

# **Cloud-Based Ransomware Detection and Recovery System Report**

By : Sanskar Solanki

## **Table of Contents**

### **Introduction**

1. Objective .....	2
2. Scope .....	2

### **Report Components**

#### **2.1 Detection System**

1. Tools and Techniques .....	2
2. Implementation Steps .....	3

#### **2.2 Mitigation System**

1. Tools and Techniques .....	5
2. Implementation Steps .....	5

#### **2.3 Recovery System**

1. Tools and Techniques .....	7
2. Implementation Steps .....	7

#### **2.4 Incident Response** **8**

#### **2.5 Environment Testing** **9**

## **1. Introduction**

### **Objective**

The objective of this project is to develop a robust system for detecting, mitigating, and recovering from ransomware attacks in a cloud-based environment using Google Cloud Platform (GCP) services. The solution aims to leverage GCP's free-tier resources to build a cost-effective yet functional security framework.

### **Scope**

This project will utilize GCP services to:

- Detect potential ransomware activity using anomaly detection in cloud logs.
- Mitigate ransomware spread through Identity and Access Management (IAM) policies and real-time monitoring.
- Enable rapid recovery through automated backups, file versioning, and disaster recovery mechanisms.

## **2. Report Components**

### **2.1 Detection System**

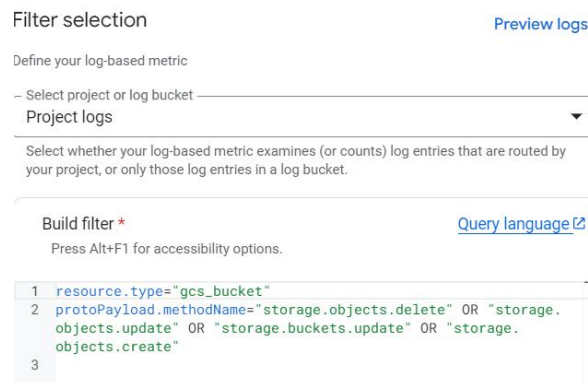
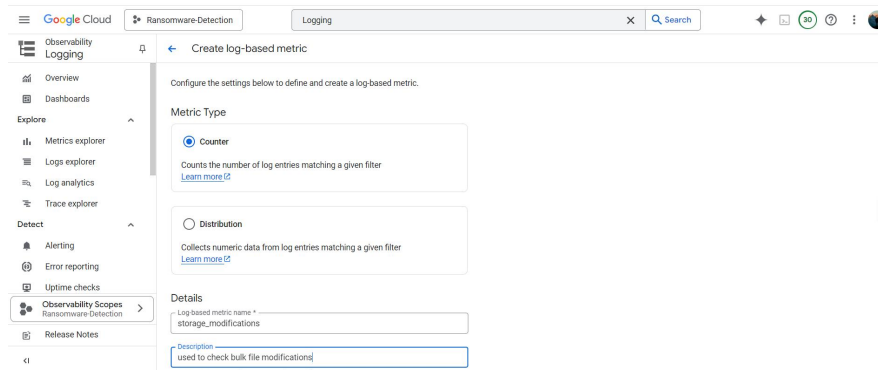
#### **Tools and Techniques:**

- **Cloud Logging:** Collect and analyze log data for unusual patterns, such as rapid file modifications or encryption activities.
- **Cloud Functions:** Automate alerts when suspicious activities occur, such as excessive failed login attempts or sudden spikes in resource utilization.
- **Job Scheduler :** Automatically backup sensitive data stored on cloud storage.
- **Pub/Sub Topics :** Triggers event , messages and alerts based on that , some action will take place to secure the system

## Implementation Steps:

### Cloud Logging :

1. First , we navigate to Logging (one of the crucial component of operations suite ) and move to **Logs Explorer** in Google Cloud Console.
2. Now we created **Log-Based Metric** , which will collect data from Logs and create metric to analyze large number of file modifications and Input /Output operations.
3. Here , we created metric to analyze cloud storage operations .
  - a) **Metric Type** : Counter
  - b) For Storage Bucket object operations



4. Next , we created metric high disk read/write operations in VM instances
  - a) **Metric Type** : Counter

Log-based metric name \*  
disk\_i/o

Description  
used to check high disk i/o operations  
Enter a description for this metric (optional)

Units

The units of measurement that apply to this metric (for example, bytes or seconds). For counter metrics, leave this blank or insert the digit '1'. For distribution metrics, you can optionally enter units, such as 's', 'ms', etc. [Learn more](#)

Filter selection Preview logs

Define your log-based metric

Select project or log bucket  
Project logs

Select whether your log-based metric examines (or counts) log entries that are routed by your project, or only those log entries in a log bucket.

Build filter \* Query language

Press Alt+F1 for accessibility options.

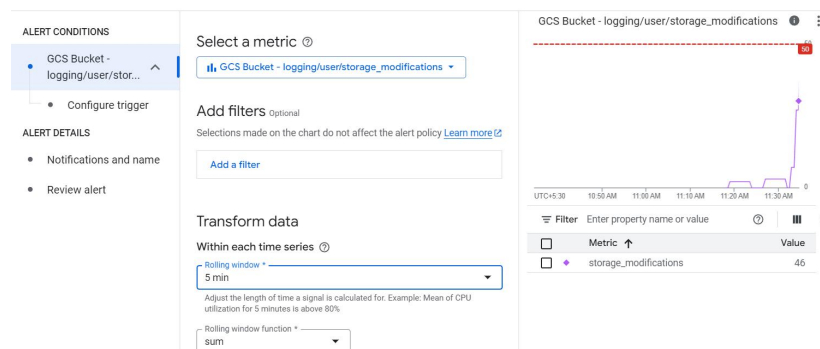
```
1 resource.type="gce_instance"
2 AND logName=("projects/ransomware-detection-453014/logs/compute.googleapis.com%2Fserial_port_output")
3 AND textPayload:"disk I/O"
```

## Cloud Monitoring :

1. To use these log-based metric for generating alerts , we used alerting policies in cloud monitoring.

2. For **Storage based metric** :

- Select metric created above , set Rolling Window : 5 min with function : sum(total operations).
- With condition type of Threshold Value : 50



C) Also add , notification channel ( email or phone). And give policy name.

Configure notifications and finalize alert

Configure notifications Recommended

☒ Use notification channel

Notification Channels

Filter Type to filter

SMS

☐ kanha

Email

☒ kanha

[Manage Notification Channels](#)

[Cancel](#) [OK](#)

3. For **Disk based Metric**

- Select metric , set Rolling Window : 5 min with function : sum.

- b) With condition Type of Threshold Value : 1500 and add notification channel for same.

### Cloud Functions Implementation :

With this step , any file uploaded on Cloud Storage send alerts through log by Cloud Function triggered by event takes place on storage objects.

1. Enable Cloud Function API by navigating to API services through console or CLI.
2. Now select or create new bucket in cloud storage ( in my case : data\_bucket989) to upload files.

Buckets <span>+ CREATE</span> <span>REFRESH</span>					
Filter Filter buckets					
<input type="checkbox"/>	Name ↑	Created	Location type	Location	Default storage class ?
<input type="checkbox"/>	<a href="#">data_bucket989</a>	Mar 8, 2025, 3:25:22 PM	Region	us-east1	Managed with Autoclass
<input type="checkbox"/>	<a href="#">data_bucket_backup989</a>	Mar 8, 2025, 3:26:01 PM	Region	us-east1	Nearline
<input type="checkbox"/>	<a href="#">gcf-v2-sources-802716810298-us-east1</a>	Mar 8, 2025, 3:33:42 PM	Region	us-east1	Standard
<input type="checkbox"/>	<a href="#">gcf-v2-uploads-802716810298-us-east1</a>	Mar 8, 2025, 3:33:29 PM	Region	us-east1	Standard

3. Create Cloud Run function files with : [main.py](#) and [requirements.txt](#) in same directory.
4. Deploy function in same region with cloud bucket :

```
sanskarsolanki417@cloudshell:~ (ransomware-detection-453014) $ gcloud functions deploy detection --runtime python39 --trigger-event google.storage.object.finalize --trigger-resource=data_bucket989 --entry-point=detect_ransomware --trigger-location=us-east1 --memory=256MB --region=us-east1
```

5. Assign , default cloud storage service account with **Pub/Sub publisher** IAM role to publish message to cloud function.

```
sanskarsolanki417@cloudshell:~ (ransomware-detection-453014) $ gcloud projects add-iam-policy-binding ransomware-detection-453014 --member=serviceAccount:802716810298-compute@developer.gserviceaccount.com --roles=pubsub.publisher
```

6. This will trigger cloud function , detection , which perform action on uploaded file and publish Pub/Sub Topic message .

## 2.2 Mitigation System

### Tools and Techniques:

- **Identity and Access Management (IAM):** Implement least privilege principles to minimize access to sensitive data.
- **Firewall Rules:** Restrict unauthorized access to cloud resources.

### Implementation Steps:

1. Define granular IAM roles and assign them to users and service accounts.
  1. Use manual service account with specific and least privilege role (**role/storage.editor**).
  2. Assign required permissions to default service account like default cloud function service account with **Cloud Function Invoker** role.
  3. Assign Role to default compute service account with required roles like **Pub/Sub Publisher**.
2. Define firewall rules to restrict traffic within boundary.
  1. Create Deny Egress Rule to malicious IP addresses like (**45.227.252.12/32**).
  2. Restrict incoming traffic only for required and allowed ports .

## 2.3 Recovery System

### Tools and Techniques:

- **Cloud Storage with Versioning:** Maintain multiple versions of files to prevent data loss.
- **Cloud Scheduler:** Automate periodic backups to offsite storage.

### Implementation Steps:

1. Enable Object Versioning in Cloud Storage buckets.

```
sanskarsolanki417@cloudshell:~ (ransomware-detection-453014) $ gsutil versioning set on gs://data_bucket989
Enabling versioning for gs://data_bucket989/...
```

2. **Cloud Scheduler :** This will help to automate tasks like backup data for disaster recovery

1. Enable Cloud Scheduler API.
2. Create new Job with test1 name , set region (any) , frequency in correct format and timezone.

The screenshot shows the 'Edit job' page for a job named 'test1' in the Cloud Scheduler console. The 'Region' is set to 'us-central1'. The 'Frequency' is set to '12 16 8 3 SAT'. Below the frequency, there is a note: 'Schedules are specified using unix-cron format. E.g. every minute: '\* \* \* \* \*', every 3 hours: '\*0 \*/3 \* \* \* \*', every Monday at 9:00: '\*0 9 \* \* 1\*'. A 'Learn more' link is provided. The 'Timezone' is set to 'India Standard Time (IST)'. A note at the bottom states: 'Jobs in set in timezones affected by Daylight Saving Time can run outside of cadence during DST change. Using a UTC timezone can avoid the problem. Learn more'.

3. Now to configure the execution , we need to trigger **HTTP request** requires Cloud Function URL . Ensure that **Job Scheduler's** service account have Cloud Functions Invoke role.

```
- members:
- serviceAccount:cloud-storage-service-account@ransomware-detection-453014.iam.gserviceaccount.com
- serviceAccount:service-802716810298@gcp-sa-cloudscheduler.iam.gserviceaccount.com
role: roles/cloudfunctions.invoker
```

4. Create **Cloud Function** : [backup\\_function](#) , copy url and add this in Job Scheduler with POST method.

5. Ensure that destination bucket is created.

## 2.4 Incident Response

1. In this we set up Pub/Sub for Alerts , create topic for **cloud function** (file detection) which will publish messages with subscription. Create topic for, **Cloud Function** (test function for compromised instances) which will get triggered once , topic receives message as **subscriber**.

Topics <span>+ CREATE TOPIC</span> <span>DELETE</span>					
LIST METRICS					
Filter Filter topics <span>?</span> <span>⌵</span>					
<input type="checkbox"/>	Topic ID <span>↑</span>	Encryption key	Topic name	Retention	Ingestion source
<input type="checkbox"/>	<a href="#">eventarc-us-east1-detection-647075-232</a>	Google-managed	projects/ransomware-detectio...	—	—
<input type="checkbox"/>	<a href="#">eventarc-us-east1-storage-735</a>	Google-managed	projects/ransomware-detectio...	—	—
<input type="checkbox"/>	<a href="#">eventarc-us-east1-storage2-318</a>	Google-managed	projects/ransomware-detectio...	—	—
<input type="checkbox"/>	<a href="#">eventarc-us-east1-trigger-k7p4jaud-876</a>	Google-managed	projects/ransomware-detectio...	—	—
<input type="checkbox"/>	<a href="#">ransomware-alerts</a>	Google-managed	projects/ransomware-detectio...	—	—
<input type="checkbox"/>	<a href="#">security-alerts</a>	Google-managed	projects/ransomware-detectio...	—	—

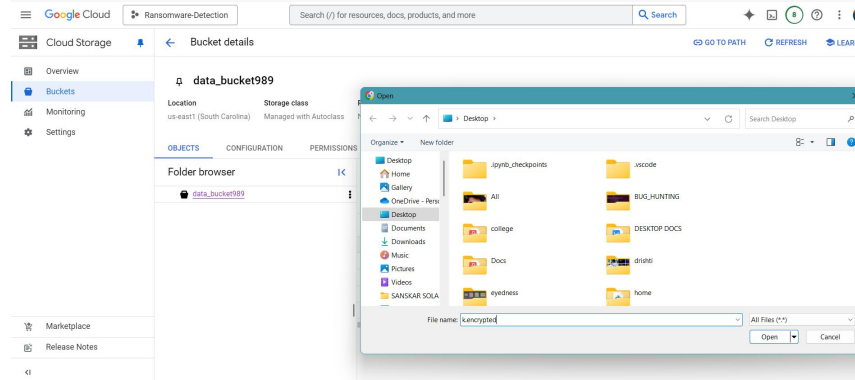
2. Implement **Cloud Function** to isolate vm instance , when it gets triggered by Pub/Sub (**security-alerts**). Function : [isolate-vm-function](#) and Requirements file : [requirements](#)

```
sanskarsolanki417@cloudshell:~ (ransomware-detection-453014)$ gcloud functions deploy isolate-vm --trigger-topic=security-alerts --runtime python39 --entry-point=isolate_vm --memory=256MB --region=us-east1
```

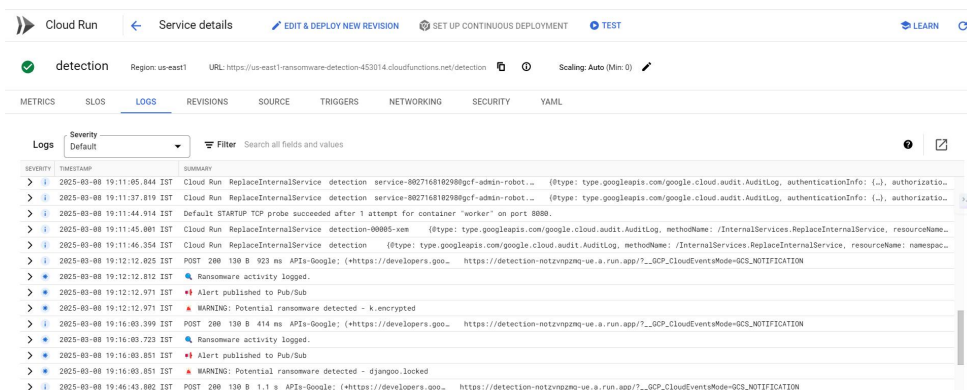


## 2.5 Environment Testing

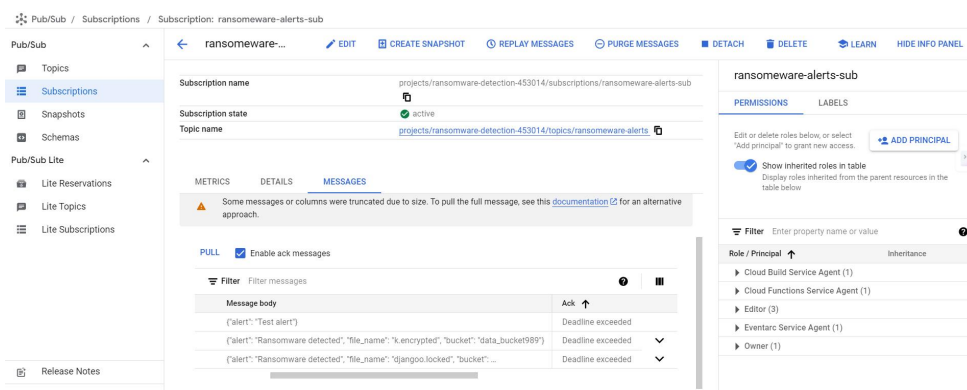
1. First by uploading any file containing malicious extension, to detect if , function writing logs and Publishes messages on Pub/Sub or not. (Here **k.encrypted**).



2. We can see , in Logs we received alert , detecting malicious file. We can also check it on Log Explorer.



3. Here , on ransomware-alerts topic of Pub/Sub we can pull messages published by cloud function.



4. Now to check , if any message Published by **Security Command Center** when it detects malicious thing happened on instance , then that vm instance gets isolated by cloud function triggered through Pub/Sub Topic message publisher.

5. To use security command center , we need to be part of any organization . So here we use **CLI** to publish message on security-alerts topic.

```
sanskarsolanki417@cloudshell:~ (ransomware-detection-453014) $ gcloud pubsub topics publish security-alerts --message='{ "instance_name": "instance-20250308-135125" }'
```

6. We can see, message is published and this will trigger cloud function to isolate vm

security-alerts-sub

PERMISSIONS LABELS

Filter Enter property name or value

Rule / Principal	Inheritance
Cloud Build Service Agent (1)	
Cloud Functions Service Agent (1)	
Editor (3)	
Eventarc Service Agent (1)	
Owner (1)	

METRICS DETAILS MESSAGES

click ACK next to the message to permanently prevent message delivery to other subscribers.

Some messages or columns were truncated due to size. To pull the full message, see this [documentation](#) for an alternative approach.

PULL ☒ Enable ack messages

Filter	Filter messages		
Publish time	Attribute keys	Message body	ACK
Mar 8, 2025, 7:41:27 PM	---	{\"instance_name\": \"malicious-vm\"}	ACK
Mar 8, 2025, 7:42:51 PM	---	{\"instance_name\": \"instance-20250308-135125\"}	ACK

7. List of all cloud run functions.

Google Cloud Ransomware-Detection run

Cloud Run Services DEPLOY CONTAINER CONNECT REPO WRITE A FUNCTION MANAGE CUSTOM DOMAINS RELEASE NOTES

A service exposes a unique endpoint and automatically scales the underlying infrastructure to handle incoming requests. Deploy a container image, source code or a function to create a service.

Services

Filter Deployment type: function Filter services

Name	Deployment type	Req/sec	Region	Authentication	Ingress	Recommendation	Last deployed	Deployed by
backup-function2	Function	0	us-east1	Allow unauthenticated	All	---	7 hours ago	Cloud Run functions
detection	Function	0	us-east1	Require authentication	All	---	6 hours ago	Cloud Run functions
isolate-vm	Function	0	us-east1	Require authentication	All	---	5 hours ago	Cloud Run functions

8. To check, if backup-function working correctly, we can forcibly run it through Job Scheduler.

1. First we upload file in data\_bucket989.

data\_bucket989

Location: us-east1 (South Carolina) Storage class: Managed with Autoclass Public access: Not public Protection: Soft Delete, Object versioning

OBJECTS CONFIGURATION PERMISSIONS PROTECTION LIFECYCLE OBSERVABILITY INVENTORY REPORTS OPERATIONS

Folder browser

Buckets > data\_bucket989

CREATE FOLDER UPLOAD TRANSFER DATA OTHER SERVICES

Filter by name prefix only Filter objects and folders Show Live objects only

Name	Size	Type
Orishiti Rakshak.docx	0 B	application/vnd.openxmlformats-officedocument.wordprocessingml.document

2. Now, we can run scheduler forcibly.

Cloud Scheduler / Jobs

Jobs CREATE JOB REFRESH FORCE RUN EDIT COPY PAUSE RESUME DELETE

SCHEDULER JOBS APP ENGINE CRON JOBS

Filter Filter jobs

Name	Status of last execution	Region	State	Description	Frequency	Target	Last run	Next run
test1	Has not run yet	us-central1	Enabled		12 16 8 3 SAT (Asia/Calcutta)	URL: https://us-east1-ransomware-detection-453014.cloudfunctions.net/backup-function2	Mar 8, 2025, 5:13:59 PM	Mar 15, 2025, 4:12:00 PM
test2	Has not run yet	us-central1	Enabled		12 16 8 3 SAT (Asia/Calcutta)	URL: https://us-east1-ransomware-detection-453014.cloudfunctions.net/backup-function2	Mar 8, 2025, 5:13:59 PM	Mar 15, 2025, 4:12:00 PM

3. And here we got success.

Jobs

CREATE JOB

REFRESH

FORCE RUN

EDIT

COPY

PAUSE

RESUME

DELETE

LEARN

SCHEDULER JOBS

APP ENGINE CRON JOBS

Filter

Filter jobs

test1

Success

us-central1

Enabled

12 16 8 3 SAT  
(Asia/Calcutta)

URL : https://us-east1-ransomware-detection-453014.cloudfunctions.net/backup-function2

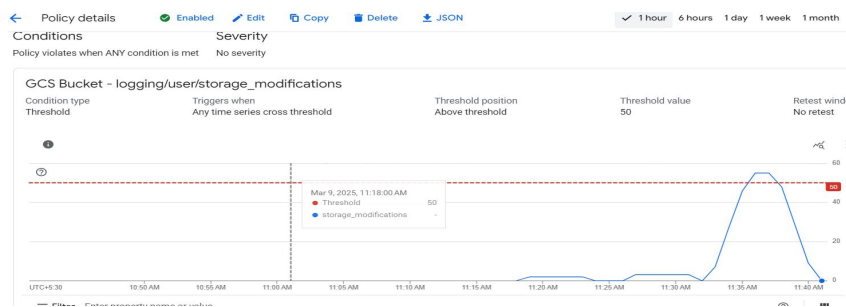
Mar 9, 2025,  
10:48:17 AM

Mar 15, 2025,  
4:12:00 PM

Mar 8, 2025,  
6:28:11 PM

- We can also check , if log-based metrics collecting data , and generating alerts or not manually.

```
sanskarsolanki417@cloudshell:~ (ransomware-detection-453014)$ for i in {1..55}; do
  echo "Test $i" > test-file-$i.txt
  gsutil cp test-file-$i.txt gs://data_bucket989
done
```



- And here we got mail from google cloud.

