altkom akademia

training code: SC-5002 / ENG DL 1d / EN

Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls

Training recipients

The course is intended for people who plan to use Secure Azure services and workloads as part of the Microsoft Defender for Cloud compliance audit assessment, or for professionals who perform the tasks of Azure security engineers in their daily work. The course bridges the gap between entry-level skills and associate-level skills. The course will also be helpful for participants who wish to become familiar with IT roles, including infrastructure, security and networking.

Benefits

Acquiring knowledge and skills in practical securing Azure services and workloads, including:

- Filtering network traffic using a network security group.
- Create a Log Analytics workspace for Microsoft Defender for Cloud.
- Configuring Microsoft Defender for the Cloud.
- Configuring just-in-time (JIT) access to the virtual machine.
- Configuring and integrating the Log Analytics agent and workspace in Defender for Cloud.
- Configure Azure Key Vault network settings and perform a key vault restore with soft erase and wipe.

Training program

1. Filter network traffic with a network security group using the Azure portal.
    - Azure resource group.

  - Azure Virtual Network.
  - How network security groups filter network traffic.
  - Application security groups.
2. Create a Log Analytics workspace for Microsoft Defender for Cloud.
   - Defender for Cloud monitoring components.
3. Set up Microsoft Defender for Cloud.
   - Implement Microsoft Defender for Cloud.
   - Security posture.
   - Workload protections.
   - Deploy Microsoft Defender for Cloud
   - Azure Arc.
   - Azure Arc capabilities.
   - Microsoft cloud security benchmark.
   - Improve your regulatory compliance.
   - Configure Microsoft Defender for Cloud policies.
   - View and edit security policies.
   - Manage and implement Microsoft Defender for Cloud recommendations.
   - Explore secure score.
   - MITRE Attack matrix.
   - Define brute force attacks.
   - Understand just-in-time VM access.
   - Implement just-in-time VM access.
4. Configure and integrate a Log Analytics agent and workspace in Defender for Cloud.
   - Collect data from your workloads with the Log Analytics agent.
   - Configure the Log Analytics agent and workspace.
5. Configure Azure Key Vault networking settings
   - Azure Key Vault basic concepts.
   - Best practices for Azure Key Vault.
   - Azure Key Vault security.
   - Configure Azure Key Vault firewalls and virtual networks.
   - Azure Key Vault soft delete overview.
   - Virtual network service endpoints for Azure Key Vault.
6. Connect an Azure SQL server using an Azure Private Endpoint using the Azure portal.
   - Azure Private Endpoint.
   - Azure Private Link.

Expected preparation of the participant

- Hands-on experience in administering Microsoft Azure and hybrid environments.

• Good understanding of Azure computing, networking and security issues and knowledge of Microsoft Entra ID.
• Knowledge of security management and vulnerability remediation techniques.
• Knowledge of threat modeling and implementing threat protection measures..

Training Includes

- manual in electronic form available on the platform:
- https://learn.microsoft.com/pl-pl/training/
- access to Altkom Akademia's student portal

Duration

1 days / 7 hours

Language

- **Training**: English
- **Materials**: English