Cloud Security Monitoring in GCP

#1 Foundations Lab Guide

1. Lab Overview

Objective

In this lab, you will deploy and configure core GCP monitoring and security services to detect suspicious IAM and network activity.
You will use Terraform for setup, simulate security events, and validate detections using Cloud Logging and the Security Command Center (SCC).

Key Learning Outcomes

- Enable and interpret Cloud Audit Logs for IAM and login activity.
- Detect privilege escalation attempts via IAM changes.
- Enable and analyze VPC Flow Logs for port scanning detection.
- Automate setup using Terraform for reproducible environments.
- (Bonus) Apply organization policies to enforce auditing.

2. Enable Cloud Audit Logs and Detect Unusual Login Events

Steps:

1. Create a Log Sink
    a. Navigate to Logging > Logs Router
    b. Notice there are two system-created log-router sinks by default: _Required and _Default. Identify the Inclusion filter for these sinks and their purpose.
    c. Create a new Sink (export_sink).
        i. Select BigQuery dataset as destination (make sure that the
        ii. Create a new dataset if needed
        iii. Include Admin Activity, Data Access and Policy Denied audit logs in the sink
2. Familiarize yourself with the logsQuery in Logs Explorer:
    a. Create a new service account service account with `roles/editor`.

Shell

```
export PROJECT_ID=your_project_id
gcloud config set project $PROJECT_ID
gcloud iam service-accounts create a-new-service-account --display-name="New SA"
```

  b. Update the service account role to “owner”. Run the following to modify IAM policy:

Shell

```
gcloud projects add-iam-policy-binding $PROJECT_ID \
--member="serviceAccount:a-new-service-account@${PROJECT_ID}.iam.gserviceaccount.com" \
  --role="roles/owner"
```

  c. Analyse the log in in Logs Explorer

Shell

```
resource.type="project"
protoPayload.methodName="SetIamPolicy"
protoPayload.serviceData.policyDelta.bindingDeltas.role="roles/owner"
```

3. Create a log alert matching the log explorer query
4. Create a second service account and set a new policy binding to get alerted.
5. In big query, create a query to filter out activities related to the creation of the service account.
    a. Explore the new table created under the destination dataset
    b. Create the sql query to filter out owner role bindings and show the user IP
    c. Create a query to list operations done from the same IP

3. Enable and Analyze VPC Flow Logs to Detect Port Scanning

Steps:

1. Create a new VPC
    a. Regional

    b. Subnet with flow logs enabled

2. Create Cloud Router
    a. Network: your newly created vpc
    b. Region: Same region
3. Create Cloud NAT
    a. NAT type: Public
    b. Network: your newly created vpc
    c. Region: Same region
    d. Cloud Router: your newly created router
    e. Logging: error only
4. Create 3 Firewall Rules: allow ssh, allow http and allow ssh via IAP
    a. Enable logs
    b. Network: your newly created vpc
    c. Priority: 1000
    d. Direction: Ingress
    e. Action on match: Allow
    f. Targets: Specified target tags
    g. Target tags:
        i. First rule: allow-ssh
        ii. 2nd rule: allow-8080
        iii. 3rd rule: allow-ssh-iap
    h. Source filter: IPv4 ranges
    i. Source IPv4 ranges:
        i. 1st and 2nd rule: 0.0.0.0/0
        ii. 3rd rule: 35.235.240.0/20 (IAP range)
    j. Protocols and ports:
        i. Check TCP
        ii. Ports:
            1. 1st and 3rd: 22
            2. 2nd: 8080
5. Create a VM (target) exposed to the internet through HTTPS.
    a. Network tags: allow-ssh, allow-8080
    b. Network interfaces: Edit default
        i. Network: your newly created vpc
        ii. Subnetwork: your newly created subnet
        iii. External IPv4 address: Ephemeral
6. Deploy a second VM (attacker) allowing access from 35.235.240.0/20, port: 22. Allow Internet outbound access using a NAT.
    a. Network tags: allow-ssh-iap
    b. Network interfaces: Edit default
        i. Network: your newly created vpc
        ii. Subnetwork: your newly created subnet
        iii. External IPv4 address: None
7. Update the Log Sink created before to include vpc flow logs

8. SSH to the attacker VM and scan the target VM using nmap (use the internal and external IP)

Shell

```
sudo apt update
sudo apt install nmap
nmap -Pn <target_internal_ip>
nmap -Pn <target_external_ip>
```

9. Explore the newly created table in the destination dataset
10. Create a query to detect port scanning activity

3. Automate lab setup using Terraform for reproducible environments

Steps:

1. Create VPC, Subnets (with enabled log configuration) and Router, Nat and the required Firewalls
2. Create the Compute Instances
3. Enable Audit Logs Configuration
4. Create a Bigquery Dataset
5. Create Log Sink for VPC Flow Logs and Audit Logs (Grant the log sink writer permission to write to BigQuery)
6. How would you enforce Audit Logs at the organization level?

Lab Resources:

- Logging query language
- Understanding audit logs
- GCP Flow Logs
- Terraform Provider for GCP
- Introduction to the Organization Policy Service