

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

The collage consists of four separate Medium.com post cards:

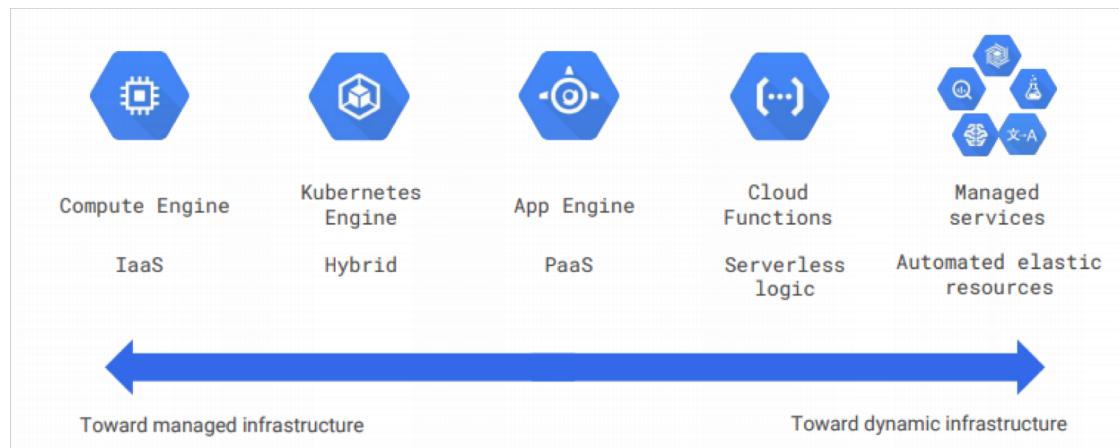
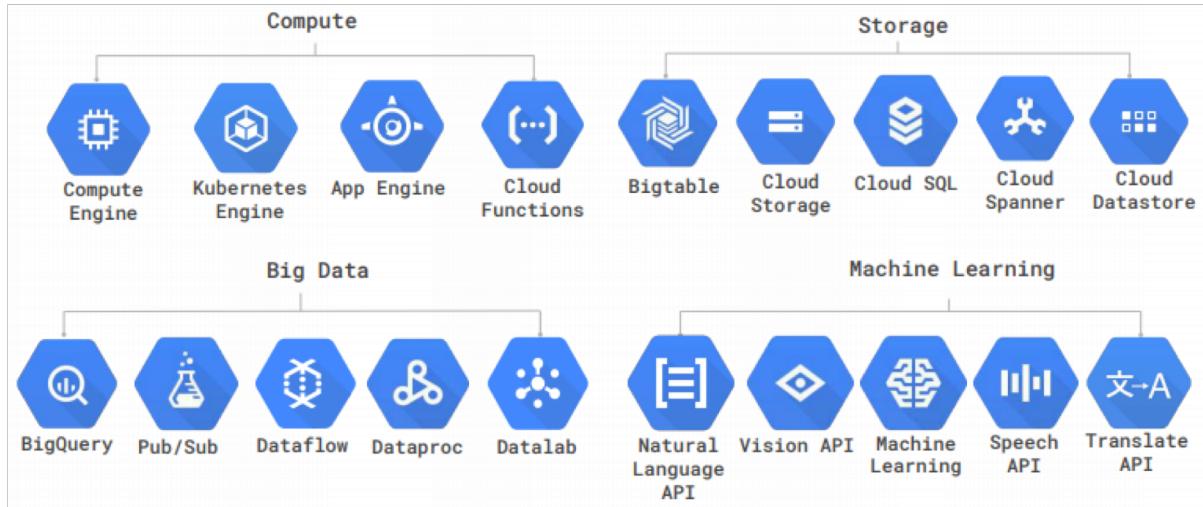
- Talking big data at Google Cloud Next '18 London** (Nov 5, 8 min) - A photo of three people on stage at Google Cloud Next '18 London. One person is speaking, and two others are listening. The background features a large screen with the King logo and names like "Vicente Hernández" and "Koenen Hackatur".
- Visualising Google Cloud** (Oct 15, 4 min) - An orange-themed post card showing the number "500" in white, representing the number of projects in secret.com organization.
- King collaborates with Google Cloud for next-generation analytics and machine learning** (Aug 20, 2 min) - A post featuring the Google Cloud logo and the King logo side-by-side. It discusses a collaboration between King and Google Cloud for analytics and machine learning.
- Benchmarking Google BigQuery at Scale** (King is currently attending the #GoogleNext18 conference at...) - A post card showing a flowchart of data processing from "ETL Processed Data" through "cloudera IMPALA" and "HIVE" to a "looker" database icon.

<https://medium.com/@TechKing>



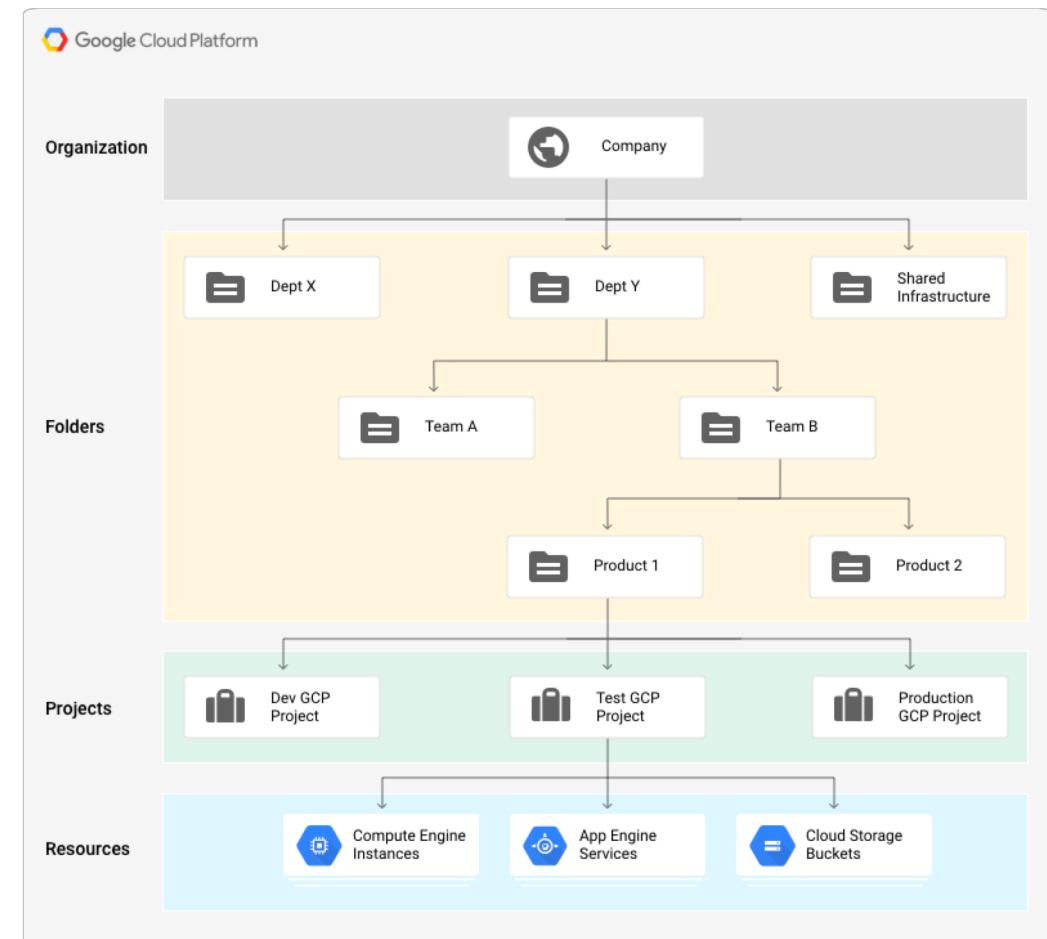
GCP Services

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



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>

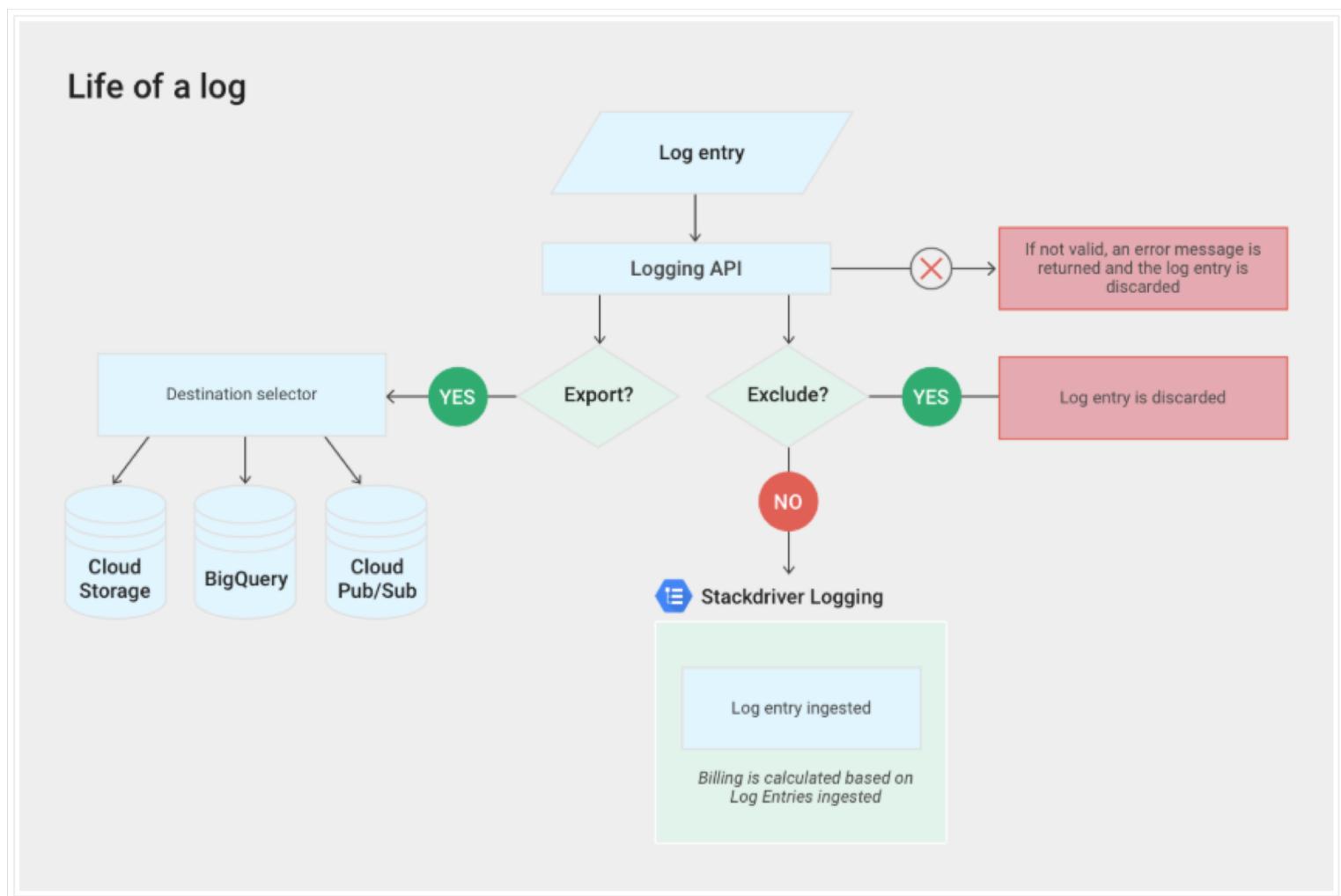
Logging and Telemetry

- 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

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



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

The top screenshot displays the Cloud Security Command Center (Alpha) dashboard. It includes a sidebar with 'Security' and 'Security Command Center' sections, and a main area with tabs for 'Dashboard', 'Asset Inventory', and 'Findings'. The 'Assets' section shows a table with columns for Type, Deleted, New, and Total. The 'Findings' section includes a 'Findings Summary' table and a 'Data Loss Prevention' table. The bottom screenshot shows the 'Assets' tab with a 'BETA' button and a 'RE-SCAN' button. It features a sidebar with navigation icons and a search bar. The main content area shows a table of assets, with the first row expanded to show details like resourceOwners, resourceType, and resourceProperties.name.

<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"
```

Today		
3:19 AM	Completed: Create VM	aef-default-20170522t135134-1mrd was created
3:18 AM	Create VM	478230560806@cloudservices.gserviceaccount.com created aef-default...
3:18 AM	Completed: Delete VM	aef-default-20170522t135134-1mrd was deleted
3:17 AM	Delete VM	478230560806@cloudservices.gserviceaccount.com deleted aef-default...
Yesterday		
3:39 PM	Completed: Create VM	aef-default-20170522t135134-wbg6 was created
3:39 PM	Create VM	478230560806@cloudservices.gserviceaccount.com created aef-default...
3:39 PM	Completed: Delete VM	aef-default-20170522t135134-wbg6 was deleted
3:38 PM	Delete VM	478230560806@cloudservices.gserviceaccount.com deleted aef-default...
1:58 AM	Completed: Create VM	aef-default-20170522t135134-1mrd was created
1:58 AM	Create VM	478230560806@cloudservices.gserviceaccount.com created aef-default...
1:58 AM	Completed: Delete VM	aef-default-20170522t135134-1mrd was deleted
1:57 AM	Delete VM	478230560806@cloudservices.gserviceaccount.com deleted aef-default...

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

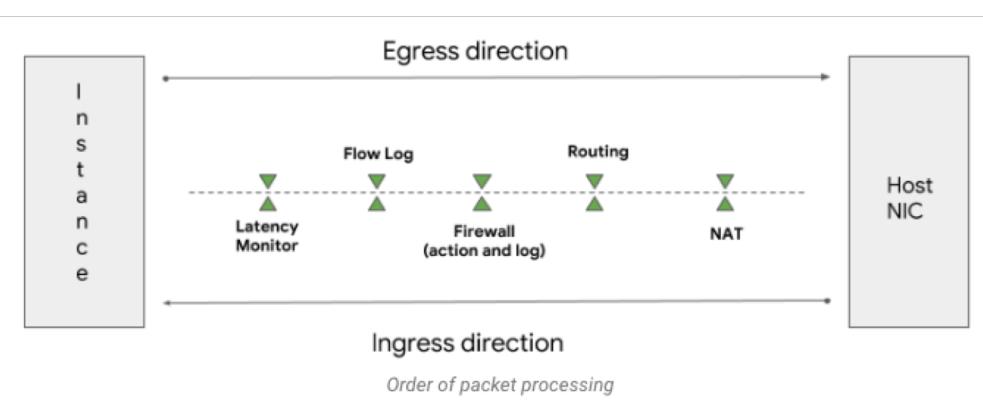
- Data Access logs for a single GCS Bucket by a user:

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

```
▼ protoPayload: {
    @type: "type.googleapis.com/google.cloud.audit.AuditLog"
    ▼ authenticationInfo: {
        principalEmail: "[REDACTED]"
    }
    ▼ authorizationInfo: [
        ▼ 0: {
            granted: true
            permission: "storage.buckets.get"
            resource: "projects/_/buckets/[REDACTED]"
            ▶ resourceAttributes: {...}
        }
    ]
    methodName: "storage.buckets.get"
```

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



- Traffic for a specific VM

```
resource.type="gce_subnetwork"
logName="projects/{#project_id}/logs/compute.googleapis.com%2Fvp
c_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%2Fvp
c_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%2Fvp
c_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



Thank you!