Guida CrowdStrike

CROWDSTRIKE

GUIDA RAPIDA PER PROTEGGERE LE APP CLOUD NATIVE

GUIDA RAPIDA PER PROTEGGERE LE APP CLOUD NATIVE

Nel moderno ciclo di vita delle applicazioni viene data grande importanza alla velocità. Gli sviluppatori che lavorano per il cloud devono costruire applicazioni cloud native supportate da un'infrastruttura programmabile che consenta alle aziende di rimodulare e riconfigurare l'infrastruttura cloud al volo. In più, l'innovazione è accelerata dall'adozione del metodo CI/CD per la distribuzione frequente delle app, che prevede l'introduzione dell'automazione e del monitoraggio continui nelle varie fasi della vita delle applicazioni: integrazione, test, distribuzione e deployment.

Quando si prevede di passare alla modalità cloud, è fondamentale rendersi conto che la gestione della sicurezza è uno dei compiti più importanti da affrontare perché i dati aziendali saranno condivisi con il proprio service provider e probabilmente collocati in data center di sua proprietà.

Per garantire la sicurezza dei dati, è necessario valutare vari fattori che spaziano dalla responsabilità condivisa fino al livello di affidabilità degli standard di sicurezza adottati dal provider. Può sembrare un'impresa titanica, soprattutto per chi non è un esperto di sicurezza.

Per questi casi abbiamo redatto una guida veloce che aiuta a proteggere le applicazioni cloud native.

1. **Imporre l'autenticazione a più fattori (MFA) per l'utente root e gli utenti IAM:** è un requisito irrinunciabile per mettere in sicurezza gli ambienti cloud. L'autenticazione a più fattori scoraggia gli attaccanti in grado di sottrarre le credenziali di accesso all'ambiente ma non abbastanza sofisticati per compromettere il dispositivo MFA associato alle credenziali. In AWS, inoltre, l'attivazione dell'autenticazione a più fattori sull'utente root fornisce un ulteriore livello di sicurezza perché rende più difficile compromettere gli account.

2. **Imporre l'uso di password complesse IAM:** questo tipo di policy aiuta a evitare le compromissioni favorite dal furto delle password e gli attacchi brute force. L'uso di password complesse è un requisito essenziale per garantire la sicurezza di base degli ambienti cloud.

3. **Abilitare la registrazione delle API a livello globale:** l'attivazione di AWS CloudTrail e servizi analoghi è essenziale per garantire la sicurezza dell'ambiente cloud perché consente di monitorare, memorizzare e reagire a tutti gli eventi che si verificano.

4. **Utilizzare specifici servizi di storage delle chiavi segrete:** servizi quali Parameter Store di AWS Systems Manager e AWS Secrets Manager consentono di memorizzare e recuperare le chiavi segrete in tutta sicurezza. È importante scegliere questi servizi rispetto a memorizzare le chiavi segrete direttamente nel codice, nelle variabili di ambiente o in qualsiasi altra entità dove possono essere visualizzate sotto forma di testo semplice.

5. **Criptare qualsiasi dato:** alcuni cloud provider, come GCP, criptano automaticamente tutti i dati, ma altri non lo fanno. Per questioni di sicurezza e compliance, sia i dati a riposo sia i dati in transito devono essere criptati attraverso i controlli messi a disposizione dal cloud provider.

6. **Abilitare e monitorare costantemente i servizi di rilevamento delle minacce:** servizi quali AWS GuardDuty e GCP Event Threat Detection individuano le potenziali attività maligne in corso nell'ambiente. Per fare in modo che i comportamenti non autorizzati vengano rilevati, è necessario abilitare e monitorare correttamente questi servizi.

7. **Eseguire backup automatici e manuali:** è importante eseguire il backup dei dati utilizzando servizi automatici e manuali quali AWS Simple Storage Service (S3), AWS Relational Database Service (RDS) e AWS Elastic Block Store (EBS). Automatizzando i backup ci si assicura che i dati vengano archiviati con regolarità anche in assenza dell'intervento dell'utente, mentre i backup manuali rappresentano una garanzia supplementare in caso di malfunzionamento dei backup automatici.

8. **Utilizzare il principio del privilegio minimo:** concedendo agli utenti solo i diritti minimi necessari allo svolgimento delle loro mansioni si riesce a contenere l'onda d'urto della compromissione di un account. Inoltre, con il principio del privilegio minimo, ci si mette al riparo dagli attacchi perpetrati da utenti interni all'azienda oltre che dall'avvio accidentale di richieste API potenzialmente distruttive.

INFORMAZIONI SU CROWDSTRIKE

CrowdStrike, leader della sicurezza informatica a livello globale, sta ridefinendo la sicurezza nell'era del cloud grazie alla sua piattaforma di protezione degli endpoint creata appositamente per bloccare le compromissioni. L'architettura basata su un unico agent a basso impatto della piattaforma CrowdStrike Falcon® applica l'intelligenza artificiale a livello del cloud per offrire protezione e visibilità istantanee sull'intera azienda e prevenire gli attacchi sugli endpoint e i carichi all'interno della rete e all'esterno. Sfruttando la tecnologia proprietaria di CrowdStrike Threat Graph®, ogni settimana CrowdStrike Falcon crea correlazioni in tempo reale tra più di 4 migliaia di miliardi di eventi legati agli endpoint provenienti da tutto il mondo, alimentando una delle piattaforme di sicurezza più avanzate mai esistite.

SOLUZIONI DI SICUREZZA PER IL CLOUD CROWDSTRIKE

Progetta, Costruisci, Proteggi

FALCON CLOUD WORKLOAD PROTECTION

Protezione completa dalle compromissioni per gli ambienti privati, pubblici, ibridi e multicloud che consente ai clienti di adottare nuove tecnologie e di proteggerle in tempi rapidi, a prescindere dal workload.

FALCON HORIZON™

Funzionalità di visibilità multicloud, monitoraggio continuo, ricerca delle minacce e gestione della conformità. I team DevOps possono implementare le applicazioni in modo più efficiente e rapido perché con Falcon Horizon la strategia di sicurezza cloud diventa un gioco da ragazzi.

SICUREZZA DEI CONTAINER

Accelera le attività di rilevamento, analisi e threat hunting eseguite sui container, anche se disattivati, consentendo ai team di sicurezza di rendere sicuri i container senza causare attriti con i team DevOps.

VALUTAZIONE DELLA SICUREZZA DEL CLOUD

Servizio di test e valutazione dell'infrastruttura cloud volto a stabilire se sono stati implementati livelli di protezione e governance sufficienti a contrastare i rischi per la sicurezza.