Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS, Nidderdale House, Beckwith Knowle, Harrogate, HG3 1SA

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

Implementing Microsoft Sentinel

CODE:	LENGTH:	PRICE:
MCS_WS-RDSCAZSENT	1 day(s)	Request Price

Description

This one-day course will cover how to secure and protect your assets with Microsoft Sentinel and discover how Microsoft brings hybrid security with the SIEM in Azure-based.

Objectives

2. Microsoft Sentinel & Defender product line integrations
Description of Content 1. Overview of Azure Core security features - M365 security and Sentinel
3. Collecting data from several sources 4. Chasing security issues
- Creating connection with data source - Hunting with KQL
- Monitoring results - View MITRE results and other alerts

Audience

This one-day course is aimed at administrators and IT professionals who want to deepen their know-how to carry out an implementation of SIEM in cloud-based and Azure Security concerns.

Prerequisites

Before attending this course, students must have:
- Good understanding of Microsoft Infrastructure elements
- Good knowledge of AAD and AD
- Good understanding of networking and security
- Understanding of TCP/IP v4
Demos are based on current version of products and could be in some cases, with interactive guides for attendees.

Programme

Module 1: “Overview of Azure Core security features”
This module discusses how to protect standard elements, such as VM, Containers, Storage on Azure & hybrid approach.
After completing this module, students will be able to:
- Understand what the Azure Core components
- Understand the basic security embedded on each Core components
Module 2: “Microsoft Sentinel & Defender product line integrations”
This module discusses the connection between Microsoft Sentinel and the Defender Product Line.
After completing this module, students will be able to:
- Create a link between Defender for Endpoint and Sentinel
- Supervise the results in Sentinel Console Module 3: “Collecting data from several sources”
This module discusses the way to manage other data sources with Sentinel and how to work with it into the solution.
After completing this module, students will be able to:
- Establish connections for 3rd party products
- Implement monitoring on data Module 4: “Chasing security issues”
This module discusseshow to prepare Microsoft Defender for Cloud and protect all elements (network and others), inside the resource groups.
After completing this module, students will be able to:
- Understand the usage of KQL for hunting
- Use MITRE and other resources to analyze security threats

Follow on courses

Microsoft Certified Security Operations Analyst SC-200

Session Dates

On request. Please contact us

Additional Information

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