# Cloud Security Incident Response Case Study

## Google Cloud Security Command Center Investigation


Author: A. Brito
Date: February 2026

# Disclaimer

***Solar Moon Energy*** is a fictional regulated energy utility organization created for professional portfolio and educational purposes. Resource names, user identities, configurations, and timestamps have been modified or simulated to protect privacy while preserving technical realism.

# 1. Executive Summary

Solar Moon Energy recently migrated a portion of its public-facing services to Google Cloud Platform (GCP) as part of a digital modernization initiative. As a regulated power utility, the organization must maintain strong security posture controls aligned with industry frameworks such as NIST and regulatory standards common to critical infrastructure operators.

During routine security monitoring using Google Security Command Center (SCC), multiple high-severity misconfigurations were identified within the cloud environment, including:

- A publicly accessible Cloud Storage bucket
- An open SSH (TCP 22) firewall rule exposed to the internet
- An open RDP (TCP 3389) firewall rule exposed to the internet
- A publicly accessible HTTP (TCP 80) firewall rule

These findings presented potential risks including unauthorized access, brute-force attacks, lateral movement, and data exfiltration.

An internal cloud security investigation was initiated to:

1. Identify the source of the misconfigurations
2. Assess risk exposure
3. Validate whether exploitation occurred
4. Remediate the vulnerabilities
5. Confirm secure baseline restoration

All exposed resources were remediated, validated, and returned to a hardened state.

# 2. Situation & Context

As part of an infrastructure testing effort, an internal cloud engineer deployed:

- A virtual machine instance within the default VPC
- Several firewall rules to allow remote administrative testing
- A Cloud Storage bucket for internal data handling validation

During configuration, permissive access controls were applied for testing purposes. However, these changes unintentionally exposed resources to the public internet.

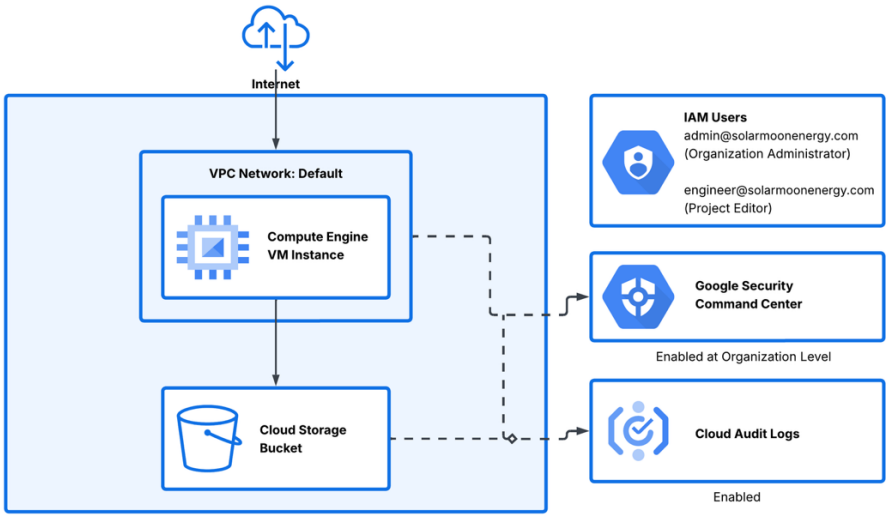
Because ***Solar Moon Energy*** operates in a regulated critical infrastructure sector, any public exposure, especially remote management ports or data storage must be treated as a potential security incident.

Security Command Center detected these exposures automatically, triggering a structured investigation.

# 3. Environment Architecture Overview

The simulated environment consisted of:

- Organization: SolarMoonEnergy.com
- Project: solar-moon-energy-ir-lab
- Two user accounts:
  - admin@solarmoonenergy.com (Organization Administrator)
  - engineer@solarmoonenergy.com (Project Editor)
- Default VPC network
- Compute Engine VM instance
- Cloud Storage bucket
- Google Security Command Center enabled at the organization level
- Cloud Audit Logs enabled



# 4. Detection Phase

## 4.1 Public Cloud Storage Bucket

Security Command Center generated a High severity finding:

**Category:** Public bucket ACL
**Finding Class:** Misconfiguration

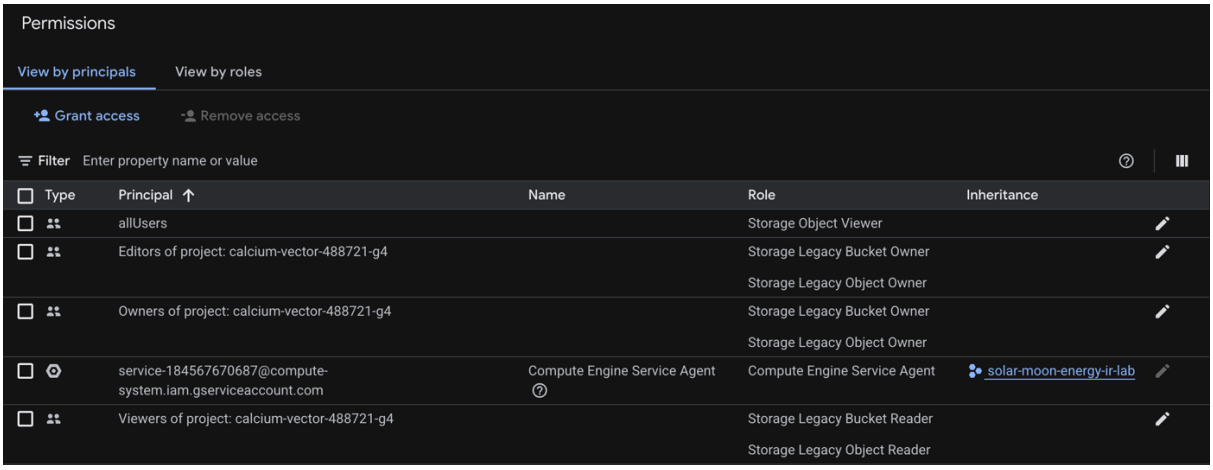
**Logs Explorer analysis confirmed:**

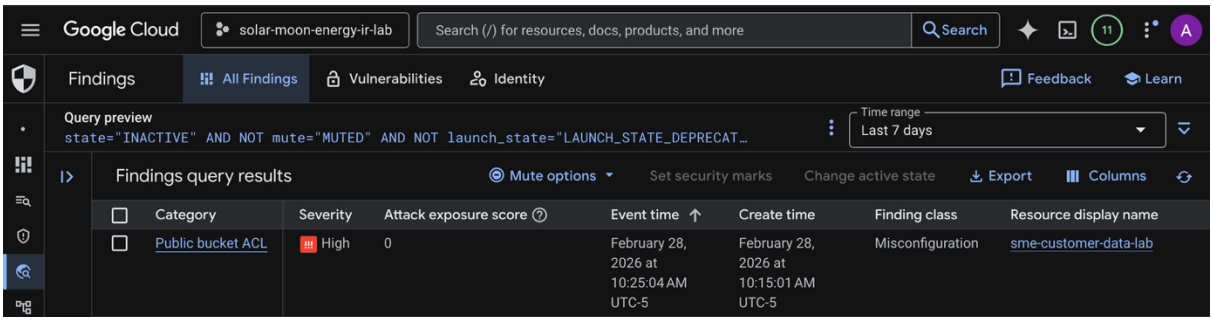
**Method:** storage.setIamPermissions
**Principal:** engineer@solarmoonenergy.com
**Resource:** Cloud Storage bucket

This indicated that the bucket permissions were modified to include:

allUsers → Storage Object Viewer

This configuration made bucket contents publicly accessible.



# 4.2 Open Firewall Exposure

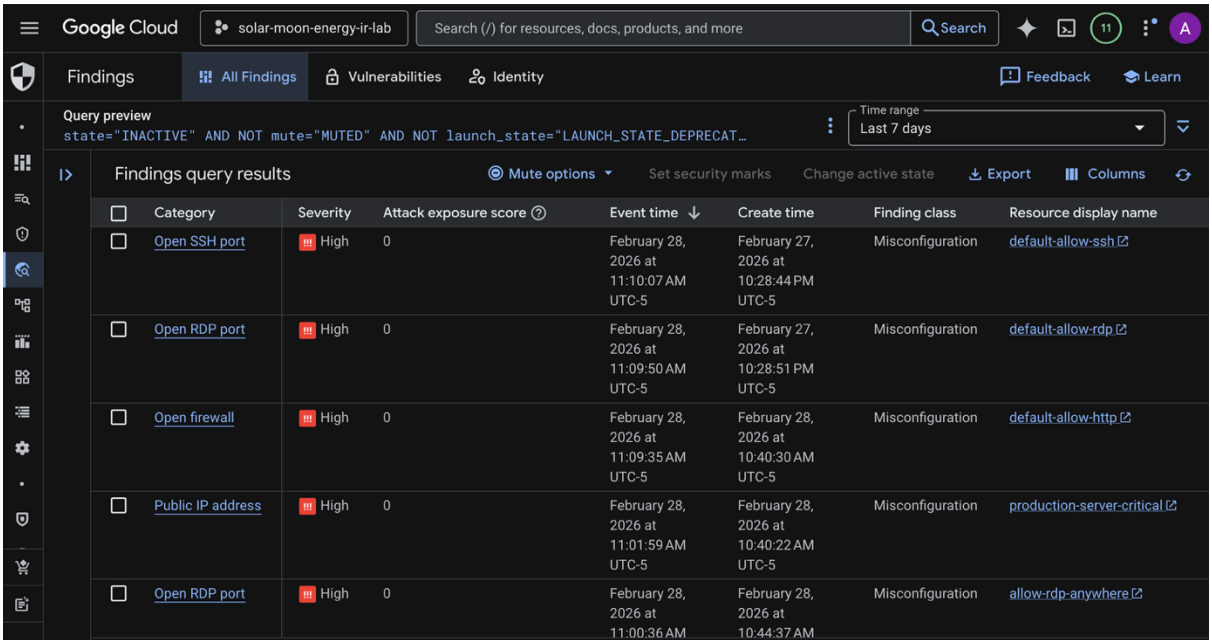
Security Command Center also identified:

- Open SSH port (TCP 22)
- Open RDP port (TCP 3389)
- Open HTTP firewall rule (TCP 80)

All rules allowed ingress from 0.0.0.0/0.

Such configurations increase risk of:

- Brute-force authentication attacks
- Credential stuffing
- Remote exploitation
- External reconnaissance



# 5. Investigation & Analysis

Cloud Audit Logs were queried using:

***protoPayload.methodName="v1.compute.instances.insert"***

This confirmed that the virtual machine instance was created by the engineer@solarmoonenergy.com account.

Timeline correlation showed:

1. VM creation
2. Firewall rule deployment
3. Storage permission modification
4. SCC detection

No evidence of unauthorized access or successful exploitation was found during log review. However, exposure duration, regardless of exploitation, was considered unacceptable under a regulated utility security model. The total exposure window was approximately 25 minutes, measured from the IAM policy modification to remediation validation.

# 6. Risk Assessment

| Finding | Severity | Likelihood | Impact | Risk Level |
|---|---|---|---|---|
| Public Storage Bucket | High | High | Data Exfiltration | Critical |
| Open SSH (22) | High | Medium | Brute Force / Lateral Movement | High |
| Open RDP (3389) | High | Medium | Remote Exploitation | High |
| Open HTTP (80) | Medium | Medium | External Enumeration | Medium |

The most critical exposure was the publicly accessible storage bucket, which could have enabled unauthorized data access.

# 7. MITRE ATT&CK Cloud Mapping

The identified misconfigurations map to the following MITRE ATT&CK techniques:

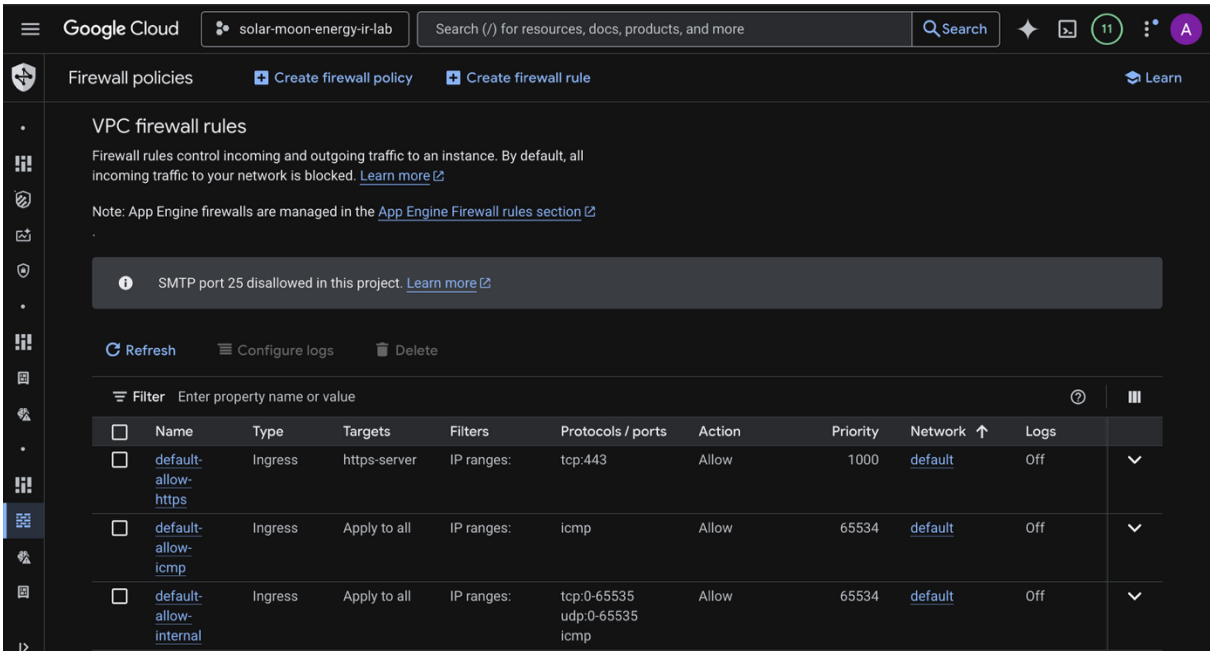
| Exposure | MITRE Technique |
|---|---|
| Public bucket | Exfiltration Over Web Service (T1567) |
| Open SSH | Valid Accounts (T1078) |
| Open RDP | Remote Services (T1021) |
| Public HTTP | External Remote Services |

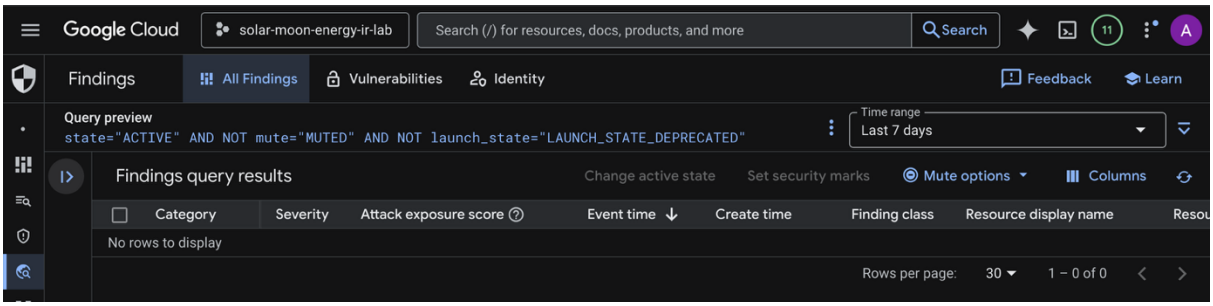
This mapping demonstrates how simple misconfigurations can enable adversary tactics across initial access and exfiltration stages.

# 8. Remediation Actions

The following corrective actions were performed:

- Removed allUsers access from Cloud Storage bucket
- Deleted default-allow-ssh firewall rule
- Deleted default-allow-rdp firewall rule
- Deleted default-allow-http firewall rule
- Verified IAM roles for least privilege
- Revalidated Security Command Center findings




Post-remediation validation confirmed:

- No public firewall exposure
- No public bucket access
- No active high-severity SCC findings

# 9. Lessons Learned

1. Temporary testing configurations can introduce high-risk exposures
2. Continuous cloud posture monitoring is critical in regulated environments
3. Security Command Center provides immediate visibility into misconfigurations
4. Identity correlation via Cloud Audit Logs enables rapid root cause analysis
5. Remediation validation is as important as detection

# 10. Conclusion

This case study demonstrates how a regulated utility organization can leverage Google Security Command Center and Cloud Audit Logs to detect, investigate, and remediate high-risk cloud misconfigurations. Even in a simulated environment, the investigation reflects real-world cloud incident response methodology:

- Detect
- Correlate
- Assess
- Remediate
- Validate

By integrating automated posture monitoring with structured investigation processes, ***Solar Moon Energy*** restored secure baseline posture while reinforcing governance controls appropriate for critical infrastructure environments.

# 11. Why This Matters for Critical Infrastructure

Critical infrastructure organizations such as energy utilities operate in environments where cyber risk directly impacts public safety, economic stability, and national security. In cloud environments, misconfigurations are among the most common and dangerous causes of exposure.

This case study demonstrates that effective cloud security in critical infrastructure requires:

- Continuous posture monitoring
- Strong identity governance
- Rapid log-based investigation capability
- Immediate remediation validation

Security Command Center, when paired with structured incident response methodology, becomes not just a monitoring tool but a governance enforcement mechanism.

Proactive detection and remediation of cloud misconfigurations is essential to maintaining grid reliability, regulatory compliance, and organizational resilience.