Guide CrowdStrike

CROWDSTRIKE

GUIDE DE DÉMARRAGE RAPIDE POUR LA SÉCURISATION DES APPLICATIONS NATIVES AU CLOUD

GUIDE DE DÉMARRAGE RAPIDE POUR LA SÉCURISATION DES APPLICATIONS NATIVES AU CLOUD

Aujourd'hui, le cycle de vie des applications privilégie la rapidité, ce qui oblige les équipes cloud à concevoir des applications natives au cloud reposant sur une infrastructure programmable qui permet aux entreprises de modifier et reconfigurer leur infrastructure cloud à la volée. Par ailleurs, les processus d'intégration/distribution continues (CI/CD) introduisent une automatisation et une surveillance continues tout au long du cycle de vie de l'application, de l'intégration et des tests à la distribution et au déploiement, permettant ainsi d'accélérer l'innovation.

Lors de la migration vers le cloud, il est absolument essentiel d'accorder une attention toute particulière aux dispositifs de blocage et aux tâches de correction des menaces de sécurité. En effet, vous partagerez vos données d'entreprise avec votre fournisseur de services et/ou les stockerez dans le centre de données de celui-ci.

Pour garantir la sécurité de vos données, de nombreux facteurs de sécurité doivent être pris en compte, qu'il s'agisse du partage des responsabilités ou de la conformité des normes de sécurité du fournisseur avec vos exigences. La tâche peut paraître insurmontable, surtout si vous n'êtes pas un expert en sécurité.

C'est pourquoi nous avons compilé un guide de démarrage rapide pour vous aider à sécuriser les applications natives au cloud.

1. **Mettez en œuvre l'authentification multifacteur pour l'utilisateur root et les utilisateurs IAM :** L'authentification multifacteur constitue une étape essentielle de la sécurisation des environnements cloud. Elle peut dissuader les cyberattaquants qui parviennent à compromettre les identifiants d'accès à l'environnement, sans toutefois réussir à compromettre le dispositif d'authentification multifacteur qui leur est associé. De plus, dans AWS, l'authentification multifacteur appliquée à l'utilisateur root complique la récupération du compte par les cyberattaquants, ce qui renforce encore la sécurité.

2. **Appliquez des règles de mots de passe IAM forts :** Les règles de mots de passe forts peuvent empêcher les utilisateurs d'être compromis lors de fuites de hachages ou d'attaques en force. Un mot de passe fort est essentiel à la sécurité de base des environnements cloud.

3. **Activez la journalisation globale des API :** L'activation de services tels qu'AWS CloudTrail est cruciale pour la sécurité des environnements cloud. En effet, elle permet de suivre, traiter et stocker tous les événements qui se produisent dans votre environnement cloud.

4. **Utilisez les services de gestion des secrets appropriés pour le stockage des secrets :** Des services tels que AWS Systems Manager Parameter Store et AWS Secrets Manager permettent de stocker et de récupérer les valeurs secrètes en toute sécurité. Il est recommandé d'utiliser ces types de services plutôt que stocker les secrets directement dans du code, des variables d'environnement ou d'autres endroits où ils peuvent être consultés en clair.

5. **Chiffrez toutes les données :** Certains fournisseurs de services cloud, tels que GCP, mettent en œuvre le chiffrement universel par défaut, mais ce n'est pas le cas de tous. Pour des raisons de conformité et de sécurité, il convient de chiffrer les données au repos et en transit avec les contrôles appropriés fournis par le fournisseur de services cloud.

6. **Activez et surveillez les services de surveillance de la sécurité :** Des services tels qu'AWS GuardDuty ou GCP Event Threat Detection identifient les activités potentiellement malveillantes dans l'environnement. Ces services doivent être activés et surveillés correctement pour garantir l'identification des activités malveillantes.

7. **Procédez à des sauvegardes automatiques *et* manuelles :** Il est important d'utiliser des fonctionnalités de sauvegarde automatiques et manuelles pour les services de données, tels qu'AWS Simple Storage Service (S3), AWS Relational Database Service (RDS) et AWS Elastic Block Store (EBS). Les sauvegardes automatiques garantissent que les données sont sauvegardées de manière régulière sans intervention de l'utilisateur, tandis que les sauvegardes manuelles fournissent l'assurance supplémentaire que les données ne seront pas perdues en cas de problème avec les sauvegardes automatiques.

8. **Appliquez le principe du moindre privilège :** En n'accordant aux utilisateurs que les autorisations nécessaires à l'exécution de leurs tâches et rien d'autre, vous vous assurez que le rayon d'action d'un compte compromis est réduit au minimum. En outre, le principe du moindre privilège réduit le risque de menaces internes et même le risque d'appels d'API accidentels potentiellement destructeurs.

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.

SÉCURITÉ DU CLOUD CROWDSTRIKE

Conception, mise en œuvre, sécurisation

FALCON CLOUD WORKLOAD PROTECTION

Offre une protection complète contre les compromissions dans les environnements cloud privés, publics, hybrides et multiclouds, permettant aux clients d'adopter et de sécuriser rapidement de nouvelles technologies indépendamment du type de charge de travail.

FALCON HORIZON™

Offre une visibilité multicloud, et assure une surveillance continue, la détection des menaces et la conformité, permettant ainsi aux équipes DevOps de déployer des applications de manière plus rapide et efficace, pour une gestion du niveau de sécurité du cloud en toute simplicité.

SÉCURITÉ DES CONTENEURS

Accélère les tâches critiques de détection, d'investigation et de chasse aux menaces effectuées sur les conteneurs, y compris sur les conteneurs éphémères après leur mise hors service, permettant ainsi aux équipes de sécurité de protéger les conteneurs à la vitesse requise par les tâches DevOps sans ajouter de friction.

ÉVALUATION DE LA SÉCURITÉ DU CLOUD

Permet de tester et d'évaluer votre infrastructure cloud afin de déterminer si les niveaux de sécurité et de gouvernance appropriés ont été mis en place pour contrer les problèmes de sécurité.