
King

Detection and Incident Response in the Cloud

Google Cloud Platform

Diana Kramer

Senior Security Engineer

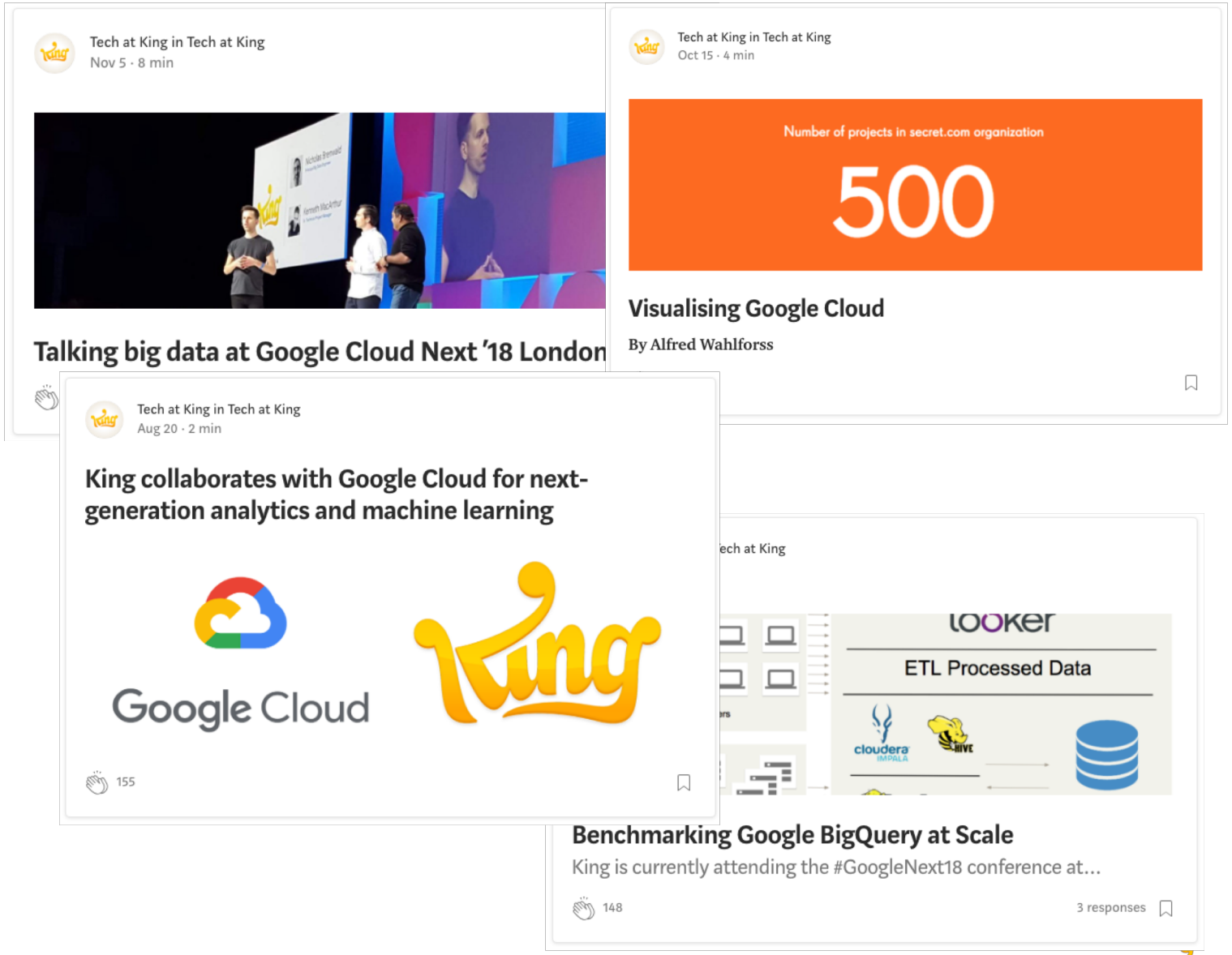
Content

- Overview of GCP
- Detection
  - Logging and Telemetry
  - Alerting
  - Cloud Security Command Center
- Investigation
  - Admin Activity
  - User Access to Resources
  - Traffic
- Containment

Google Cloud Platform

King in GCP

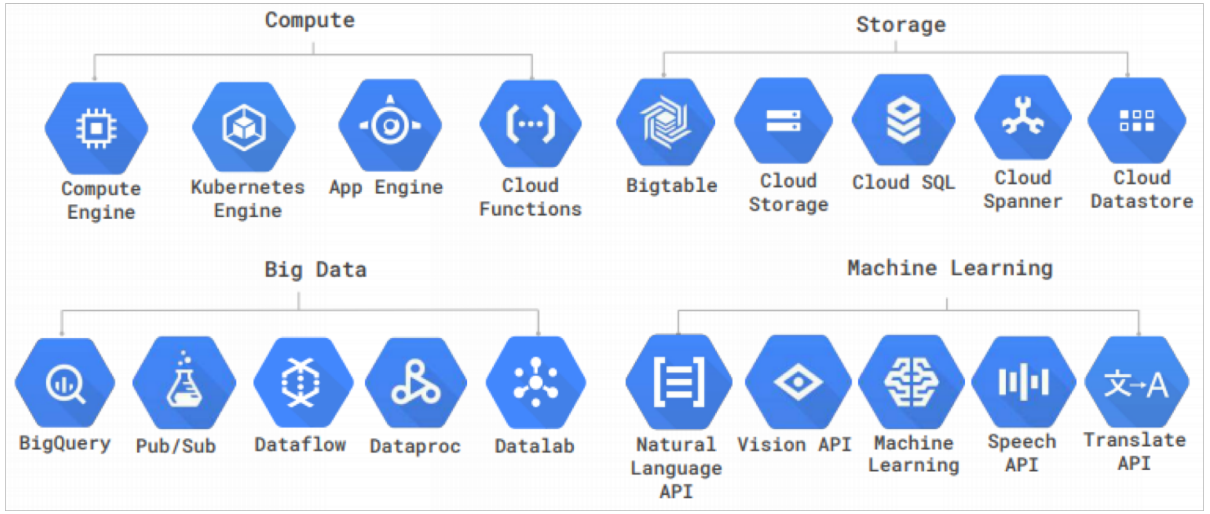
- Numbers
- Big Data
  - 33,7 millions Candy hammers
  - 50 billion daily events
  - 500k events/second
  - Biggest Hadoop cluster in Europe
- Machine Learning
  - Virtual players
  - 25 millions game rounds

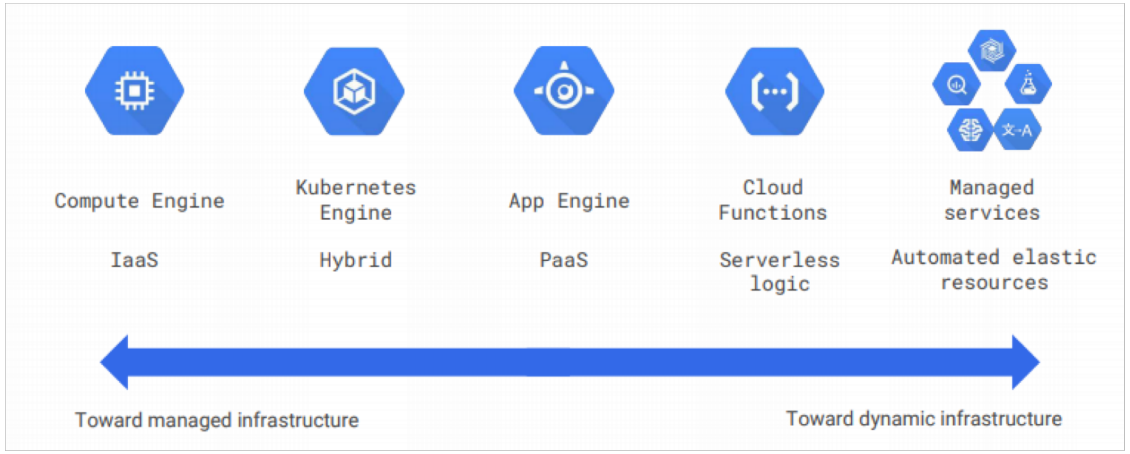


https://medium.com/@TechKing

GCP Services

- Services
  - Compute
  - Storage
  - Big Data
  - Machine Learning
- What problem do we have?
  - Shared Responsibility
  - Controls
  - News
- How do we solve it?
  - GCP native tools

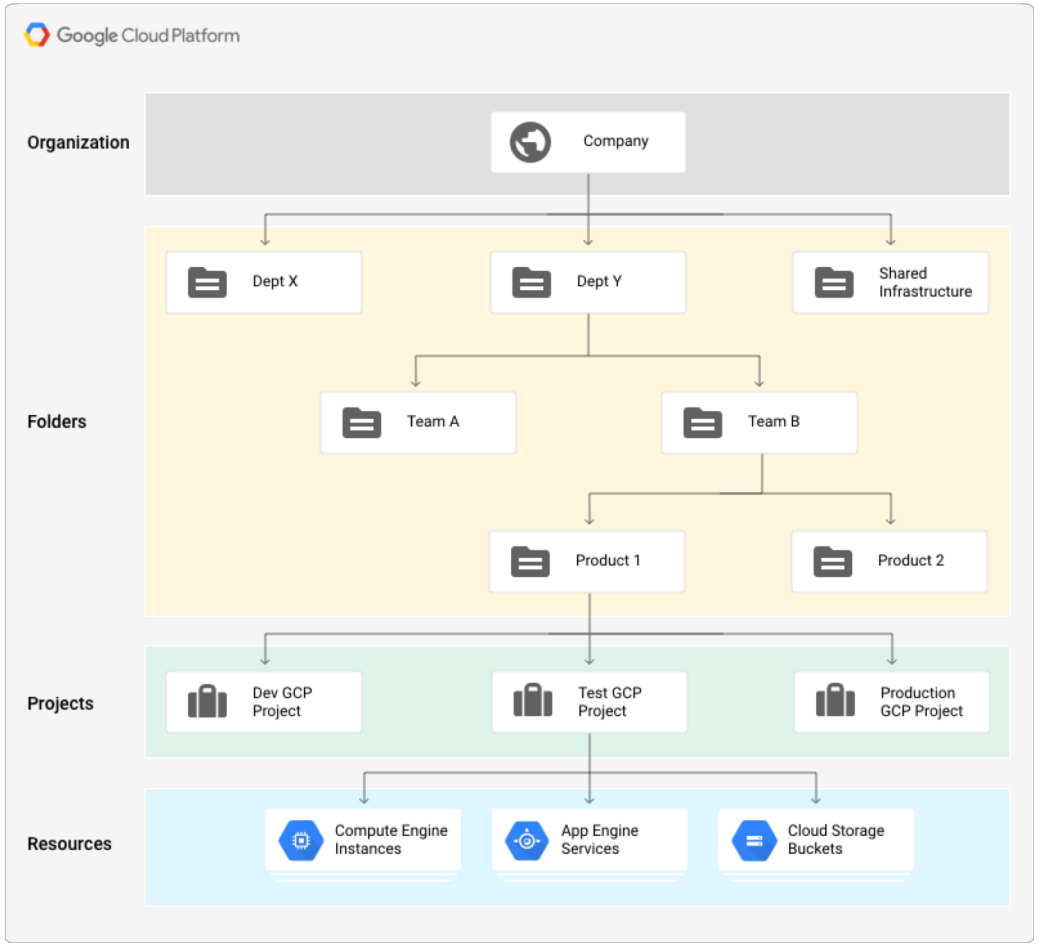




https://cloud.google.com/products/

Resource Hierarchy

- Resource Hierarchy
  - Organization
  - Folders
  - Projects
- Project
  - Contain resources
  - Project owner rules
  - Independent
  - Communication between projects
    - Managed services
    - Shared VPC



https://cloud.google.com/resource-manager/docs/cloud-platform-resource-hierarchy

Logging and Telemetry

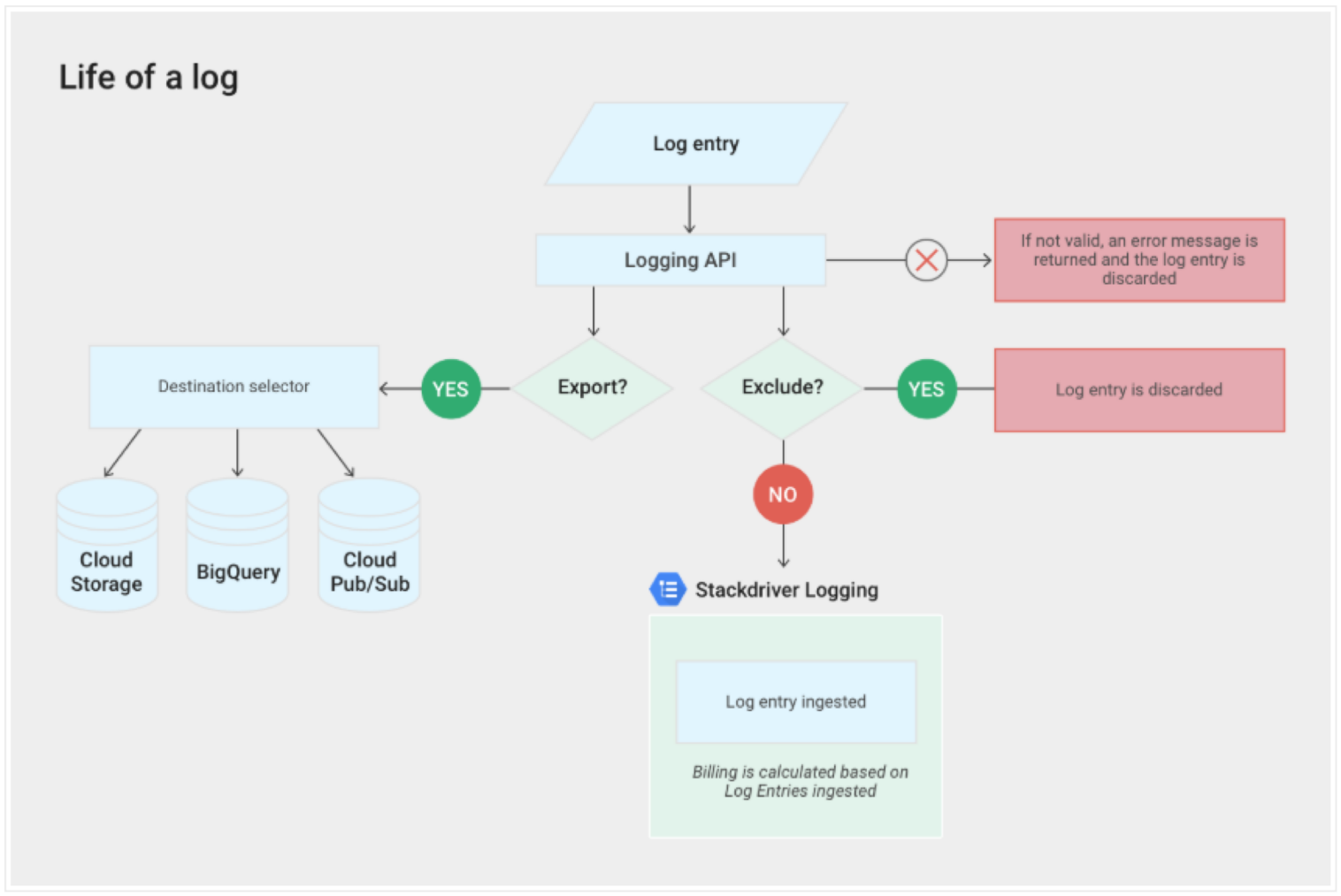
- Cloud Audit Logging
  - Admin Activity
  - System Event
  - Data Access
- BigQuery Data Access
- Application logs
  - AppEngine requests
  - Functions execution, etc
- VPC Flows
  - Reports on all TCP and UDP flows
  - Samples every 5 seconds
  - 5-tuple, volume, information about project, VM, VPC
  - No performance impact
- Firewall logs (BETA)
  - 5-tuple and information about project and rule
  - Only for GCE
  - No performance impact

LOG ALL FOREVER AND EVER

https://cloud.google.com/logging/docs/audit/

Alerting

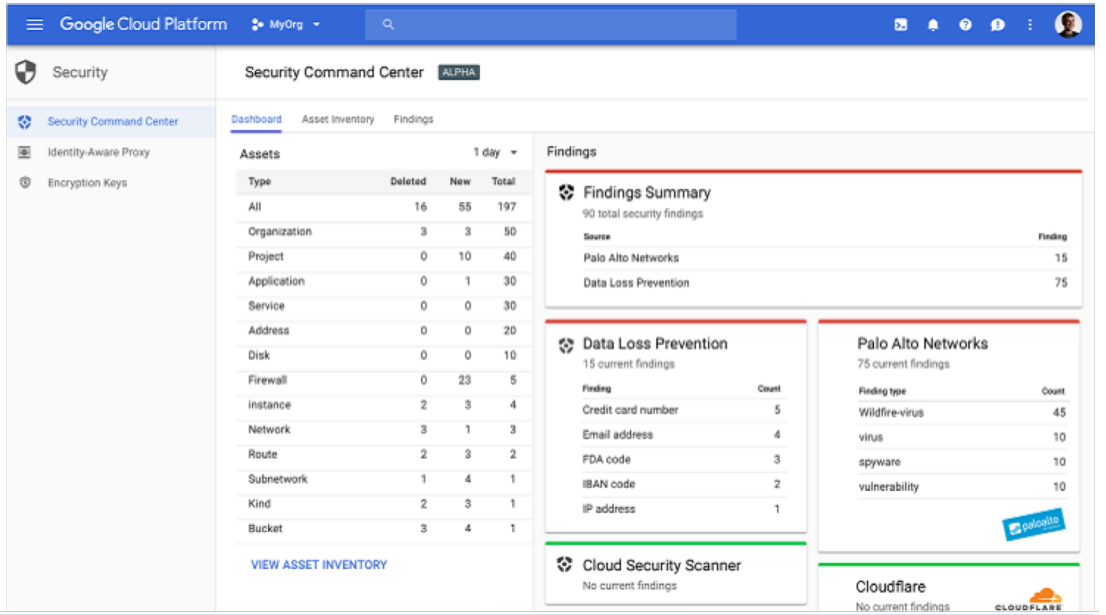
- Log Collection
  - Stackdriver
  - SIEM
  - BigQuery
- Alerts
  - Firewall and VPC flows changes
  - IAM changes on selected projects
  - Public buckets and objects
  - Creation of uncompliant VM
  - Denied bucket and object access
  - Non-domain accounts accessing GCP
  - Large outbound transfers



https://cloud.google.com/vpc/docs/using-flow-logs, https://cloud.google.com/vpc/docs/using-firewall-rules-logging

Cloud Security Command Center (BETA)

- Asset Inventory
  - Asset metadata
  - IAM policies
    - Ownership of resources
  - Services per project
  - VMs per project
- Security Sources
  - AppEngine vulnerability scanner
  - DLP API
  - 3rd party tools
- Anomaly Detection from Google
- Notification and alerting



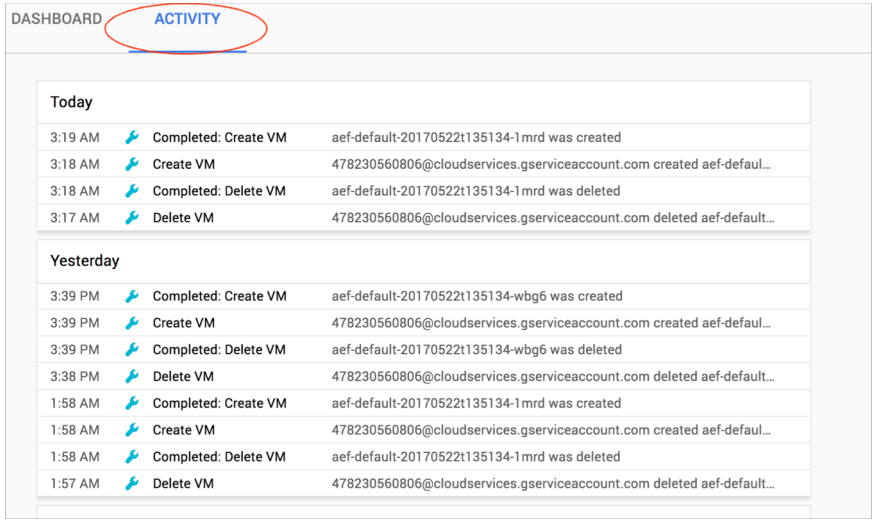
https://cloud.google.com/security-command-center/

Admin Activity

- Activity performed by admin over resources
  - Resource creation, IAM permissions, etc
  - Information
    - callerIP
    - UserAgent
    - methodName
    - resourceName
    - projectName
    - Specific information per log (FW IP addresses added, etc)

- Admin Activity logs for a single Compute Engine VM instance:

```
resource.type = "gce_instance" AND
resource.labels.instance_id = "[INSTANCE_ID]" AND
logName  =
"projects/[PROJECT_ID]/logs/cloudaudit.googleapis.com%2Factivity "
```



https://cloud.google.com/logging/docs/audit

User Access to Data

- Data accessed by the user
  - Not enabled by default (per service)
  - API calls that create, modify or read user-provided data
    - Which users and accounts performed various GCP calls/actions
    - When/where the calls occurred (date/time, region)
    - Who called/made them (region/location, source IP, user agent, user name, etc)
  - Information
    - callerIP
    - UserAgent
    - methodName
    - resourceName
    - projectName
    - authorizationInfo.granted

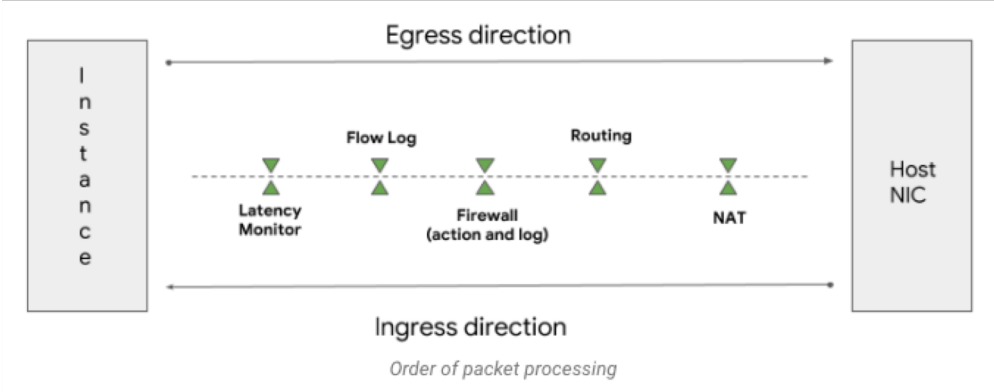
- Data Access logs for a single GCS Bucket by a user:

resource.type = "gcs_bucket" AND
resource.labels.bucket_name = "[BUCKET_NAME]" AND
authenticationInfo.principalEmail = "[EMAIL]" AND
logName = "projects/[PROJECT_ID]/logs/cloudaudit.googleapis.com%2Fdata_access"

https://cloud.google.com/logging/docs/audit/configure-data-access

Traffic to/from VM

- Connection
  - src_ip, src_port, dest_ip, dest_port, protocol
- Traffic volume
  - bytes_sent, packets_sent
- VPC Network Details
  - project_id, vpc_name, subnetwork_name



https://cloud.google.com/vpc/docs/using-flow-logs

- Traffic for a specific VM

resource.type="gce_subnetwork"
logName="projects/{#project_id}/logs/compute.googleapis.com%2Fvpc_flows"
jsonPayload.src_instance.vm_name="{#vm_name}"

- Traffic for a specific port and protocol

resource.type="gce_subnetwork"
logName="projects/{#project_id}/logs/compute.googleapis.com%2Fvpc_flows"
jsonPayload.connection.src_port={#port}
jsonPayload.connection.protocol={#protocol}

- Traffic for a specific prefix

resource.type="gce_subnetwork"
logName="projects/{#project_id}/logs/compute.googleapis.com%2Fvpc_flows"
ip_in_net(jsonPayload.connection.dest_ip, {#subnet})

Containment

- Preparation
  - Create Incident Responder IAM role
    - Read-Only
  - Create Isolated VPC
    - Set up VPC without any routes or only a route to internet
      - Ensure zero communications is allowed between this isolation VPC and others
    - Enable Monitoring
      - VPC Flows
      - Firewall logs
  - Create dedicated GCS Bucket for collected images
  - Clear ownership/responsability of resources
- Compute Engine VM Instances
  - Add VM instance to Isolated VPC
  - Export image to bucket
- Managed Services
  - Change IAM permissions
  - Disabled user
- Enforcing
  - Automate
    - Scripts
    - Functions
    - 3rd party tools

https://cloud.google.com/compute/docs/images/export-image,

Thank you!