+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 15/04/2024

Sign up

SC-100© Certification Training

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

4 days (28 hours)

Presentation

In a world where hackers are very creative, invest in cybersecurity to ensure a secure future for your company. With Microsoft Cybersecurity Architect (SC-100)© certification, you can prove your skills in the field of security.

During the course, you'll explore identity and access security with Azure Active Directory, data protection with Azure Information Protection, and threat management with Microsoft Defender.

This certification develops your skills in designing and implementing cybersecurity solutions based on Microsoft technologies, equipping you with the knowledge you need to effectively protect your IT environments against threats.

Boost your career with this specialized training that will guarantee you new opportunities. We'll prepare you for the Microsoft exam.

Objectives

- Creating effective security operations
- Preparing for the SC-100© exam
- Mastering the implementation of security strategies

Target audience

- Cybersecurity Consultant
- Auditors
- Cybersecurity Analyst
- Cloud engineers

Prerequisites

- Practical experience in IT security
- Good understanding of Microsoft Azure technologies

Note: Ambient IT is not the owner of Microsoft Cybersecurity Architect (SC-100)©, this certification belongs to *Microsoft*©, Inc.

SC-100® training program

Designing a global security strategy and architecture

- Introducing Zero Trust
- Developing integration points in an architecture
- Develop safety requirements based on business objectives
- Translating safety requirements into technical capabilities
- Designing safety for a resilience strategy
- Design a security strategy for hybrid and multi-tenant environments
- Design technical aspects and governance strategies for traffic filtering and segmentation
- Understanding protocol security

Create a security operations strategy

- Safety operations processes and procedures
- Design a security, logging and auditing strategy
- Develop security operations for hybrid and multi-cloud environments
- Design a security information and event management (SIEM) strategy
- Evaluate safety workflows
- Review security strategies for incident management
- Evaluate security operations strategy to share technical threat intelligence
- Monitor sources for information on threats and mitigation measures

Creating an identity security strategy

- Secure access to cloud resources
- Recommend an identity store for security
- Recommend secure authentication and authorization strategies
- Secure conditional access
- Design a role assignment and delegation strategy

Assessing a regulatory compliance strategy

- Tracking the requirements lifecycle
- Monitor the progress of requirements
- Update requirement statuses
- Communicating the status of requirements
- Managing requirement changes

Cloud architecture practices

- Secure access to cloud resources
- Recommend an identity store for security
- Recommend secure authentication and authorization strategies
- Secure conditional access
- Design a role assignment and delegation strategy

Data security strategy

- Prioritizing the mitigation of data threats
- Design a strategy to identify and protect sensitive data
- Specify an encryption standard for data at rest and in motion

Safety posture and technical strategies

- Evaluate safety postures using references
- Assessing security postures with Microsoft Defender for Cloud
- Evaluate safety postures using safety scores
- Assessing the safety hygiene of cloud workloads
- Designing safety for an Azure landing zone
- Interpreting technical information on threats
- Recommend capacities or safety controls

Application security requirements

- Understanding application threat modeling
- Specify priorities for mitigating threats to applications
- Specify a security standard for the integration of a new application
- Specifying a security strategy for applications and APIs

Strategy for securing server and client endpoints

- Specify security baselines for server and client endpoints

- Specifying requirements
  - security for mobile devices and customers
  - security for servers
  - to secure Active Directory domain services
- Understand security operations frameworks, processes and procedures
- Understand in-depth investigation procedures by resource type

Strategies for exam success

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.

Training organization registered under number 11 75 54743 75. This registration does not imply government approval.
Ambient IT 2015-2024. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg