Verifiche di compliance in ambienti Cloud

Niccolò Volontè - 20642A
Università degli Studi di Milano
Corso di Laurea in Sicurezza dei Sistemi e delle Reti Informatiche
Anno Accademico 2024/2025

9 luglio 2025

Il presente elaborato riguarda il tema della sicurezza in ambienti cloud, con particolare riferimento alle verifiche di compliance all'interno della piattaforma Amazon Web Services (AWS). In un contesto in cui le infrastrutture cloud sono sempre più adottate da organizzazioni pubbliche e private, garantire la corretta configurazione dei servizi in conformità agli standard di sicurezza internazionali è un'esigenza fondamentale. L'obiettivo principale della tesi è stato quindi quello di progettare e sviluppare una suite di sonde di assurance in grado di eseguire controlli automatici sulla configurazione delle risorse AWS, verificando la loro conformità rispetto a benchmark riconosciuti come il CIS AWS Foundations Benchmark e altri documenti specifici come il CIS Amazon EKS Benchmark, le raccomandazioni NIST SP 800-53.

Dopo una parte introduttiva e teorica, incentrata sull'analisi dello stato dell'arte, degli standard di sicurezza (CIS, NIST e AWS Security Hub) e delle caratteristiche dei principali servizi AWS, il lavoro si è focalizzato sulla realizzazione concreta delle sonde. Le sonde sono state integrate nella piattaforma MoonCloud, un sistema pensato per offrire supporto alle attività di assurance su ambienti ICT attraverso l'automazione, l'orchestrazione e la visualizzazione dei risultati. MoonCloud consente la creazione delle sonde in ambienti containerizzati, il monitoraggio continuo delle risorse e l'interazione tramite una dashboard centralizzata che ne permette anche l'esecuzione manuale o pianificata.

Durante il tirocinio curricolare, ho seguito tutte le fasi dello sviluppo: dalla comprensione degli standard di sicurezza e delle API AWS, alla progettazione dell'architettura di ciascuna sonda, fino all'implementazione, ai test, al deploy automatizzato tramite pipeline CI/CD e infine all'integrazione nella dashboard MoonCloud. Questo ha richiesto non solo capacità tecniche, ma anche una gestione attenta dell'organizzazione del lavoro, della documentazione e della coerenza tra le sonde per garantire un'interpretazione uniforme dei risultati.

Il lavoro ha portato alla realizzazione di 13 sonde classificate in base alla tipologia di controlli. Un primo gruppo comprende le sonde conformi al CIS AWS Foundations Benchmark v3, che si occupano di verificare la configurazione di servizi come Identity and Access Management (IAM), Elastic Compute 2 (EC2), Simple Storage Service (S3), Relational Database Service (RDS), Config, CloudTrail, Key Management Service (KMS) e altri. Ogni controllo è stato tradotto da descrizione testuale a logica eseguibile, analizzando la documentazione delle API AWS per identificare le funzioni necessarie a ottenere i parametri richiesti per la verifica.

Accanto a queste, è stato sviluppato un secondo gruppo di sonde che, pur non rientrando nel benchmark principale, si basa su raccomandazioni ufficiali del Center for Internet Security o di AWS Security Hub. È il caso, ad esempio, delle sonde per Amazon EKS e SQS, che utilizzano benchmark specifici, o della sonda per Amazon Inspector, che verifica l'attivazione di diverse modalità di scansione previste dal servizio. Questi strumenti consentono di estendere l'assurance

anche a componenti non ancora pienamente coperte dai benchmark generici, migliorando la copertura complessiva e la vastità dei controlli.

Un ulteriore contributo importante è rappresentato dalla sonda `aws_vulnerability`, che si discosta dalle altre in quanto non controlla configurazioni statiche, ma esegue analisi dinamiche alla ricerca di vulnerabilità note (CVE) sfruttando ciò che risulta dalle scansioni di AWS Inspector. Questo approccio permette di valutare il rischio operativo in base allo stato effettivo delle risorse, offrendo una visione aggiuntiva dello stato di sicurezza delle istanze EC2, ECR e Lambda.

Tutte le sonde sono state sviluppate in Python, utilizzando la libreria Boto3 per l'interfacciamento con AWS, e costruite in immagini Docker secondo lo standard previsto dal driver MoonCloud. Ogni sonda implementa una macchina a stati finiti, con gestione degli errori, rollback e generazione di output strutturato, in modo da garantire affidabilità, chiarezza dei risultati e facilità di integrazione. Particolare attenzione è stata dedicata alla sicurezza delle credenziali e alla definizione dei parametri di input tramite JSON schema.

Questo progetto mi ha permesso di applicare concretamente le competenze acquisite nel percorso accademico, affrontando problematiche reali in un contesto professionale. Ha richiesto un impegno costante, autonomia nello studio e nell'analisi delle tecnologie coinvolte e capacità di adattamento a un ambiente complesso ma stimolante. Il lavoro ha contribuito ad arricchire la piattaforma MoonCloud con nuove funzionalità operative e, allo stesso tempo, mi ha consentito di maturare una maggiore consapevolezza della complessità e dell'importanza della sicurezza negli ambienti cloud.