FOR509 – Enterprise Cloud Forensics and Incident Response - General Theory

Topics

C

Cloud Access Options 1–54
Cloud Flows 1–56
Cloud Models & Logs (Iaas, Pass, Saas & Serverless & Containers) 1–46
Common attacks 1–45

D

DFIR in the Cloud 1–50

K

Key Logs for Investigations 1–53

M

Mitre ATT&CK Cloud version 1–43

P

Pricing 1–57

S

Shared Responsability Model 1–52
Snapshots 1–55
SOF-ELK 1–17
  Kibana Search Examples 1–33
  Kibana Search Process 1–22
  Supported logs 1–17

T

Terminology Across Clouds 1–60