tenable.cs
cloud security

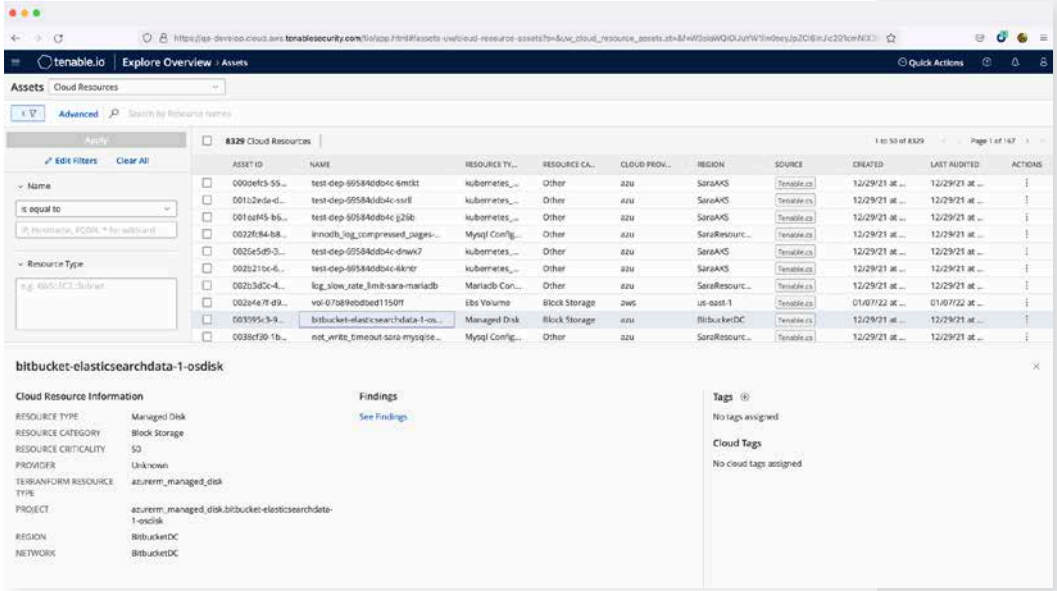
SCHEDA INFORMATIVA

PIATTAFORMA TENABLE DI PROTEZIONE DELLE APPLICAZIONI CLOUD-NATIVE

PROTEGGI OGNI FASE DAL **CODICE AL CLOUD**

Tenable.cs offre in un'unica piattaforma la piena e continua visibilità delle esposizioni in tutte le tue risorse e asset cloud. Grazie a Tenable.cs puoi individuare e correggere errori di configurazione dell'infrastruttura cloud nelle fasi di progettazione, compilazione e runtime del ciclo di vita di sviluppo del software. Imposta protezioni nelle pipeline DevOps per evitare che le esposizioni raggiungano la produzione. Monitora costantemente gli ambienti AWS, Azure e GCP per assicurarti che ogni modifica al runtime rispetti i criteri e crea automaticamente richieste di unione per rimediare alle deviazioni nella configurazione.

Tenable.cs fornisce inoltre la continua visibilità sulle vulnerabilità dell'host cloud e delle immagini dei container, senza la necessità di gestire scansioni pianificate, credenziali o agenti. Gli asset cloud e le immagini dei container vengono riesaminati ogni volta che vengono aggiunti nuovi rilevamenti o distribuiti nuovi asset. Questo approccio always-on ti consente di dedicare più tempo alle vulnerabilità con la priorità più elevata e meno alla gestione delle scansioni e del software.



VANTAGGI PRINCIPALI

Previeni i problemi di sicurezza
Individua e rimuovi i difetti del cloud durante lo sviluppo, prima che possano raggiungere la produzione.

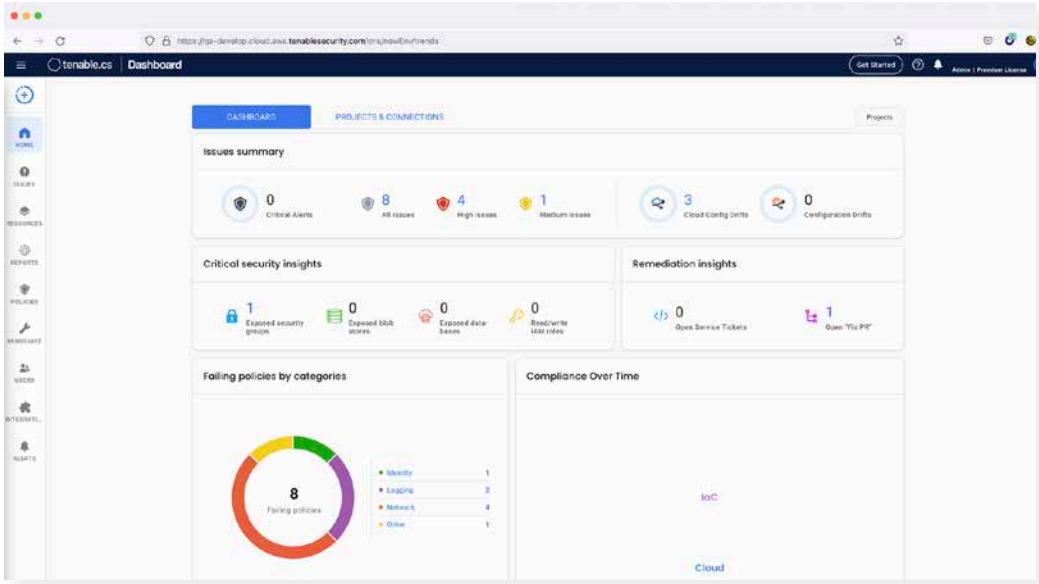
Accelera i tempi di risposta
Fornisci automaticamente le risoluzioni agli sviluppatori tramite le richieste di unione.

Applica criteri coerenti
Approfitta di oltre 1.800 criteri in tutti gli standard principali o creane di tuoi.

Migliora la collaborazione
Migliora la comunicazione tra i team DevOps, della sicurezza e delle operazioni nel cloud per una maggiore efficienza.

Ottieni una visibilità unificata
Comprendi il profilo di sicurezza degli ambienti cloud insieme a quello degli asset on-premise.

Insieme, Tenable.io e Tenable.cs consentono alle organizzazioni di individuare e correggere in modo programmato gli errori di configurazione dell'infrastruttura cloud nelle fasi di progettazione, compilazione e runtime.



Tenable.cs aiuta le organizzazioni a impostare protezioni nelle pipeline e nei flussi di lavoro automatizzati (CI/CD) per evitare che vulnerabilità o errori di configurazione non risolti raggiungano l'ambiente di runtime. Monitora l'infrastruttura distribuita in AWS, Azure e GCP per garantire che le modifiche di runtime siano coerenti e le deviazioni vengano propagate all'IaC.

FUNZIONALITÀ CHIAVE

Proteggi l'infrastruttura come codice

Verifica che non ci siano violazioni dei criteri nei modelli dell'infrastruttura come codice (IaC), tra cui Terraform, AWS CloudFormation, Azure Resource Manager e Kubernetes. Integra la sicurezza dell'infrastruttura cloud nella pipeline DevOps per evitare che eventuali problemi di sicurezza raggiungano la produzione. Rimedia rapidamente agli errori di configurazione dell'IaC direttamente dagli strumenti di sviluppo per applicare criteri nelle fasi di compilazione e runtime.

Previeni deviazioni del profilo cloud

Individua discrepanze tra l'IaC e l'ambiente cloud in esecuzione. Assicurati che l'origine di riferimento sia sempre aggiornata e applica i controlli di sicurezza in fase di runtime.

Rimedia automaticamente alle vulnerabilità

Fornisci automaticamente suggerimenti di correzione tramite richieste pull o di unione per ridurre il carico sui team di sviluppo e facilitarli negli strumenti che conoscono. Ciò garantisce di raggiungere nel minor tempo possibile la risoluzione necessaria per la conformità.

Visibilità negli asset cloud

Rileva e valuta costantemente gli asset cloud senza la necessità di installare agenti, configurare una scansione o gestire credenziali. Individua rapidamente i problemi di sicurezza non appena vengono rilevate nuove vulnerabilità e il tuo ambiente cloud cambia con l'avvio e l'interruzione di istanze.

Contestualizza i rischi

Comprendi le vulnerabilità delle applicazioni nel contesto delle loro configurazioni dell'infrastruttura per ottenere un quadro realistico del rischio che presentano. Comprendi i percorsi di violazione e stabilisci la priorità della loro risoluzione.

Regolamenta la conformità

Verifica e documenta la conformità agli standard del settore e stabilisci le best practice, come CIS, PCI e GDPR. Approfitta di oltre 1.800 criteri in 10 standard per una valutazione completa. Puoi inoltre creare criteri personalizzati basati sulle tue esigenze specifiche.

Sicurezza di Kubernetes e dei container

Ottieni visibilità sul profilo di sicurezza dell'infrastruttura e delle immagini dei container. Integra i test della sicurezza per le nuove immagini di container e configurazioni Kubernetes nelle pipeline DevOps per assicurarti che l'IaC e le nuove compilazioni siano conformi ai criteri aziendali. Visualizza i dati sulla vulnerabilità, gli inventari dei pacchetti e gli errori di configurazione di tutte le tue immagini di container e dell'infrastruttura Kubernetes. Sincronizza le immagini di container dai registri di terzi per verificarle costantemente rispetto alle nuove vulnerabilità scoperte. Proteggi le distribuzioni Kubernetes e previeni deviazioni nella configurazione.

Sicurezza del runtime per l'infrastruttura cloud

Applica criteri all'ambiente cloud in esecuzione. Gli avvisi e le correzioni in tempo reale garantiscono la conformità. I criteri sono unificati dall'IaC al cloud. Genera report per dimostrare il profilo di sicurezza sul campo nel tempo.

Per ulteriori informazioni: visita tenable.com/products/tenable-cs
Contatti: invia un'e-mail a sales@tenable.com o visita tenable.com/contact