

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

RELATORE

Prof. Marco Anisetti

CORRELATORE

Dott. Antongiaco Polimeno

3 luglio 2025

Il presente elaborato affronta il tema della sicurezza in ambienti cloud, con particolare riferimento alle verifiche di compliance all'interno della piattaforma Amazon Web Services (AWS).

Scopo della tesi è garantire l'aderenza degli ambienti cloud a benchmark di sicurezza e best practice, come il *CIS AWS Foundations Benchmark*, il *CIS Amazon EKS Benchmark* e le raccomandazioni *NIST SP 800-53*. Per raggiungere questo obiettivo, è stata sviluppata una suite di **13** sonde di *security assurance* in grado di eseguire **51** controlli automatizzabili sulla configurazione delle risorse AWS, verificandone la conformità.

Il lavoro si articola in quattro fasi principali:

1. **Analisi dello stato dell'arte**, con studio degli standard di sicurezza (CIS, NIST, AWS Security Hub) e delle caratteristiche dei principali servizi offerti da AWS. Inoltre, comprensione del framework MoonCloud e delle sue funzionalità, che fornisce un ambiente di esecuzione e deployment per le sonde di assurance, oltre che alla gestione dei dati in input per la configurazione delle stesse.
2. **Progettazione delle sonde di assurance**, traducendo i controlli descrittivi dei benchmark in logiche eseguibili. Ogni sonda è stata progettata per un servizio AWS specifico:
 - `aws_sqs`: 3 controlli, relativi a crittografia a riposo, tagging e policy di accesso.
 - `aws_inspector`: 4 controlli, relativi all'abilitazione del servizio.
 - `aws_iam`: 13 controlli, relativi alla configurazione delle policy IAM, gestione delle credenziali e dei permessi.
 - `aws_ec2`: 7 controlli, relativi alla sicurezza della rete, logging e crittografia.
 - `aws_s3`: 6 controlli, relativi alla verifica degli accessi, logging e sicurezza delle operazioni sui bucket.
 - `aws_account`: 1 controllo, relativo alla verifica del contatto di sicurezza.
 - `aws_config`: 1 controllo, relativo alla registrazione delle configurazioni delle risorse.
 - `aws_cloudtrail`: 4 controlli, relativi alle code multi-regione, crittografia e log su bucket S3.
 - `aws_efs`: 1 controllo, relativo alla crittografia a riposo.

- `aws_kms`: 1 controllo, relativo alla rotazione delle chiavi.
 - `aws_rds`: 3 controlli, relativi alla verifica degli accessi, crittografia e aggiornamenti automatici.
 - `aws_eks`: 7 controlli, relativi all'uso di versioni supportate, crittografia a riposo, tagging e logging.
3. **Implementazione e testing**, attraverso lo sviluppo di 13 sonde in Python containerizzate con Docker e dotate di pipeline CI/CD per l'integrazione nel framework MoonCloud. Ogni sonda segue un'architettura standard e produce output strutturato, adatto ad una valutazione intuitiva.
 4. **Integrazione nella piattaforma MoonCloud**, che consente l'esecuzione delle sonde in ambienti reali, la pianificazione periodica dei controlli e la visualizzazione dei risultati globali tramite dashboard.

Le sonde sono classificate in base alla tipologia di controlli: una parte è conforme al benchmark CIS AWS Foundations v3, un'altra estende le verifiche a componenti come Amazon EKS, SQS e Inspector, non coperti dai benchmark principali. Di particolare rilievo è la sonda `aws_vulnerability`, che esegue analisi dinamiche sulle vulnerabilità note (CVE), offrendo una valutazione della sicurezza delle risorse AWS ECR, EC2, e Lambda.

Tutte le componenti sono state progettate con attenzione all'affidabilità, all'integrazione e alla gestione degli errori. Il lavoro ha richiesto competenze tecniche, capacità di documentazione e organizzazione del lavoro.

Sviluppi futuri prevedono l'estensione delle sonde ad altri cloud provider, l'integrazione con nuovi benchmark, e l'estensione delle sonde per coprire regioni multiple e servizi aggiuntivi.