kod szkolenia: SC-100 / ENG DL 4d

Microsoft Cybersecurity Architect

Authorized Microsoft Cybersecurity Architect **SC-100** Distance Learning training.

Target audience:

- Administrator
- IT specialist
- IT security specialist

Purpose of the training

People who would like to be acquainted with the rules of designing and assessing the strategy of cybersecurity in the following areas: Zero Trust, Governance Risk Compliance (GRC), Security Operations (SecOps), as well as data and apllications. The participants also get familiar with the method of architecting solutions with the use of Zero Trust rules and specify security requirements for cloud infrastructure in various service models (SaaS, PaaS, IaaS). The course is specifically addressed to IT specialists who have a lot of experience and expertise in vast scope of areas of security engineering, including identity and acess, platform security, security operations. It is also recommended to have experience in implementing hybrid and cloud solutions. The course consists of such topics as:

- Designing Zero Trust strategy and architecture,
- Assessing technical strategies and security operation strategies in Governance Risk Management and Compliance (GRC),
- Designing infrastructure security,
- Designing strategy for data and applications.

Benefits of completing the training

Gaining knowledge and practical skills in area of security management on Microsoft platform. It includes:

- The process of designing strategies and Zero Trust architecture.
- Evaluation of technical strategies and strategies of security operations in the ara of Risk Management (GRC).
- The process of designing security for infrastructure.
- The process of designing strategies projektowania strategii dla danych i aplikacji.

Examination method

Egzamin w formie **on-line**. Zapis na stronie https://home.pearsonvue.com/Clients/Microsoft.aspx

Exam description

After the SC-100 course, you can take Microsoft certification exams:an Authorized Test Center,online being monitored by an offsite proctor. Details on the website:
https://docs.microsoft.com/en-us/certifications/exams/sc-100

Expected Listener Preparation

At least 2 years of experience from Managing Active Directory Infrastructure, 2 years of experience from managing cloud environment, possessing knowledge and expertise in a vast scope of security areas, including identity and access, platform security , security operations. It is also recommended to be experienced in hybrid and cloud implementations.
An ability to use English language materials.
To make work more convenient and training more effective we suggest using additional screen. Lack of extra screen does not make it impossible to participate in the training, but significantly influences the convenience of work during classes
Information and requirements conerning participation in distance learning trainings is available at: https://www.altkomakademia.pl/distance-learning/#FAQ

Training Language

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

Training Includes

* electronic handbook available at:
https://learn.microsoft.com/pl-pl/training/
* access to Altkom Akademia student portal

Training method:

- Lecture+workshops.

Czas trwania

4 dni / 28 godzin

Training agenda

1. Building general strategy and security architecture:
   - Introduction
   - Zero Trust review
   - Designing integration points in architecture
   - Designing security requirements based on business goals
   - Transposing security requirements to technical opportunities
   - Designing securities for vulnerability strategies
   - Planning security strategies for hybrid and multi-access strategies
   - Designing technical and management strategies for filtering and segmenting traffic
   - Acquaintance with protocol securities .
2. Designing security operation strategies:
   - Introduction
   - Understanding structure, processes and procedures related to security
   - Designing strategies of logging and audit strategies
   - Planning security operations for hybird and multi-cloud environments
   - Planning Security Information and Event Management (SIEM) strategy and security orchestration,
   - Evaluation of workflows related to security
   - Review of security strategies related to incident management
   - Evaluating strategy of security operations in terms of sharing information about technical threats
   - Monitoring sources to gain insight into threats and mitigation measures.

3. Designing strategies of identity security:
   - Introduction
   - Secure access to cloud resources
   - Security recommendations for dentity storage
   - Security recommendations for strategies of secure authentication and authorization
   - Secure conditional access
   - Designing strategies of assigning roles and delegating
   - Defining identity management for access reviews and authorization management
   - Designing security strategies for the role of priviliged access to infrastructure
   - Designing security strattegies for privileged operations
   - Acquaintance with protocol securities.
4. Evaluating rule compliance strategies:
   - Introduction
   - Interpreting requirements of compliance and their technical capabilities
   - Evaluating compliance's infrastructure using Microsoft Defender for Cloud
   - Interpreting evaluation of compliance and recommended operations to solve problmes or improve security
   - Designing and verifying Azure Policy implementations
   - Designing requirements in terms of data residences
   - Transposing requirements related to privacy into requirements related to security solutions.
5. Evaluating the state of security and recommended technical Risk Management strategies:
   - Introduction
   - Evaluating security attitude using comparisn tests
   - Evaluating state security using Microsoft Defender for Cloud
   - Evaluating security attitude using secure results
   - Evaluating security hygiene of Cloud Workloads
   - Designing securities for Azure Landing Zone
   - Interpreting the analysis of technical threates and recommended means limiting the risk
   - Recommended security functions or means of control in order to mitigate identified threats
6. Acquaintance with best practices related to architecture and their change in cloud:
   - Introduction
   - Planning and implementing security strategies in teams
   - Specifying strategies and the process of proactive and constant evolution of security strategy
   - Acquaintance with network protocols and best practices related to network segmentation and traffic filtering.
7. Designing strategy of securing server and client end points:
   - Introduction
   - Specifying fundamentals of security of server's and client's end points
   - Specifying security requirements for servers
   - Specifying security requirements for mobile devices and clients
   - Specifying requirements related to securing domain services in Active Directory
   - Designing strategy of managing secrets, keys and certificates

- Designing strategies of secure remote access
- Understanding structure, processes and security procedures
- Understanding procedures of deep forensics according to the type of resources.

8. Designing strategy of securing PaaS, IaaS and SaaS strategies:
   - Introduction
   - Specifying security fundamentals for PaaS services
   - Specifying security fundamentals for IaaS services
   - Specifying security fundamentals for SaaS services
   - Specifying requirements related to securities for IoT overloads
   - Specifying security fundamentals for data overloads
   - Specifying security fundamentals for Internet overloads
   - Specifying security fundamentals for mass storage overloads
   - Specifying security fundamentals for containers
   - Specifying security fundamentals for containers orchestration.
9. Specifying security fundamentals for applications:
   - Introduction
   - Understanding application threat modelling
   - Specifying priorities of threats for applications
   - Specifying security standards during new application implementation
   - Specifying security strategy for applications and API interfaces.
10. Planning data security strategy:
    - Introduction
    - Prioritetization of data threat mitigation
    - Planning strategy of identification and sensitive data protection
    - Specifying data coding standard at rest and in motion.