tenable.cs
cloud security

DATENBLATT

TENABLE-PLATTFORM FÜR CLOUD-NATIVEN ANWENDUNGSSCHUTZ

ABSICHERUNG JEDES SCHRITTS **VOM CODE BIS ZUR CLOUD**

Tenable.cs bietet umfassende und kontinuierliche Transparenz über Expositionen in all Ihren Cloud-Ressourcen und -Assets in einer einzigen Plattform. Mit Tenable.cs können Sie Fehlkonfigurationen der Cloud-Infrastruktur bereits in den Design-, Build- und Runtime-Phasen Ihres Software Development Lifecycle (SDLC) erkennen und beheben. Richten Sie Schutzvorkehrungen in DevOps-Pipelines ein, um zu verhindern, dass Expositionen in Produktionsumgebungen gelangen. Überwachen Sie AWS-, Azure- und GCP-Umgebungen kontinuierlich, um sicherzustellen, dass sämtliche Runtime-Änderungen richtlinienkonform erfolgen, und erstellen Sie Merge-Requests automatisch, um Konfigurationsdrifts zu korrigieren.

Tenable.cs bietet darüber hinaus einen kontinuierlichen Einblick in Schwachstellen von Cloud-Hosts und Container-Images, ohne dass Scan-Zeitpläne, Zugangsdaten oder Agents verwaltet werden müssen. Cloud-Assets und Container-Images werden neu bewertet, wenn neue Schwachstellenerkennungen hinzugefügt und neue Assets bereitgestellt werden. Durch diesen „Always-on"-Ansatz haben Sie mehr Zeit, sich auf Schwachstellen mit der höchsten Priorität zu konzentrieren, und müssen weniger Zeit mit der Verwaltung von Scans und Software verbringen.

WICHTIGE VORTEILE

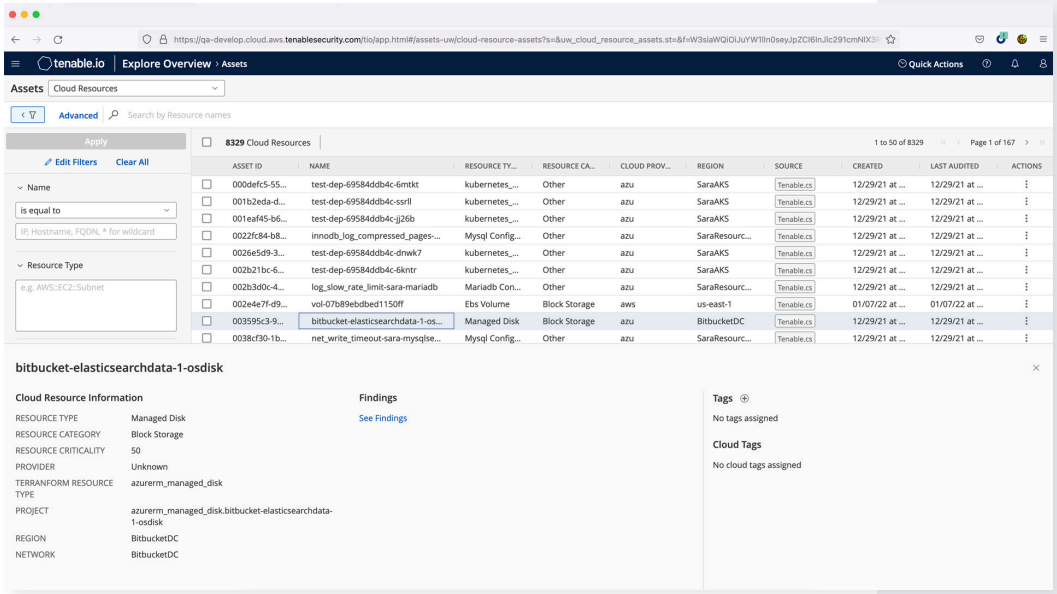
Verhindern von Sicherheitsproblemen
Identifizieren und beseitigen Sie Cloud-Sicherheitsmängel während der Entwicklung, noch bevor sie in Produktionsumgebungen gelangen.

Beschleunigte Reaktionsmaßnahmen
Stellen Sie Entwicklern Behebungsmaßnahmen mithilfe von Merge-Requests automatisch zur Verfügung.

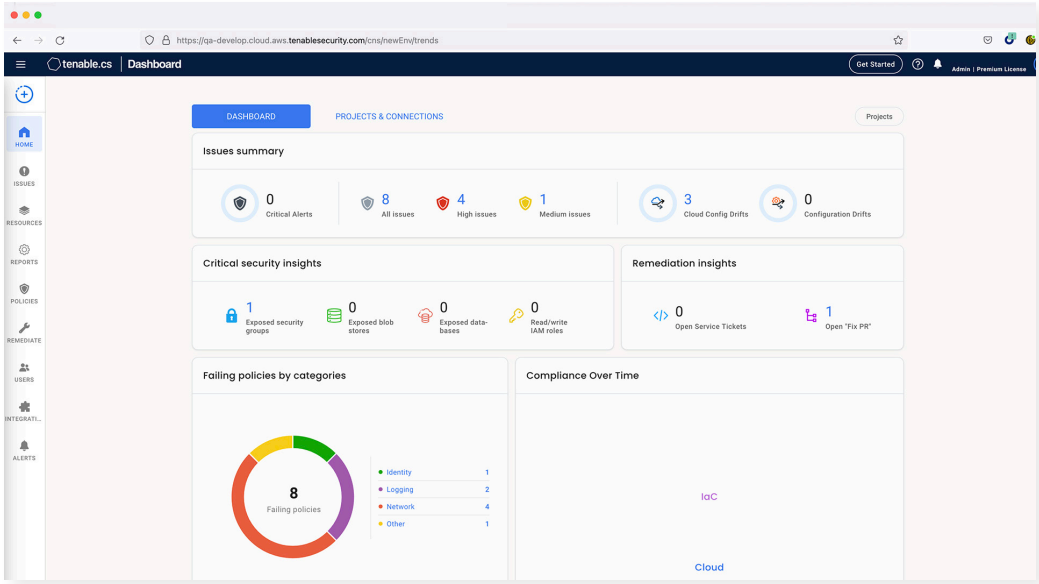
Durchsetzung einheitlicher Richtlinien
Profitieren Sie von 1.800 Richtlinien zu allen führenden Standards oder erstellen Sie Ihre eigenen.

Verbesserte Zusammenarbeit
Verbessern Sie die Kommunikation zwischen Security-, Cloud-Operations- und DevOps-Teams und profitieren Sie von größerer Effizienz.

Einheitliche Sichtbarkeit
Machen Sie sich ein Bild von der Sicherheitslage Ihrer Cloud-Umgebungen und der Ihrer On-Premise-Assets.



Mit Tenable.io innerhalb von Tenable.cs sind Unternehmen in der Lage, Fehlkonfigurationen in der Cloud-Infrastruktur in der Design-, Build- und Runtime-Phase programmgesteuert zu erkennen und zu beheben.



Mithilfe von Tenable.cs können Unternehmen Schutzvorkehrungen in Pipelines und automatisierten Workflows (CI/CD) einrichten, um zu verhindern, dass unbeseitigte Fehlkonfigurationen oder Schwachstellen in die Runtime-Umgebung gelangen. Tenable.cs überwacht in AWS, Azure und GCP bereitgestellte Infrastruktur, um zu gewährleisten, dass Runtime-Änderungen konform erfolgen und Drifts zurück an die IaC übertragen werden.

WICHTIGE FUNKTIONEN

Infrastructure as Code absichern

Bewerten Sie IaC-Vorlagen (Infrastructure as Code) – einschließlich Terraform, AWS CloudFormation, Azure Resource Manager und Kubernetes – auf Richtlinienverstöße. Integrieren Sie Cloud-Infrastruktursicherheit in die DevOps-Pipeline, um zu verhindern, dass Sicherheitsprobleme in Produktionsumgebungen gelangen. Beheben Sie IaC-Fehlkonfigurationen im Handumdrehen direkt in Entwicklungstools, um Richtlinien während der Build-Time- und Runtime-Phasen durchzusetzen.

Drift der Cloud-Sicherheitslage verhindern

Ermitteln Sie Unstimmigkeiten zwischen IaC und der laufenden Cloud-Umgebung. Stellen Sie sicher, dass Ihre Source of Truth immer auf dem neuesten Stand ist, und setzen Sie Ihre Sicherheitskontrollen zur Laufzeit durch.

Schwachstellen automatisch beheben

Entlasten Sie Ihre Entwicklungsteams und kommen Sie Entwicklern in den ihnen vertrauten Tools entgegen, indem Sie Behebungsvorschläge automatisch über Pull- oder Merge-Requests bereitstellen. Dies gewährleistet die kürzeste Zeit bis zur Behebung, um Compliance zu erzielen.

Einblick in Cloud-Assets

Ermöglicht die kontinuierliche Erfassung und Bewertung von Cloud-Assets, ohne dass Sie Agents installieren, einen Scan konfigurieren oder Zugangsdaten verwalten müssen. So können Sie Sicherheitsprobleme schnell erkennen, wenn neue Schwachstellen bekannt werden und wenn sich Ihre Cloud-Umgebung durch das Hoch- und Herunterfahren von Instanzen verändert.

Risiken kontextualisieren

Interpretieren Sie Anwendungsschwachstellen im Kontext ihrer jeweiligen Infrastrukturkonfigurationen, um sich ein genaues Bild davon zu machen, welches Risiko sie darstellen. Vollziehen Sie Angriffswege nach und priorisieren Sie deren Beseitigung.

Compliance überwachen

Prüfen und dokumentieren Sie die Einhaltung von Branchenstandards und bewährten Best Practices wie CIS, PCI und DSGVO. Nutzen Sie über 1.800 Richtlinien für 10 verschiedene Standards zur umfassenden Prüfung. Zudem besteht die Möglichkeit, benutzerdefinierte Richtlinien auf Basis Ihrer individuellen Anforderungen zu erstellen.

Kubernetes- und Container-Sicherheit

Verschaffen Sie sich Einblick in den Sicherheitsstatus Ihrer Container-Images und -Infrastruktur. Integrieren Sie Sicherheitstests für neue Container-Images und Kubernetes-Konfigurationen in DevOps-Pipelines, um zu gewährleisten, dass neue Builds und IaC den Unternehmensrichtlinien entsprechen. Zeigen Sie Schwachstellendaten, Paketverzeichnisse und Fehlkonfigurationen all Ihrer Container-Images und Kubernetes-Infrastruktur an. Synchronisieren Sie Container-Images aus Drittanbieter-Registrys, um diese kontinuierlich auf neu aufgedeckte Schwachstellen zu prüfen. Sorgen Sie für die Sicherheit von Kubernetes-Bereitstellungen und verhindern Sie Konfigurationsdrift.

Runtime-Sicherheit für Cloud-Infrastruktur

Setzen Sie Ihre Richtlinien in der laufenden Cloud-Umgebung durch, wobei die Compliance durch Warnmeldungen und Behebungsmaßnahmen in Echtzeit gewährleistet wird – mit einheitlichen Richtlinien von IaC bis hin zur Cloud. Generieren Sie Berichte, um Ihre Sicherheitslage in der Praxis im Zeitverlauf zu belegen.

Weitere Informationen: Besuchen Sie de.tenable.com/products/tenable-cs

Kontakt: Senden Sie eine E-Mail an sales-de@tenable.com oder besuchen Sie de.tenable.com/contact