



# Verifiche di compliance in ambienti Cloud

Presentazione dell'elaborato finale

Laurea Triennale in Sicurezza dei Sistemi e delle Reti Informatiche

**Niccolò Volontè** (20642A)

Relatore: Prof. Marco Anisetti

Correlatore: Dott. Antongiacomo Polimeno

16 luglio 2025



UNIVERSITÀ  
DEGLI STUDI  
DI MILANO



# Introduzione e contesto normativo

Cloud, compliance e obiettivi

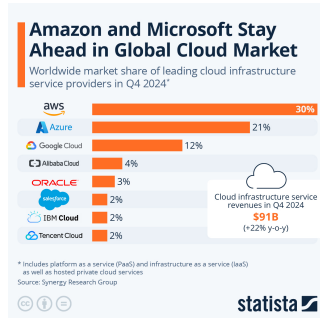
- Crescita del Cloud Computing e della sua adozione



# Introduzione e contesto normativo

Cloud, compliance e obiettivi

- Crescita del Cloud Computing e della sua adozione

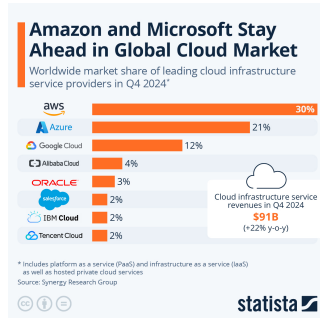




# Introduzione e contesto normativo

Cloud, compliance e obiettivi

- Crescita del Cloud Computing e della sua adozione
- La *compliance* nel cloud: ambiente dinamico rende difficile la verifica del profilo di sicurezza

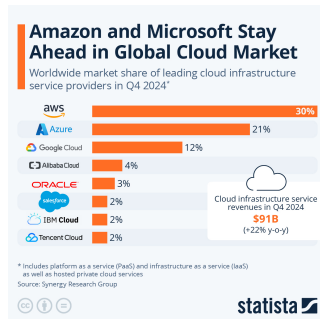




# Introduzione e contesto normativo

Cloud, compliance e obiettivi

- Crescita del Cloud Computing e della sua adozione
- La *compliance* nel cloud: ambiente dinamico rende difficile la verifica del profilo di sicurezza
- **Standard di riferimento:**
  - CIS AWS Foundations Benchmark
  - NIST SP 800-53

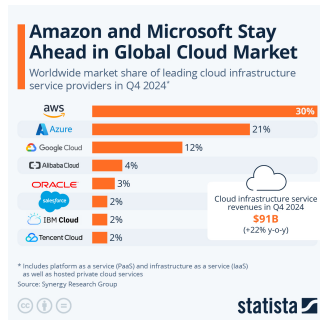




# Introduzione e contesto normativo

Cloud, compliance e obiettivi

- Crescita del Cloud Computing e della sua adozione
- La *compliance* nel cloud: ambiente dinamico rende difficile la verifica del profilo di sicurezza
- **Standard di riferimento:**
  - CIS AWS Foundations Benchmark
  - NIST SP 800-53
- **Obiettivo:** *sviluppare sonde* automatizzabili per verifiche di *compliance* su **AWS**, *integrabili* nella piattaforma **Moon Cloud**





# Standard di riferimento

Esempio di controllo per `aws_account`

## 1.4 Ensure MFA is enabled for the 'root' user account (Automated)

- **Profile Applicability:** Level 1
- **Description:** The 'root' user account is the most privileged user in an AWS account. Multi-factor Authentication (MFA) adds an extra layer of protection on top of a username and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their username and password as well as for an authentication code from their AWS MFA device.
- **Rationale:** Enabling MFA provides increased security for console access as it requires the authenticating principal to possess a device that emits a time-sensitive key and have knowledge of a credential.



# Analisi della documentazione

## AWS Security Hub, Boto3 Account



Get started Service guides Developer tools AI resources



### [Account.1] Security contact information should be provided for an AWS account

**Related requirements:** NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

**Category:** Identify > Resource Configuration

**Severity:** Medium

**Resource type:** AWS:::Account

**AWS Config rule:** [security-account-information-provided](#)

**Schedule type:** Periodic

**Parameters:** None

This control checks if an Amazon Web Services (AWS) account has security contact information. The control fails if security contact information is not provided for the account.

Alternate security contacts allow AWS to contact another person about issues with your account in case you're unavailable. Notifications can be from Support, or other AWS service teams about security-related topics associated with your AWS account usage.

#### Remediation

To add an alternate contact as a security contact to your AWS account, see [Update the alternate contacts for your AWS account](#) in the *AWS Account Management Reference Guide*.



### Boto3 1.39.4 documentation

Q Search

#### Feedback

Do you have a suggestion to improve this website or boto3?  
[Give us feedback.](#)

#### Quickstart

[A Sample Tutorial](#)

[Code Examples](#)

[Developer Guide](#)

[Security](#)

[Available Services](#)

[AccessAnalyzer](#)

[Account](#)

[ACM](#)

[ACMPCA](#)

[AIOps](#)

[PrometheusService](#)

[Account](#) / [Client](#) / [get\\_alternate\\_contact](#)



## get\_alternate\_contact

`Account.Client.get_alternate_contact(**kwargs)`

Retrieves the specified alternate contact attached to an Amazon Web Services account.

For complete details about how to use the alternate contact operations, see [Access or updating the alternate contacts](#).

#### Note

Before you can update the alternate contact information for an Amazon Web Services account that is managed by Organizations, you must first enable integration between Amazon Web Services Account Management and Organizations. For more information, see [Enabling trusted access for Amazon Web Services Account Management](#).

See also: [AWS API Documentation](#)

#### Request Syntax

```
response = client.get_alternate_contact(
    AccountId='string',
    AlternateContactType='BILLING'|'OPERATIONS'|'SECURITY'
)
```

#### PARAMETERS:

- AccountId (string)** – Specifies the 12 digit account ID number of the Amazon Web Services account that you want to access or modify with this operation.  
  
If you do not specify this parameter, it defaults to the Amazon Web Services account of the identity used to call the operation.  
  
To use this parameter, the caller must be an identity in the [organization's management account](#) or a delegated administrator account, and the specified account ID must be a





## Suite di sonde

Elenco delle sonde sviluppate

**13** sonde sviluppate con **51** controlli

- `aws_sqs`
- `aws_inspector`
- `aws_iam`
- `aws_ec2`
- `aws_s3`
- `aws_account`



## Suite di sonde

Elenco delle sonde sviluppate

**13** sonde sviluppate con **51** controlli

- `aws_sqs`
- `aws_inspector`
- `aws_iam`
- `aws_ec2`
- `aws_s3`
- `aws_account`
- `aws_config`
- `aws_cloudtrail`
- `aws_efs`
- `aws_kms`
- `aws_rds`
- `aws_eks`



## Suite di sonde

Elenco delle sonde sviluppate

**13** sonde sviluppate con **51** controlli

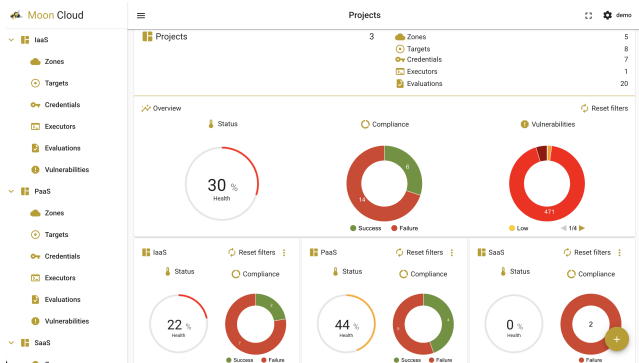
- `aws_sqs`
- `aws_inspector`
- `aws_iam`
- `aws_ec2`
- `aws_s3`
- `aws_account`
- `aws_config`
- `aws_cloudtrail`
- `aws_efs`
- `aws_kms`
- `aws_rds`
- `aws_eks`
- `aws_vulnerability`: aggregazione vulnerabilità da AWS Inspector (sonda fuori standard)



# Moon Cloud

Piattaforma, funzionalità e architettura

- Esegue sonde di assurance su infrastrutture ICT

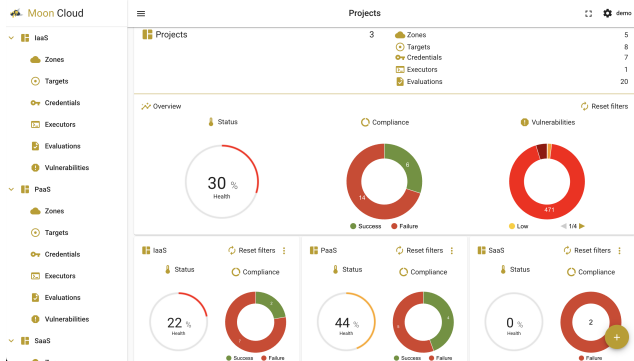




# Moon Cloud

Piattaforma, funzionalità e architettura

- Esegue sonde di assurance su infrastrutture ICT
- Architettura basata su immagini Docker e CI/CD

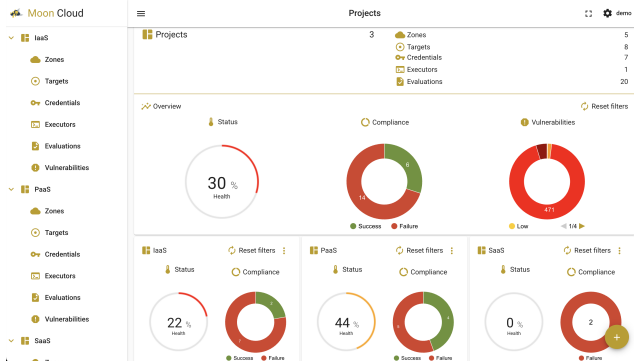




# Moon Cloud

Piattaforma, funzionalità e architettura

- Esegue sonde di assurance su infrastrutture ICT
- Architettura basata su immagini Docker e CI/CD
- Dashboard per la gestione dei target, credenziali e risultati

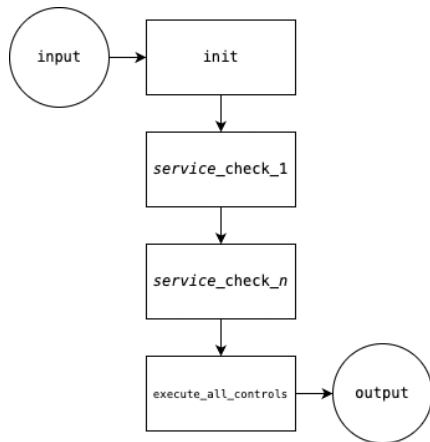




## Struttura di una sonda

Componenti per la creazione

- Struttura con atoms eseguiti in sequenza

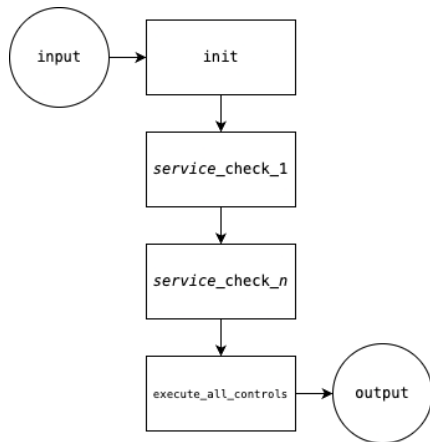




## Struttura di una sonda

Componenti per la creazione

- Struttura con `atoms` eseguiti in sequenza
- Modello a stati finiti: **forward** e **rollback**



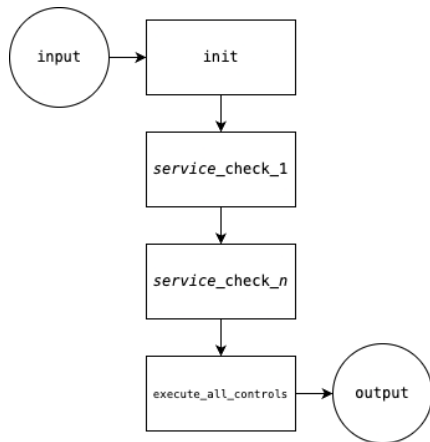




## Struttura di una sonda

Componenti per la creazione

- Struttura con `atoms` eseguiti in sequenza
- Modello a stati finiti: **forward** e **rollback**
- Output *strutturato*





## Esempio: aws\_sqs

Controllo cifratura, tag e accesso pubblico

- Controlli relativi a crittografia, tagging, e policy pubbliche

### Snippet: gestione client multiregione e controllo SQS.1

```
specific_regions = re.split(r'[,\s]+', raw_regions) if raw_regions else []
for idx, region in enumerate(specific_regions[:6], start=1):
    self.clients[f'client_{idx}'] = boto3.client(...)
```

```
attr_response = client.get_queue_attributes(
    AttributeNames=['SqsManagedSseEnabled'],
    QueueUrl=queue_url
)
if attr_response.get('Attributes', {}).get('SqsManagedSseEnabled') == 'true':
    encrypted_queues.append(...)
else unencrypted_queues.append(...)
```



## Esempio: aws\_sqs

Controllo cifratura, tag e accesso pubblico

- Controlli relativi a crittografia, tagging, e policy pubbliche
- Intera scansione multiregione

### Snippet: gestione client multiregione e controllo SQS.1

```
specific_regions = re.split(r'[,\s]+', raw_regions) if raw_regions else []  
for idx, region in enumerate(specific_regions[:6], start=1):  
    self.clients[f'client_{idx}'] = boto3.client(...)
```

```
attr_response = client.get_queue_attributes(  
    AttributeNames=['SqsManagedSseEnabled'],  
    QueueUrl=queue_url  
)  
if attr_response.get('Attributes', {}).get('SqsManagedSseEnabled') == 'true':  
    encrypted_queues.append(...)  
else unencrypted_queues.append(...)
```



## Esempio: aws\_sqs

Controllo cifratura, tag e accesso pubblico

- Controlli relativi a crittografia, tagging, e policy pubbliche
- Intera scansione multiregione
- Ogni controllo è una funzione separata

### Snippet: gestione client multiregione e controllo SQS.1

```
specific_regions = re.split(r'[,\s]+', raw_regions) if raw_regions else []  
for idx, region in enumerate(specific_regions[:6], start=1):  
    self.clients[f'client_{idx}'] = boto3.client(...)
```

```
attr_response = client.get_queue_attributes(  
    AttributeNames=['SqsManagedSseEnabled'],  
    QueueUrl=queue_url  
)  
if attr_response.get('Attributes', {}).get('SqsManagedSseEnabled') == 'true':  
    encrypted_queues.append(...)  
else unencrypted_queues.append(...)
```



## aws\_vulnerability

Sonda per la gestione CVE

- Sonda che non aderisce a standard ma che elenca CVE trovate da AWS Inspector



## aws\_vulnerability

Sonda per la gestione CVE

- Sonda che non aderisce a standard ma che elenca CVE trovate da AWS Inspector
- Analisi di Elastic Container Registry (ECR), Elastic Compute Cloud (EC2) e *Lambda functions*



## aws\_vulnerability

Sonda per la gestione CVE

- Sonda che non aderisce a standard ma che elenca CVE trovate da AWS Inspector
- Analisi di Elastic Container Registry (ECR), Elastic Compute Cloud (EC2) e *Lambda* functions
- Consente una visione dinamica del rischio



# aws\_vulnerability

Sonda per la gestione CVE

- Sonda che non aderisce a standard ma che elenca CVE trovate da AWS Inspector
- Analisi di Elastic Container Registry (ECR), Elastic Compute Cloud (EC2) e *Lambda* functions
- Consente una visione dinamica del rischio

The screenshot shows the Moon Cloud SaaS interface. On the left is a sidebar with navigation items: Moon Cloud, IaaS, PaaS, SaaS, Zones, Targets, Credentials, Executors, Evaluations, and Vulnerabilities (highlighted). The main panel is titled 'SaaS' and 'Vulnerabilities'. It features a search bar and a table of vulnerabilities.

VULNERABILITY IDENTIFIER	TARGET	ZONE	SEVERITY	CVSS SCORE
CVE-2019-10172 - org.codehaus.jackson:jackson-mapper-asl	AWS Cloud Target - SaaS	Public Service	High	7.5
CVE-2019-10202 - org.codehaus.jackson:jackson-mapper-asl	AWS Cloud Target - SaaS	Public Service	Critical	9.8
CVE-2020-36518 - com.fasterxml.jackson.core:jackson-databind	AWS Cloud Target - SaaS	Public Service	High	7.5
CVE-2021-46877 - com.fasterxml.jackson.core:jackson-databind	AWS Cloud Target - SaaS	Public Service	High	7.5
CVE-2022-42003 - com.fasterxml.jackson.core:jackson-databind	AWS Cloud Target - SaaS	Public Service	High	7.5
CVE-2022-42004 - com.fasterxml.jackson.core:jackson-databind	AWS Cloud Target - SaaS	Public Service	High	7.5
CVE-2025-49128 - com.fasterxml.jackson.core:jackson-core	AWS Cloud Target - SaaS	Public Service	Medium	4.0
CVE-2025-52999 - com.fasterxml.jackson.core:jackson-core	AWS Cloud Target - SaaS	Public Service	High	





# Deploy e output delle sonde

Esecuzione, integrazione e risultati

## Esecuzione e integrazione

- Pipeline CI/CD su GitLab per ogni sonda
- Definizione rigorosa di *Input* e *Output*
- Definizione nel backend di Moon Cloud
- Integrazione nel frontend di Moon Cloud con *template form*

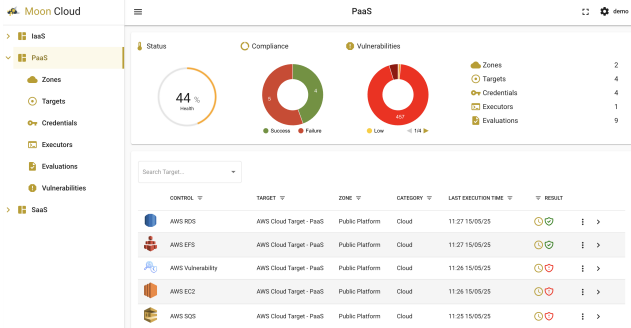


# Deploy e output delle sonde

Esecuzione, integrazione e risultati

## Esecuzione e integrazione

- Pipeline CI/CD su GitLab per ogni sonda
- Definizione rigorosa di *Input* e *Output*
- Definizione nel backend di Moon Cloud
- Integrazione nel frontend di Moon Cloud con *template form*





# Risultati ottenuti e sviluppi futuri

Riflessioni e prospettive

## Risultati ottenuti

- Risultato numerico e descrittivo
- Sommario con percentuale di conformità
- Log dettagliato con eccezioni gestite
- Conformità a standard come CIS e NIST



# Risultati ottenuti e sviluppi futuri

Riflessioni e prospettive

## Risultati ottenuti

- Risultato numerico e descrittivo
- Sommario con percentuale di conformità
- Log dettagliato con eccezioni gestite
- Conformità a standard come CIS e NIST

## Sviluppi futuri

- Estensione a nuovi benchmark e servizi AWS
- Apertura verso altri cloud provider
- Supporto multi regione



*Grazie per l'attenzione!*