Course Name : Zero Trust
Duration : 24 Hours
Course Type : Koenig Originals

Course Overview:

The Microsoft Zero Trust training is a comprehensive program designed to equip participants with the knowledge and skills necessary to implement a Zero Trust security approach within their organizations. Zero Trust is a security model that focuses on protecting digital assets by assuming that no user or device should be trusted by default, regardless of their location or network environment. This training provides a deep understanding of Zero Trust concepts, principles, and best practices, along with hands-on experience in implementing Zero Trust solutions using Microsoft technologies.

Course Objectives:

1. Understand the fundamentals of Zero Trust security and its importance in today's evolving threat landscape.
2. Explore the core principles and components of the Microsoft Zero Trust framework.
3. Gain insights into identity-centric security and learn how to implement strong identity and access controls using Microsoft Azure Active Directory and related tools.
4. Discover techniques to secure devices and endpoints, including secure configuration, device health monitoring, and conditional access policies using Microsoft Endpoint Manager.
5. Learn about network segmentation, micro-segmentation, and secure network connectivity using Microsoft technologies such as Azure Virtual Networks and Azure Firewall.
6. Explore data protection strategies in a Zero Trust environment, including data classification, encryption, and data loss prevention (DLP) using Microsoft Information

Protection tools.

7. Understand the application-level security considerations in a Zero Trust architecture and learn to protect applications using Microsoft solutions such as Azure App Service and Azure Kubernetes Service.
8. Gain practical knowledge in monitoring, logging, and threat detection in a Zero Trust environment using Microsoft Defender for Endpoint and Azure Sentinel.
9. Learn best practices for incident response, remediation, and continuous security assessment and improvement within the context of Zero Trust.
10. Explore real-world case studies and examples to understand the practical implementation of Zero Trust using Microsoft technologies.

Course Modules:

Module 1: Introduction to Zero Trust

- Lesson 1: Understanding the Zero Trust security model
- Lesson 2: Benefits and principles of Zero Trust
- Lesson 3: Evolution of security architectures

Module 2: Zero Trust Identity

- Lesson 1: Identity as the foundation of Zero Trust
- Lesson 2: Identity verification and authentication
- Lesson 3: Role-based access control (RBAC)
- Lesson 4: Multi-factor authentication (MFA)
- Lesson 5: Identity and access management (IAM) solutions
- Lab: Implementing Zero Trust Identity Solutions

Module 3: Zero Trust Device

- Lesson 1: Device identification and trust evaluation
- Lesson 2: Device health and security assessment
- Lesson 3: Endpoint protection and management
- Lesson 4: Conditional access policies for devices

- Lesson 5: Device identity and access controls
- Lab: Securing Devices in a Zero Trust Environment

Module 4: Zero Trust Network

- Lesson 1: Network segmentation and micro-segmentation
- Lesson 2: Secure network connectivity (VPNs, SD-WAN)
- Lesson 3: Network monitoring and traffic analysis
- Lesson 4: Network access controls and policies
- Lesson 5: Software-defined perimeters (SDPs)
- Lab: Implementing Zero Trust Networking Solutions

Module 5: Zero Trust Data

- Lesson 1: Data classification and protection
- Lesson 2: Data encryption and data loss prevention (DLP)
- Lesson 3: Data access controls and permissions
- Lesson 4: Data governance and compliance
- Lesson 5: Data-centric security solutions
- Lab: Securing Data in a Zero Trust Environment

Module 6: Zero Trust Application

- Lesson 1: Application-level security controls
- Lesson 2: Application identity and authentication
- Lesson 3: Application security testing and scanning
- Lesson 4: Secure software development lifecycle (SDLC)
- Lesson 5: Application isolation and containerization
- Lab: Protecting Applications in a Zero Trust Environment

Module 7: Zero Trust Operations and Analytics

- Lesson 1: Zero Trust monitoring and logging
- Lesson 2: Threat intelligence and detection
- Lesson 3: Security analytics and behavior analysis
- Lesson 4: Incident response and remediation
- Lesson 5: Continuous security assessment and improvement
- Lab: Monitoring and Responding to Threats in a Zero Trust Environment

Module 8: Implementing Microsoft Zero Trust Solutions

- Lesson 1: Microsoft Zero Trust framework and architecture
- Lesson 2: Microsoft technologies and solutions for Zero Trust
- Lesson 3: Deploying and configuring Zero Trust components
- Lesson 4: Best practices for implementing Zero Trust with Microsoft tools
- Lesson 5: Case studies and real-world examples
- Lab: Implementing Microsoft Zero Trust Solutions

Module 9: Future Trends in Zero Trust

- Lesson 1: Emerging technologies in the Zero Trust space
- Lesson 2: Evolving threats and security challenges
- Lesson 3: Advancements in Zero Trust frameworks and solutions
- Lesson 4: Industry trends and predictions

Module 10: Conclusion

- Lesson 1: Recap of key concepts and takeaways
- Lesson 2: Importance of adopting a Zero Trust approach
- Lesson 3: Next steps for implementing Zero Trust in your organization