tenable.cs
cloud security

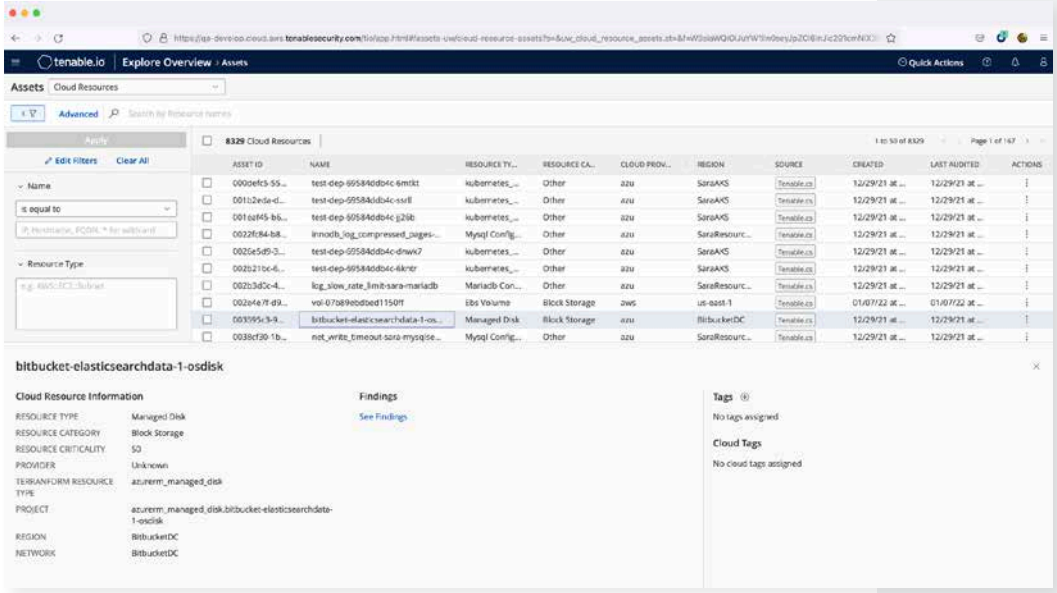
FICHE TECHNIQUE

PLATEFORME D'APPLICATION CLOUD-NATIVE DE PROTECTION TENABLE

SÉCURISER CHAQUE ÉTAPE, DU **CODE AU CLOUD**

Tenable.cs offre une visibilité complète et continue des expositions sur toutes vos ressources et assets, le tout dans une seule et même plateforme. Avec Tenable.cs, vous pouvez détecter et corriger les erreurs de configuration de l'infrastructure cloud pendant les phases de conception, de build et de runtime du cycle de vie de votre développement logiciel. Mettez en place des garde-fous dans les pipelines DevOps avant que l'exposition ne se propage vers la production. Surveillez en permanence les environnements AWS, Azure et GCP pour vous assurer que toutes les modifications du runtime sont conformes aux politiques, et créez automatiquement des merge request pour remédier aux dérives de configuration.

Tenable.cs offre également une visibilité continue des vulnérabilités de l'hébergeur cloud et de l'image de conteneur, sans qu'il soit nécessaire de gérer la planification des scans, les informations d'authentification ou les agents. Les assets cloud et les images de conteneur sont réévalués à mesure que de nouvelles détections des vulnérabilités sont ajoutées et que de nouveaux assets sont déployés. Cette approche « en continu » vous permet de consacrer plus de temps aux vulnérabilités prioritaires et moins de temps à la gestion des scans et du logiciel.



PRINCIPAUX AVANTAGES

Prévenir les problèmes de sécurité
Identifiez et supprimez les failles cloud pendant le développement avant qu'elles ne se propagent en production.

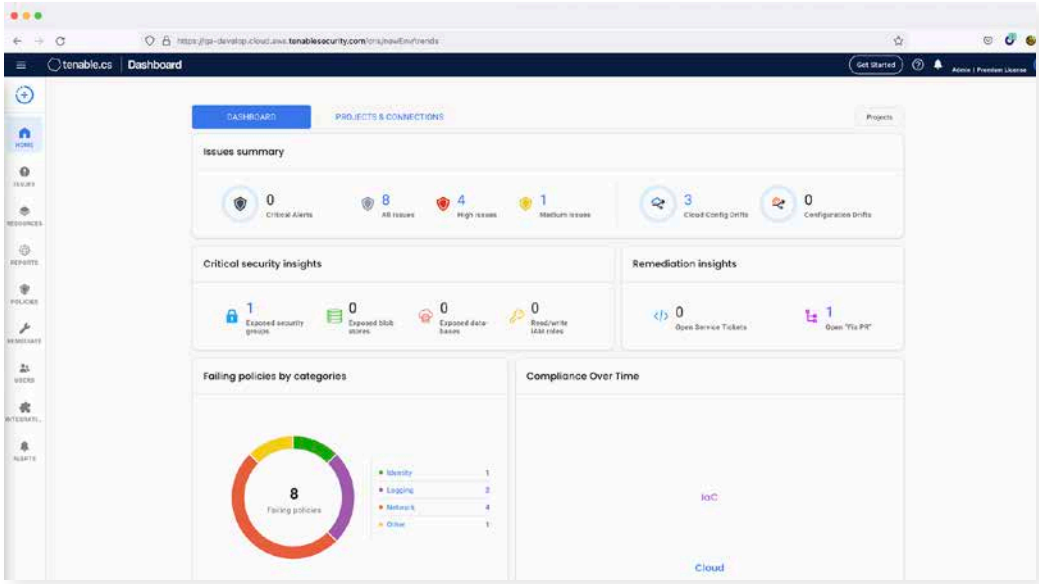
Accélérer le temps de réponse
Envoyez automatiquement les remédiations aux développeurs via des merge request.

Appliquer des politiques cohérentes
Profitez des 1 800 politiques issues des principales normes, ou créez les vôtres.

Améliorer la collaboration
Améliorez la communication entre les équipes de sécurité, d'opérations cloud et DevOps pour une plus grande efficacité.

Obtenir une visibilité unifiée
Comprenez la posture de sécurité de vos environnements cloud et de vos assets sur site.

Tenable.io au sein de Tenable.cs permet aux entreprises de détecter et de corriger programmatiquement les erreurs de configuration de l'infrastructure cloud au niveau de la conception, du build et du runtime.



Tenable.cs aide les entreprises à mettre en place des garde-fous dans les pipelines et les workflows automatisés (CI/CD), afin d'éviter que des erreurs de configuration ou des vulnérabilités non résolues ne se propagent dans l'environnement runtime. Il surveille l'infrastructure déployée dans AWS, Azure et GCP pour s'assurer que les modifications du runtime sont conformes, et que les dérives sont propagées vers l'IaC.

FONCTIONS CLÉS

Sécurisation de l'infrastructure as code

Évaluez les modèles d'infrastructure as code (IaC), notamment Terraform, AWS CloudFormation, Azure Resource Manager et Kubernetes, pour détecter les violations de politiques. Intégrez la sécurité de l'infrastructure cloud dans le pipeline DevOps pour empêcher les problèmes de sécurité de se propager dans la production. Remédiez rapidement aux erreurs de configuration IaC directement dans les outils de développement afin d'appliquer les politiques pendant le temps de build et le runtime.

Prévention de la dérive de posture cloud

Identifiez les divergences entre l'IaC et votre environnement cloud en cours. Assurez-vous que votre source d'informations fiables est toujours à jour et appliquez vos contrôles de sécurité au moment du runtime.

Application automatique d'une remédiation aux vulnérabilités

Fournissez automatiquement des suggestions de correction via des pull request et des merge request pour réduire la charge de travail de vos équipes de développement, et communiquer avec les développeurs via des outils qu'ils connaissent. Cela permet d'accélérer la remédiation pour atteindre la conformité.

Visibilité sur les assets du cloud

Découvrez et évaluez vos assets cloud en continu sans qu'il soit nécessaire d'installer des agents, de configurer des scans ni de gérer des identifiants. Détectez rapidement les problèmes de sécurité lorsque de nouvelles vulnérabilités sont révélées et que votre environnement change avec des instances qui évoluent constamment.

Contextualisation des risques

Comprenez les vulnérabilités des applications dans le contexte de configuration de leur infrastructure, afin d'obtenir une représentation réelle du risque qu'elles présentent. Comprenez les chemins de violation et priorisez leur remédiation.

Gouvernance de la conformité

Évaluez et documentez la conformité aux normes du secteur et mettez en place les meilleures pratiques, telles que CIS, PCI et RGPD. Profitez de plus de 1 800 politiques réparties sur 10 normes pour une évaluation complète. Vous pouvez également créer des politiques personnalisées en fonction de vos besoins individuels.

Kubernetes et Container Security

Obtenez plus de visibilité sur la posture de sécurité de vos images de conteneur et de votre infrastructure. Intégrez des tests de sécurité pour les nouvelles images de conteneur et des configurations Kubernetes dans les pipelines DevOps pour vous assurer que les nouveaux builds et l'IaC sont conformes aux politiques de l'entreprise. Consultez les données sur les vulnérabilités, les inventaires de paquets et les mauvaises configurations de toutes vos images de conteneur et de votre infrastructure Kubernetes. Synchronisez les images de conteneur à partir de registres tiers pour les évaluer en continu afin de détecter les vulnérabilités récemment découvertes. Sécurisez les déploiements Kubernetes et évitez les dérives de configuration.

Sécurité du runtime pour l'infrastructure cloud

Appliquez vos politiques dans votre environnement cloud. Les alertes en temps réel et la remédiation assureront la conformité. Les politiques sont unifiées de l'IaC au cloud. Générez des rapports pour démontrer votre posture de sécurité sur le terrain au fil du temps.

Pour plus d'informations : rendez-vous sur fr.tenable.com/products/tenable-cs

Contact : envoyez un e-mail à sales@tenable.com ou rendez-vous sur fr.tenable.com/contact