FOR509 – Enterprise Cloud Forensics and Incident Response - M365

Topics

A

Azure Active Directory 1–101
- ADFS Sign-in Log 1–102
- Managed Identity Sign-in Log 1–102
- Non-interactive Sign-in Log 1–102
- Service Principal Sign-in Log 1–102
- Sign-in Log 1–102

Azure AD Attack Matrix 1–107
Azure AD Incident Response Steps 1–108

C

Crowdstrike Reporting Tool for Azure 1–132

E

Exchange
- ForwardingSMTPAddress 1–95
- Mail Clients 1–87
- MailItemsAccess 1–89
- Message Tracing 1–97-99

G

Graph API 1–117
- Refresh Token 1–125
- Risky Permissions 1–123

H

Hawk 1–114

M

MFSweep 1–106

S

SolarWinds Case Study 1–114
Sparrow 1–114

U

Unified Audit Log 1–66
- Collection Tools 1–75
- Exchange Auditing 1–86
- Last Audit Change 1–69
- Log Retention 1–70
- Microsoft Purview
  - Searching UAL 1–71
- Powershell 1–63
  - 1.Connecting 1–63
  - 2.Minimal Account Permissions 1–64
  - 3.UAL Searching 1–72-73
- Time Delay 1–67
- Turn on Audit Log 1–69
- Workloads 1–76
  - Exchange 1–83-85
  - OneDrive 1–80
  - Sharepoint 1–79
  - Teams 1–81-82