

FOR509 – Enterprise Cloud Forensics and Incident Response - Google Cloud

Topics

C

Capturing a VM Disk Image	5-80
Cloud Identity	5-19
Common attacks goals	5-79
Compute Overview	5-75

D

Data transfert pricing	5-15
Default logs	5-47
DFIR mission example	5-67

F

Filtering on IAM logs	5-39
Filtering on storage logs	5-111

G

gcloud	4-144
Collect Logs	5-66, 4-149
Service Account Permissions	4-146
gcp-organisation-admins	5-28
gcplot	5-38

H

Hunt for Data Exfiltration by bill	5-108
--	-------

I

Identity and Access Management	5-18
Challenges	5-26, 5-34
Identity Setup	5-19
Logical Grouping	5-27
Member(Users)	5-21
Owner vs Editor	5-33
Policy(Binding)	5-21, 5-25
Role(Permissions)	5-21, 5-23
Service Account	5-29, 5-31

K

Key Resources for DFIR	5-14
Kubernetes	5-135
AKS (Azure Kubernetes Service)	5-144

Architecture	5-141
Attacks (MITRE ATTCK)	5-149
Attacks in the cloud	5-153
ECS (Amazon Elastic Kebernetes Service) ..	5-144
EKS (Amazon Elastic Container Service) ..	5-144
GKE (Kubernietes Engine	5-144
klog	5-143
Logging Overview	5-143
Node	5-139
Pod	5-138

L

Log Cloud Pub/Sub	5-68
Log Explorer	5-49
Log Ingestion	5-48
Log Queueing Shipping	5-68
Log Retention (400 days)	5-47
Log Sinks	5-57
Create	5-62
Log Storage	5-48

O

Ops Agent	5-82
Fluent Bit	5-85
VM Agent Log example	5-90
Organisation Overview	5-10

P

Preemptible VM	5-78
----------------------	------

S

Shielded VM	5-78
Snapshot	5-80
Storage	5-96
Block Storage	5-96
Bucket	5-98
Attacking tool GCPBucketBrute	5-101
Audit logs	5-102
gsutils	5-105
Storage Logs	5-105, 106
Usage Logs	5-105, 106
Cloud Storage (Bucket)	5-96
File Storage	5-96

V

VPC	5-117
Firewall Rules	5-124
Flow logs	
Sampled logs	5-121
Packet Mirroring	5-126

