Syllabus
Overview of Cloud based SIEM/SOAR
Azure Sentinel
Defining Azure Security Architecure

Topics to choose from
Understand Modern SIEM Architecture
Understand SOAR Concepts
Traditional SOC Challenges
Understand Sentinel
Overview of Sentinel Portal
Log Analytics Workspace
Data connectors
Workbooks
Sentinel Analytics Rules
Investigating Incidents
Sentinel Threat Hunting
Auto Remediation Concept (SOAR Capability)
Demo showing how to create and investigate incident rules
Explaining the architecture of how Azure Components can be connected together (Azure Security Center,Office 365 Security,Azure Sentinel)