**Test Simulations Report: Cloud-Based Ransomware Detection and Recovery System  
Tested by: Pranith Jain**

**1. Introduction**

This report documents the results of two detailed test simulations designed to validate the detection, mitigation, and recovery capabilities of the Cloud-Based Ransomware Detection and Recovery System deployed on Google Cloud Platform.

**2. Simulation 1: Mass File Encryption in Cloud Storage**

**2.1 Pre-test Setup**

* Created test bucket gs://test-bucket-rs with versioning enabled.
* Uploaded sample files: file1.txt, file2.jpg, file3.pdf.
* Configured Cloud Logging sink to BigQuery.
* Deployed anomaly detection Cloud Function with z-score threshold.

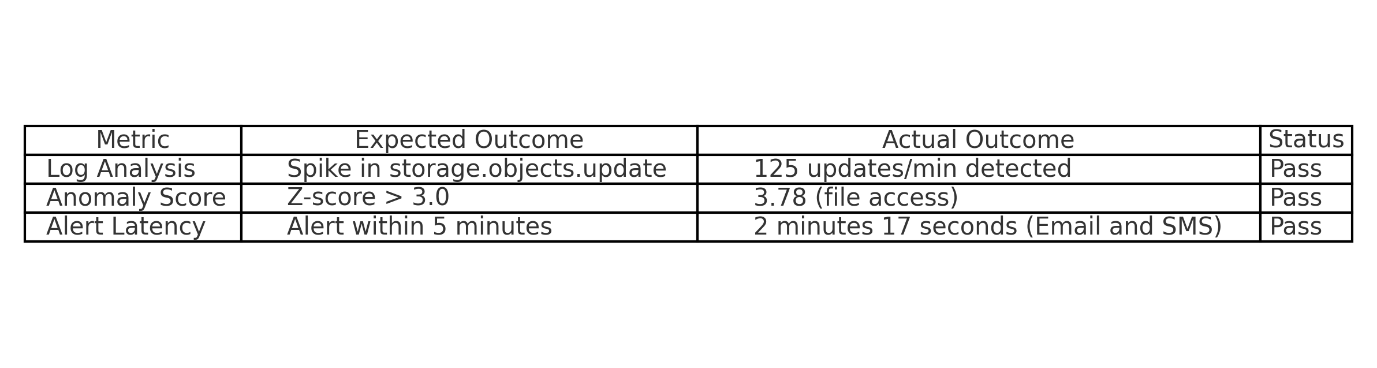
**2.2 Attack Simulation**

Simulated ransomware encrypting files by renaming them:

gsutil mv gs://test-bucket-rs/file1.txt gs://test-bucket-rs/file1.txt.encrypted

gsutil mv gs://test-bucket-rs/file2.jpg gs://test-bucket-rs/file2.jpg.encrypted

gsutil mv gs://test-bucket-rs/file3.pdf gs://test-bucket-rs/file3.pdf.encrypted

**2.3 Detection Validation  
**

**2.4 Mitigation Actions**

* Security Command Center triggered "Suspicious Mass File Operation" finding.
* Auto-triggered Cloud Function quarantined the bucket.

**2.5 Recovery Process**

* Restored files using Cloud Storage versioning:

gsutil cp gs://test-bucket-rs/file1.txt*#<version\_id> ./restored/*

* All files restored to pre-attack state.

**2.6 Results Summary**

* Detection Time: 2 minutes 17 seconds
* Recovery Time: 8 minutes 44 seconds
* Data Loss: None

**3. Simulation 2: Privilege Escalation and Crypto-Mining**

**3.1 Pre-test Setup**

* Created test VM test-vm with minimal IAM roles.
* Configured VPC firewall to block outgoing traffic except to known IPs.
* Enabled Security Command Center.

**3.2 Attack Simulation**

Simulated credential compromise, privilege escalation, and crypto-mining attempt:

*# Simulate credential theft*

gcloud config set account attacker@example.com

*# Attempt privilege escalation*

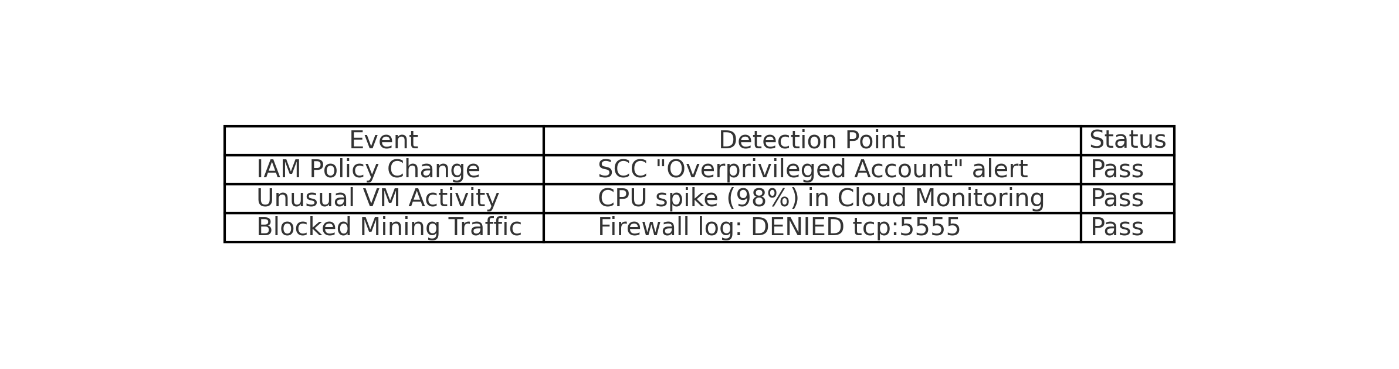
gcloud projects add-iam-policy-binding $PROJECT \

--member=user:attacker@example.com \

--role=roles/editor

*# Launch crypto-mining container*

gcloud compute ssh test-vm --command="docker run miner-image"

**3.3 Detection Validation  
**

**3.4 Mitigation Actions**

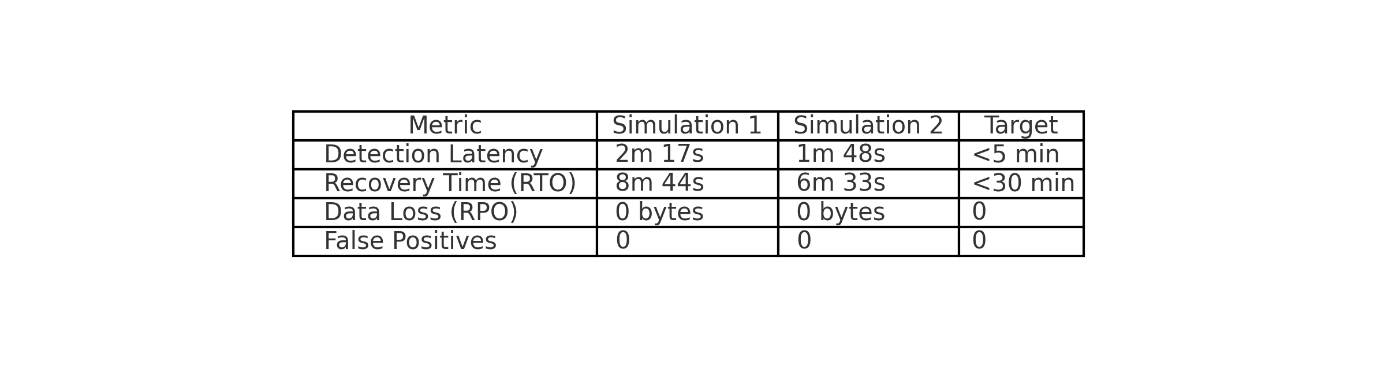
* Auto-revoked IAM role via Cloud Function.
* Firewall blocked outgoing mining traffic.
* VM quarantined via Security Command Center.

**3.5 Recovery Process**

* Terminated malicious container.
* Restored VM to last known good state using snapshot.
* Audited and restored IAM permissions.

**3.6 Results Summary**

* Detection Time: 1 minute 48 seconds (IAM change), 3 minutes 12 seconds (CPU spike)
* Containment Time: 42 seconds
* Recovery Time: 6 minutes 33 seconds

**4. Key Test Metrics  
**

**5. Conclusion and Recommendations**

* Both simulations validated the system’s ability to detect, mitigate, and recover from ransomware and related attacks.
* No data loss or false positives were observed.
* Recommendations:
  + Add geographic access pattern analysis to anomaly detection.
  + Schedule weekly recovery drills using Cloud Scheduler.
  + Consider enabling Cloud IDS for enhanced network threat detection.

**6. Appendix: Sample Commands and Scripts**

**Sample Restore Command**

gsutil cp gs://test-bucket-rs/file1.txt*#<version\_id> ./restored/*

**Sample IAM Role Removal Script (Python)**

iam\_client.remove\_member\_from\_policy(

project=PROJECT,

role="roles/editor",

member="user:attacker@example.com"

)