Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow Enterprise Computing Solutions Ltd, Part 1st Floor, Suite 1D/1, Central House, Otley Road, Harrogate, HG3 1UG

Email: educationteam.ecs.uk@arrow.com
Phone: 0870 251 1000

SC-100T00: Microsoft Cybersecurity Architect

CODE:	LENGTH:	PRICE:
MCS_SC-100T00	32 Hours (4 days)	£2,545.00

Description

This course prepares students with the background to design and evaluate cybersecurity strategies in the following areas: Zero Trust, Governance Risk Compliance (GRC), security operations (SecOps), and data and applications. Students will also learn how to design and architect solutions using zero trust principles and specify security requirements for cloud infrastructure in different service models (SaaS, PaaS, IaaS).

Objectives

Skills gained
• Design a Zero Trust strategy and architecture
• Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies
• Design security for infrastructure
• Design a strategy for data and applications

Audience

IT professionals with advanced experience and knowledge in a wide range of security engineering areas, including identity and access, platform protection, security operations, securing data, and securing applications. They should also have experience with hybrid and cloud implementations.

Prerequisites

Before attending this course, students must have:
• Advanced experience and knowledge in identity and access, platform protection, security operations, securing data and securing applications.
• Experience with hybrid and cloud implementations.

Programme

Module 1: Build an overall security strategy and architecture
Learn how to build an overall security strategy and architecture.
Lessons
• Introduction
• Zero Trust overview
• Develop Integration points in an architecture
• Develop security requirements based on business goals
• Translate security requirements into technical capabilities
• Design security for a resiliency strategy
• Design a security strategy for hybrid and multi-tenant environments
• Design technical and governance strategies for traffic filtering and segmentation
• Understand security for protocols
• Exercise: Build an overall security strategy and architecture
• Knowledge check
• Summary
After completing this module, students will be able to:
• Develop Integration points in an architecture
• Develop security requirements based on business goals
• Translate security requirements into technical capabilities
• Design security for a resiliency strategy

• Design security strategy for hybrid and multi-tenant environments
• Design technical and governance strategies for traffic filtering and segmentation
Module 2: Design a security operations strategy
Learn how to design a security operations strategy.
Lessons
• Introduction
• Understand security operations frameworks, processes, and procedures
• Design a logging and auditing security strategy
• Develop security operations for hybrid and multi-cloud environments
• Design a strategy for Security Information and Event Management (SIEM) and Security Orchestration,
• Evaluate security workflows
• Review security strategies for incident management
• Evaluate security operations strategy for sharing technical threat intelligence
• Monitor sources for insights on threats and mitigations
After completing this module, students will be able to:
• Design a logging and auditing security strategy
• Develop security operations for hybrid and multi-cloud environments.
• Design a strategy for Security Information and Event Management (SIEM) and Security Orchestration, A
• Evaluate security workflows.
• Review security strategies for incident management.
• Evaluate security operations for technical threat intelligence.
• Monitor sources for insights on threats and mitigations.
Module 3: Design an identity security strategy
Learn how to design an identity security strategy.
Lessons
• Introduction
• Secure access to cloud resources
• Recommend an identity store for security
• Recommend secure authentication and security authorization strategies
• Secure conditional access
• Design a strategy for role assignment and delegation
• Define Identity governance for access reviews and entitlement management
• Design a security strategy for privileged role access to infrastructure
• Design a security strategy for privileged activities
• Understand security for protocols
After completing this module, students will be able to:
• Recommend an identity store for security.
• Recommend secure authentication and security authorization strategies.
• Secure conditional access.
• Design a strategy for role assignment and delegation.
• Define Identity governance for access reviews and entitlement management.
• Design a security strategy for privileged role access to infrastructure.
• Design a security strategy for privileged access.
Module 4: Evaluate a regulatory compliance strategy
Learn how to evaluate a regulatory compliance strategy.
Lessons
• Introduction
• Interpret compliance requirements and their technical capabilities
• Evaluate infrastructure compliance by using Microsoft Defender for Cloud
• Interpret compliance scores and recommend actions to resolve issues or improve security
• Design and validate implementation of Azure Policy
• Design for data residency Requirements
• Translate privacy requirements into requirements for security solutions
After completing this module, students will be able to:
• Interpret compliance requirements and their technical capabilities
• Evaluate infrastructure compliance by using Microsoft Defender for Cloud
• Interpret compliance scores and recommend actions to resolve issues or improve security
• Design and validate implementation of Azure Policy
• Design for data residency requirements
• Translate privacy requirements into requirements for security solutions
Module 5: Evaluate security posture and recommend technical strategies to manage risk
Learn how to evaluate security posture and recommend technical strategies to manage risk.
Lessons
• Introduction
• Evaluate security postures by using benchmarks
• Evaluate security postures by using Microsoft Defender for Cloud
• Evaluate security postures by using Secure Scores
• Evaluate security hygiene of Cloud Workloads
• Design security for an Azure Landing Zone

• Interpret technical threat intelligence and recommend risk mitigations
• Recommend security capabilities or controls to mitigate identified risks
After completing this module, students will be able to:
• Evaluate security postures by using benchmarks
• Evaluate security postures by using Microsoft Defender for Cloud
• Evaluate security postures by using Secure Scores
• Evaluate security hygiene of Cloud Workloads
• Design security for an Azure Landing Zone
• Interpret technical threat intelligence and recommend risk mitigations
• Recommend security capabilities or controls to mitigate identified risks
Module 6: Understand architecture best practices and how they are changing with the Cloud
Learn about architecture best practices and how they are changing with the Cloud.
Lessons
• Introduction
• Plan and implement a security strategy across teams
• Establish a strategy and process for proactive and continuous evolution of a security strategy
• Understand network protocols and best practices for network segmentation and traffic filtering
After completing this module, students will be able to:
• Describe best practices for network segmentation and traffic filtering.
• Plan and implement a security strategy across teams.
• Establish a strategy and process for proactive and continuous evaluation of security strategy.
Module 7: Design a strategy for securing server and client endpoints
Learn how to design a strategy for securing server and client endpoints.
Lessons
• Introduction
• Specify security baselines for server and client endpoints
• Specify security requirements for servers
• Specify security requirements for mobile devices and clients
• Specify requirements for securing Active Directory Domain Services
• Design a strategy to manage secrets, keys, and certificates
• Design a strategy for secure remote access
• Understand security operations frameworks, processes, and procedures
• Understand deep forensics procedures by resource type
After completing this module, students will be able to:
• Specify security baselines for server and client endpoints
• Specify security requirements for servers
• Specify security requirements for mobile devices and clients
• Specify requirements for securing Active Directory Domain Services
• Design a strategy to manage secrets, keys, and certificates
• Design a strategy for secure remote access
• Understand security operations frameworks, processes, and procedures
• Understand deep forensics procedures by resource type
Module 8: Design a strategy for securing PaaS, IaaS, and SaaS services
Learn how to design a strategy for securing PaaS, IaaS, and SaaS services.
Lessons
• Introduction
• Specify security baselines for PaaS services
• Specify security baselines for IaaS services
• Specify security baselines for SaaS services
• Specify security requirements for IoT workloads
• Specify security requirements for data workloads
• Specify security requirements for web workloads
• Specify security requirements for storage workloads
• Specify security requirements for containers
• Specify security requirements for container orchestration
After completing this module, students will be able to:
• Specify security baselines for PaaS, SaaS and IaaS services
• Specify security requirements for IoT, data, storage, and web workloads
• Specify security requirements for containers and container orchestration
Module 9: Specify security requirements for applications
Learn how to specify security requirements for applications.
Lessons
• Introduction
• Understand application threat modeling
• Specify priorities for mitigating threats to applications
• Specify a security standard for onboarding a new application
• Specify a security strategy for applications and APIs
After completing this module, students will be able to:
• Specify priorities for mitigating threats to applications

• Specify a security standard for onboarding a new application
• Specify a security strategy for applications and APIs
Module 10: Design a strategy for securing data
Learn how to design a strategy for securing data.
Lessons
• Introduction
• Prioritize mitigating threats to data
• Design a strategy to identify and protect sensitive data
• Specify an encryption standard for data at rest and in motion
After completing this module, students will be able to:
• Prioritize mitigating threats to data
• Design a strategy to identify and protect sensitive data
• Specify an encryption standard for data at rest and in motion

Session Dates

On request. Please Contact Us

Additional Information

This training is also available as onsite training. Please contact us to find out more.