CROWDSTRIKE

FALCON HORIZON GESTION DU NIVEAU DE SÉCURITÉ DU CLOUD

Arrêtez net les intrusions dans le cloud grâce à une visibilité unifiée, à la détection des menaces et à une surveillance et un contrôle de la conformité continus pour les environnements multiclouds

VOIR PLUS, EN SAVOIR PLUS, FAIRE PLUS

L'adoption du cloud a révolutionné l'approche commerciale des entreprises et le développement des applications modernes. Aujourd'hui, le cycle de vie du développement d'applications privilégie la rapidité de mise sur le marché, ce qui oblige les équipes de développement à concevoir des applications natives au cloud reposant sur une infrastructure programmable qui permet aux entreprises de modifier et reconfigurer l'infrastructure cloud à la volée.

Cette évolution présente de nouveaux défis qui compliquent considérablement la tâche des équipes de sécurité. Cela se traduit par une mauvaise visibilité et un contrôle déficient des ressources cloud, des approches fragmentées de la détection et de la prévention des erreurs de configuration, un nombre croissant d'incidents de sécurité et une incapacité à assurer la conformité.

Falcon Horizon simplifie la gestion du niveau de sécurité du cloud tout au long du cycle de vie du développement des applications, quel que soit le cloud, ce qui vous permet de déployer des applications dans le cloud en toute sécurité, de façon plus rapide et efficace. La plateforme native au cloud CrowdStrike Falcon® propose une visibilité sur l'ensemble de votre infrastructure cloud, une surveillance continue des erreurs de configuration et une détection proactive des menaces, permettant ainsi aux équipes DevSecOps de corriger les problèmes plus rapidement et d'être plus productives.

PRINCIPAUX AVANTAGES

- Visibilité multicloud complète avec une source d'informations fiables unique pour les ressources cloud
- Prévention automatique des erreurs de configuration du cloud et des vulnérabilités des applications
- Évaluation de la sécurité des comptes cloud et élimination des infractions à la conformité
- Réduction de la lassitude face aux alertes répétées et accélération de la réponse à incidents
- Amélioration de la qualité du code et raccourcissement du cycle de distribution
- Protection native au cloud sans agent

FALCON HORIZON
GESTION DU NIVEAU DE SÉCURITÉ DU CLOUD

PRINCIPAUX AVANTAGES

DÉCOUVERTE ET VISIBILITÉ

Découverte et visibilité de l'infrastructure et des ressources cloud :

- Accédez à une source d'informations fiables unique pour les actifs cloud et les configurations de sécurité des environnements et comptes multiclouds.
- Découvrez automatiquement les ressources cloud et les détails lors du déploiement, notamment les erreurs de configuration, les métadonnées et les informations de mise en réseau, de sécurité et de contrôle d'accès, ainsi que les activités de modification. Services pris en charge :

AWS		
ACM	EKS	RDS
API Gateway v1	ElastiCache	Redshift
CloudTrail	ELB	Route 53
CloudFront	EMR	S3
CloudFormation	GuardDuty	SES
Config	IAM	SNS
DynamoDB	Kinesis	SQS
EBS	KMS	SSM
EC2	Lambda	VPC
ECR	NLB/ALB	

Azure	
Active Directory (AD)	Kubernetes Service
App Service	Load Balancer
Container Registry	Surveillance
Disque	Groupes de sécurité réseau
Service de fichiers	PostgreSQL
Identité	Machine virtuelle SQL Server
Coffres de clés	Compte de stockage

- Gérez les règles des groupes de sécurité pour les comptes, les projets, les régions et les réseaux virtuels depuis une console unique.
- Obtenez un aperçu de tous les appels d'API de plan de contrôle et identifiez les risques de sécurité au sein des clusters Kubernetes gérés.
- Identifiez les ressources cloud non protégées par Falcon Horizon.

GESTION ET CORRECTION DES ERREURS DE CONFIGURATION

Élimination des risques de sécurité et accélération du processus de distribution :

- Comparez les configurations des applications cloud aux références de l'entreprise et du secteur afin d'identifier les brèches et de les corriger en temps réel.
- Corrigez les problèmes qui exposent les ressources cloud, p. ex. les erreurs de configuration, les ports IP ouverts et les modifications non autorisées, à l'aide de mesures correctives guidées et de garde-fous permettant aux développeurs d'éviter les erreurs critiques.
- Surveillez le stockage pour vous assurer que les autorisations sont sécurisées et ne sont pas accessibles au public.
- Empêchez les utilisateurs de mettre votre entreprise en péril en automatisant la détection et la correction des risques liés à l'identité dans Azure.
- Assurez-vous que les groupes, utilisateurs et applications Azure AD disposent des autorisations appropriées grâce aux nouveaux rapports **Identity Analyzer**.
- Résolvez les problèmes plus rapidement et réduisez la lassitude face aux alertes répétées grâce à une gestion améliorée des règles pour les comptes cloud, les régions ou des ressources spécifiques.
- Surveillez les instances de base de données et vérifiez que la haute disponibilité, les sauvegardes, e chiffrement et les groupes de sécurité sont activés pour limiter l'exposition.

ÉLIMINATION DES ANGLES MORTS EN MATIÈRE DE SÉCURITÉ GRÂCE À FALCON HORIZON

Unification de la visibilité et du contrôle dans les environnements multiclouds : Falcon Horizon offre une découverte et une visibilité continues des actifs natifs au cloud, et fournit du contexte et des informations précieuses sur le niveau de sécurité global et les actions nécessaires pour prévenir les incidents de sécurité potentiels.

Prévention des erreurs de configuration du cloud et des infractions à la conformité : Falcon Horizon assure une surveillance intelligente des ressources cloud afin de détecter de manière proactive les erreurs de configuration, les vulnérabilités et les menaces de sécurité, et offre des fonctionnalités de correction guidée pour remédier aux risques de sécurité et permettre aux développeurs d'éviter les erreurs coûteuses et d'assurer la conformité dans les environnements multiclouds.

Réduction de la lassitude face aux alertes répétées grâce à une détection des menaces ciblée : Falcon Horizon surveille en permanence les anomalies et les activités suspectes, et s'intègre de manière transparente aux solutions SIEM, permettant ainsi aux équipes de sécurité de gagner en visibilité, de hiérarchiser les menaces, de réduire la lassitude face aux alertes répétées en éliminant celles qui ne sont pas pertinentes, et de résoudre les problèmes plus rapidement.

FALCON HORIZON
GESTION DU NIVEAU DE SÉCURITÉ DU CLOUD

DÉTECTION DES MENACES EN TEMPS RÉEL

Détection proactive des menaces tout au long du cycle de développement des applications :

- Faites le tri dans les alertes de sécurité des environnements multiclouds grâce à une approche ciblée de l'identification et de la gestion des menaces.
- Réduisez considérablement le nombre d'alertes en vous concentrant sur les domaines que les cyberadversaires sont le plus susceptibles d'exploiter.
- Priorisez les vulnérabilités en fonction de votre environnement et empêchez le code vulnérable d'atteindre la phase de production.
- Surveillez en permanence les activités malveillantes, les comportements non autorisés et l'accès aux ressources cloud grâce à la détection des menaces en temps réel.

CONTRÔLE CONTINU DE LA CONFORMITÉ

Évaluation de la sécurité des comptes cloud et élimination des infractions à la conformité :

- Contrôlez en permanence l'état de conformité de toutes vos ressources cloud à partir d'une console unique.
- Bénéficiez d'un rapport détaillé basé sur les références CIS vous permettant d'évaluer la sécurité des comptes cloud par rapport aux références CIS de Docker et Kubernetes.
- Identifiez les violations des règles et prenez des mesures immédiates pour les corriger.

INTÉGRATION DES PROCESSUS DEVSECOPS

Gestion native au cloud et sans agent du niveau de sécurité permettant de réduire la charge administrative et d'éliminer les frictions et la complexité associées à la multiplication des fournisseurs et des comptes multiclouds :

- Bénéficiez d'une visibilité et d'un contrôle centralisés sur toutes les ressources cloud afin de garantir que les équipes DevOps et en charge des opérations de sécurité disposent d'une source d'informations fiables unique.
- Offrez aux équipes de sécurité les moyens d'empêcher les actifs compromis de progresser dans le cycle de vie des applications.
- Optimisez la visibilité sur les opérations de sécurité et bénéficiez d'informations et de contexte sur les erreurs de configuration et les infractions aux règles pour une réponse aux incidents accélérée, grâce à l'intégration à la solution SIEM.
- Bénéficiez d'une intégration et d'une correction plus rapides au sein des outils DevOps et de collaboration que vous utilisez déjà (messagerie électronique, Slack, PagerDuty, etc.) grâce à l'API unique.
- Favorisez l'alignement et une compréhension commune au sein des équipes chargées des opérations de sécurité, des tâches DevOps et de l'infrastructure grâce aux rapports et aux tableaux de bord.

À PROPOS DE CROWDSTRIKE

CrowdStrike, leader mondial de la cybersécurité, redéfinit la sécurité pour l'ère du cloud en proposant une plateforme de protection des endpoints conçue spécifiquement pour empêcher les compromissions. L'architecture à agent léger unique de la plateforme CrowdStrike Falcon® s'appuie sur l'intelligence artificielle à l'échelle du cloud pour offrir une visibilité et une protection en temps réel au sein de l'entreprise et prévenir les attaques sur les endpoints, qu'ils soient connectés ou non au réseau. Optimisé par la base de données propriétaire CrowdStrike Threat Graph®, CrowdStrike Falcon met en corrélation en temps réel plus de quatre billions d'événements liés aux endpoints identifiés chaque semaine dans le monde, qui viennent enrichir l'une des plateformes de données les plus avancées au monde en matière de sécurité.

Profiter d'un essai gratuit
de notre antivirus de nouvelle génération

Pour en savoir plus, consultez le site **crowdstrike.fr**.