moderne a isolare e sradicare le esposizioni informatiche prioritarie dalle infrastrutture di IT agli ambienti cloud, fino alle infrastrutture cruciali e tutto ciò che risiede nel mezzo. Con Tenable One, le aziende possono distinguere all'interno di un rumoroso mare di scoperte quali combinazioni di rischi costituiscono una vera esposizione. Questo porta a una maggiore produttività del personale esistente e a investimenti più informati che aiutano a ottimizzare la posizione di sicurezza generale e la conformità.

One: la scelta vincente

Tenable One è una piattaforma unica progettata per risolvere la principale sfida della sicurezza moderna: un approccio profondamente diviso nell'individuare e contrastare il rischio informatico.

Visibilità unificata

Ottieni la vista aziendale del rischio informatico sull'intera superficie di attacco con un'unica soluzione, esponendo le lacune che rendono più vulnerabili agli attacchi in tutti i tipi di asset e percorsi.

Informazioni aggregate

Analizza in modo unificato il contesto e le informazioni del rischio informatico su tutta la superficie di attacco, unisci i punti per identificare le esposizioni che minacciano il valore, la reputazione e l'affidabilità della tua attività.

Un'azione coordinata

Unisci i leader aziendali e i team di sicurezza per combattere insieme, mobilitando tutte le risorse aziendali per trovare e correggere le esposizioni dove la probabilità di un attacco e l'impatto sull'azienda sono maggiori.

Vantaggi principali

- Comunica con semplicità la posizione di rischio al consiglio di amministrazione, alle business unit e ai team.
- Riduci sensibilmente le esposizioni informatiche dimostrando conformità.
- Consolida gli strumenti e dai priorità agli investimenti che hanno l'impatto maggiore.
- Ottimizza la produttività, riduci il tasso di abbandono del personale e aumenta le risorse e le competenze limitate.

"Essere in grado di vedere la nostra esposizione di sicurezza in un'unica vista comune è cruciale. Tenable One ci aiuta a consolidare soluzioni mirate costose e ottenere una visibilità completa migliore su tutta la superficie di attacco sotto un'unica lente.

La capacità di report all'interno di Tenable One ci permette inoltre di svolgere le nostre attività d'impresa. Che si tratti di comunicare la nostra posizione sulla sicurezza informatica al consiglio di amministrazione o creare un piano d'azione dettagliato per il team, possiamo impostare la "modalità facile" per fornire report adatti a ogni tipo di pubblico."

Deputy CISO,
Fortune 500 Enterprise

Visibilità unificata

Scopri l'intera superficie di attacco

Elimina i punti ciechi con un'investigazione completa della tua superficie di attacco, compresi gli asset rivolti all'interno e all'esterno: cloud, IT, OT, IoT, container, Kubernetes, applicazioni e asset nascosti; oltre alle identità delle persone e dei dispositivi.

Individua i rischi legati agli asset e alle identità

Valuta i tuoi asset e le identità per ottenere una vista completa delle tre varietà di rischio che rendono possibile ogni violazione: vulnerabilità, configurazioni errate e privilegi eccessivi, sia on-premise che in tutto il cloud.

Unifica l'inventario degli asset

Visualizza gli asset e le identità su tutta la superficie di attacco end-to-end in un'unica vista centrale, insieme a un'intelligenza profonda degli asset che comprende la loro configurazione, i dettagli, le debolezze, i tag, l'ACR (Asset Critically Rating), l'AES (Asset Exposure Score), i percorsi di attacco relativi e altro ancora.

Informazioni aggregate

Normalizza la classificazione dei rischi in tutti i domini

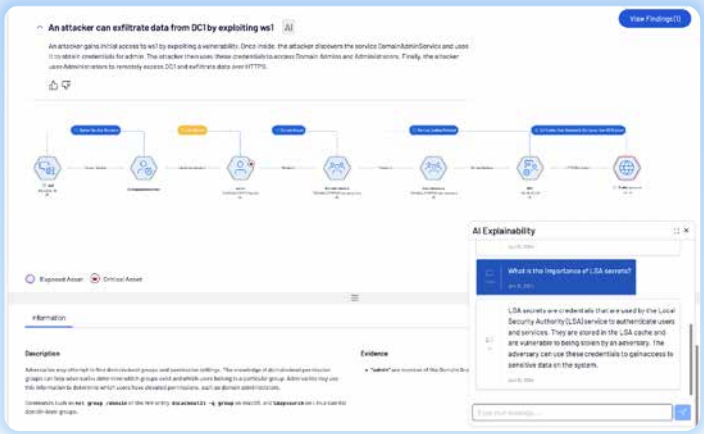
Sfrutta un approccio coerente per valutare il rischio secondo i tipi di rischio e le classi degli asset. Un VPR (Vulnerability Priority Rating) valuta le variabili statiche e dinamiche nel panorama delle minacce in costante evoluzione, compresa la presenza di codice sfruttabile e la frequenza con cui i malintenzionati lo utilizzano al fine di adattare continuamente la classificazione dei rischi. VPR lavora con ACR per calcolare e fornire un AES generale per ogni asset, permettendo ai team di valutare rapidamente quali asset presentino la minaccia più grave per l'azienda al fine di prioritizzarne la correzione.

Dai la priorità ai percorsi di attacco che portano agli asset più importanti

L'analisi dei percorsi di attacco fornisce una comprensione dettagliata degli asset, delle identità e delle relazioni sui rischi che possono essere sfruttate dai malintenzionati per compromettere gli asset più importanti e di valore: quegli asset con un impatto materiale potenziale molto alto sull'azienda. Visualizza un elenco dei percorsi di attacco secondo priorità e cerca facilmente le caratteristiche dei percorsi di attacco utilizzati nelle violazioni ad alto profilo (ad es. SolarWinds), visualizza tecniche MITRE specifiche e ottieni spiegazioni chiare per ogni passaggio con l'IA generative e le query in linguaggio naturale.

Migliora la correzione con i punti di blocco

Invece che cercare e correggere ogni scoperta o ogni passaggio in un percorso di attacco, accedi rapidamente alle informazioni dei punti di blocco grazie alla guida per la correzione. Con la visibilità all'interno dei percorsi di attacco e i punti di blocco, il personale addetto alla sicurezza può vedere quali correzioni rimuoveranno il numero maggiore di percorsi di attacco verso gli asset più importanti, riducendo il rumore non necessario che porta all'abbandono e a una minore produttività.



Un'azione coordinata

Ottieni una vista allineata dalle esposizioni aziendali

Le schede di esposizione generali e personalizzate all'interno di Lumin Exposure View rendono possibili azioni di sicurezza concentrate fornendo una vista della posizione di sicurezza aziendale chiara e allineata all'azienda, organizzata per dominio o per qualsiasi altro raggruppamento logico degli asset. Ad esempio, le aziende possono costruire schede di esposizione personalizzate per un servizio o un processo aziendale cruciale oppure per fornitore, come un produttore di dispositivi. Un CES (Cyber Exposure Score) unisce i punteggi AES individuali per tutti gli asset all'interno di una scheda di esposizione, fornendo una quantificazione su misura della posizione di sicurezza.

Traccia i trend e ottimizza gli investimenti

Le visualizzazioni dei trend, il tracciamento SLA e la Tag Performance aiutano a rispondere a domande fondamentali come:

- Come è cambiata la nostra posizione di sicurezza nel tempo?
- Quali domini o aree funzionali richiedono un investimento maggiore?
- Stiamo rispettando i nostri impegni sulla correzione?

Questo permette una comunicazione migliore e un allineamento strategico degli obiettivi oltre a una spesa del budget con le parti interessate e i team.

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, unifica la visibilità, 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.

082024