

FOR509 – Enterprise Cloud Forensics and Incident Response - AWS

Topics

A

Access Keys	3-49
Accessing AWS	3-19-20
API Calls that return Credentials	3-52
ARN (Amazon Resource Name)	3-11, 3-37
AssumedRole	3-34, 3-79
Athena	3-101, 3-111, 3-114
AWS Detective	3-115
AWS Load Balancers	3-88
Application Load Balancer	3-88
Classic AWS Load Balancer	3-88
Network Load Balancer	3-88
AWS Organisation	3-6-9
AWS System Manager	3-132

C

Capturing Linux Memory	3-133
Capturing Windows Memory	3-134
CloudTrail	3-24
90 days retention	3-24
IAM investigation examples	3-41
Access to the Console	3-42
Finding Exposed API Keys	3-51
New API Keys creation	3-44
Threat Hunting	3-54
Insights	3-31
logs fields for IR	3-33, 3-36
Logs retention 90d	3-26
Management Data Events	3-25
Pricing	3-32
Retrieve default logs	3-29
Retrieve logs from S3	3-30
Trail creation	3-27
User Agents	3-47
userIdentity Types	3-34
AssumedRole	3-34
AWSAccount	3-34
FederatedUser	3-34
UTC Timezone	3-24

E

EC2	3-61
Types	3-62
Elastic Block Store (EBS)	3-68
Elastic File Store (EFS)	3-78

G

Glue	3-101, 3-111, 112
GuardDuty	3-56

I

Identity and Access Management	3-11
1.Roles	3-11
2.Rules	3-11
3.Responsibilities	3-11
Account	3-12
ARN	3-11
Policy	3-13, 3-15
IAM Policy Simulator	3-16
Roles	3-13
Internet Gateways	3-87
IR account	3-6, 3-10
IR in Cloud	3-128

K

Kubernetes (EKS)	3-135
------------------------	-------

L

Lambda Functions	3-120
Logs sources	3-110

R

Root Account	3-7, 3-12
Route 53 : DNS	3-93

S

S3 Buckets	3-96
Access Restrictions	3-97
Logging	3-106
S3 Transfert Acceleration	3-5
Shared Responsibilities Model	3-20
Snapshots	3-72
CLI	3-74

T

Transfert Acceleration	3-101
------------------------------	-------

V

Virtual Private Cloud (VPC)	3-81, 3-84
AWS Load Balancers	3-88
Flowlogs	3-91
Internet Gateways	3-87

