

Advanced Azure Security and Secure DevOps Practices

10-Days Custom Course Outline

Day 1: Advanced Identity and Access Management (Part 1)

- Advanced Identity and Access Management
- Conditional Access Policies
- Privileged Identity Management (PIM)
- Identity Protection
- Tools/Portals: Microsoft Entra ID Protection (formerly Azure AD Identity Protection)

Day 2 – Advanced Security Techniques (Part 2): Network Security

- Advanced Network Security
- Azure Application Gateway
- Web Application Firewall (WAF)
- Azure DDoS Protection
- Tools/Portals: Azure DDoS Protection
- Practical demonstration of network security configurations

Day 3 – Advanced Security Techniques (Part 3): Hybrid Network Security

- Azure VPN Gateway
- Azure ExpressRoute
- Secure hybrid connectivity
- Network security architecture and best practices
- Practical scenarios involving secure connectivity and network protection

Day 4 – Data Security and Governance

- Azure Information Protection (AIP)
- Microsoft Purview Information Protection
- Data Loss Prevention (DLP)
- Data classification and sensitivity labels
- Tools/Portals: Microsoft Purview

Day 5 – Advanced Threat Protection

- Azure Defender (now Microsoft Defender for Cloud)
- Microsoft Sentinel

- Integration with Microsoft Defender for Cloud
- Threat detection, security monitoring, and incident investigation
- Practical security monitoring demonstration

Day 6 – Secure DevOps Practices (Part 1): Infrastructure and CI/CD

- Infrastructure as Code (IaC)
- Continuous Integration and Continuous Deployment (CI/CD)
- Secure infrastructure deployment
- Security in CI/CD pipelines
- Secure deployment practices using Azure DevOps

Day 7 – Secure DevOps Practices (Part 2): Compliance and Risk Management

- Compliance and Risk Management
- Azure Policy
- Microsoft Purview Compliance Manager
- Risk Assessment and Mitigation
- Tools/Portals: Azure Policy and Compliance Manager
- Practical policy evaluation and compliance assessment

Day 8 – Multiple Applications and Use Cases (Part 1): Live Demonstrations

- Advanced Threat Detection with Microsoft Sentinel
- Automating Security Responses with Azure Logic Apps
- Tools/Portals: Microsoft Sentinel, Azure Logic Apps, and Azure DevOps
- Practical demonstration of security incident detection and automated response

Day 9 – Multiple Applications and Use Cases (Part 2): Case Studies and Best Practices

- Case Studies and Best Practices
- Real-World Security Scenarios
- Best Practices from Industry Leaders
- Incident response and security remediation scenarios
- Applying identity, network, data, and threat protection controls
- Q&A and Discussion

Day 10 – Review and Practical Application

- Review of Key Concepts
- Recap of Advanced Identity and Access Management
- Recap of Advanced Network Security
- Recap of Data Security and Governance
- Recap of Advanced Threat Protection
- Final Q&A and Course Wrap-Up