

FOR509 – Enterprise Cloud Forensics and Incident Response - Google Workspace

Topics

A

Admin Audit Logs	4-93
Admin Investigator Tool	4-107
Admin Log Events	4-21
Anti Phishing & Malware solution	4-86
API Controls	4-110
API Permission	4-43

B

Blocked attachment types	4-68
--------------------------------	------

D

Domain Wide delegation	4-47
------------------------------	------

G

Gmail Export	4-80
Gmail Logs	4-61
Gmail Messages	4-61
Google Bault	4-70
Google Drive	
Audit Log Fields	4-129
Audit Log GUI Export	4-126
File recover	4-119
Investigation Tools	4-117
Logs Lag Time (none)	4-117
Logs Lag Time in investigation tool (12G+)	4-120
Groups	4-14, 4-23
GWS Editions	4-12
Plus	4-12
Standard	4-12
Starter/Essential	4-12

I

Inspecting Groups	4-26
-------------------------	------

L

Log Collection : API setup	4-41
1.API Persmission	4-43
2.OAuth Consebt Screen	4-45
3.Create Service Account	4-46
4.Authorise Service Account	4-47
5.Log Extraction Script	4-49
Log Collection : API vs Admin interface	4-35
Log Lag	4-31
Log Retentions	4-31
Log types	4-32

M

MFA Changes	4-95
Mitre ATT&CK	4-55

O

OAuth	4-102
Revoke Tokens	4-110
OAuth Abuse with 3rd party App	4-103
OAuth Consebt Screen	4-45
OAuth Log Events	4-106
Client Types	4-109
Product Bucket	4-109
OAuth Log Events via API	4-108
Organizational Units	4-14

S

Sending Logs to Google cloud	4-38
Service Account	4-46

T

Takeout	
Audit Logs	4-137
Customer Takeout	4-139
Export Process	4-136
Setup	4-135

U

User Audit Logs	4-95
User Log Events	4-99
User Login Types	4-98