NAAN MUDHALVAN COURSE

UNIT I – INTRODUCTION TO SECURITY PRINCIPLES IN CLOUD COMPUTING

Introduction to cloud security lifecycle – Definition of cybersecurity in the cloud context – Roles and responsibilities of a cloud security analyst – Common security tools and automation for cloud environments – Digital transformation and its impact on security – Overview of foundational cloud concepts relevant to security.

UNIT II – STRATEGIES FOR CLOUD SECURITY RISK MANAGEMENT

Risk-management frameworks and security domains in the cloud – Compliance standards such as NIST CSF, HIPAA, SOC – Assessing risk, controls, and the compliance lifecycle in a cloud environment – Governance, policy creation and security controls for cloud infrastructure – Practical strategies to reduce cloud security risk.

UNIT III – CLOUD SECURITY RISKS: IDENTIFY AND PROTECT AGAINST THREATS

Identity management, access control and auditing (AAA) for cloud resources – Credential management, certificate handling and privilege escalation risk – Vulnerability management and threat identification in cloud-native environments – Data protection strategies, asset/inventory management and secure configurations.

UNIT IV – DETECT, RESPOND, AND RECOVER FROM CLOUD CYBERSECURITY ATTACKS

Logging, monitoring, alerting and incident detection in cloud environments – Security Information and Event Management (SIEM) and threat-feed integration – Incident response lifecycle, root cause analysis, business continuity and disaster recovery in the cloud – Post-incident analysis, lessons learned and future mitigation planning.

UNIT V – PUT IT ALL TOGETHER: PREPARE FOR A CLOUD SECURITY ANALYST JOB

End-to-end capstone simulation of a cloud security scenario – Integrating IAM, risk management, monitoring and incident response into a cloud security solution – Resume, portfolio and interview preparation for cloud security analyst roles – Professional behaviour, stakeholder communication and presentation of findings.