Configure SIEM Security Operations Using Microsoft Sentinel – Intensive Training («SC5X1»)

Get started with Microsoft Sentinel security operations by configuring the Microsoft Sentinel workspace.

Duration: 1 day
Price: 900.–
Course documents: Official Microsoft Courseware on Microsoft Learn

Content

1 Create and maange Microsoft Sentinel workspaces
Learn about the architecture of Microsoft Sentinel workspaces to ensure you configure your system to meet your organization's security operations requirements.

2 Connect Microsoft services to Microsoft Sentinel
Learn how to connect Microsoft 365 and Azure service logs to Microsoft Sentinel.

3 Connect Windows hosts to Microsoft Sentinel
One of the most common logs to collect is Windows security events. Learn how Microsoft Sentinel makes this easy with the Security Events connector.

4 Threat detection with Microsoft Sentinel analytics
In this module, you learned how Microsoft Sentinel Analytics can help the SecOps team identify and stop cyber attacks.

5 Automation in Microsoft Sentinel
By the end of this module, you'll be able to use automation rules in Microsoft Sentinel to automated incident management.

6 Configure SIEM security operations using Microsoft Sentinel
In this module, you learned how to configure SIEM security operations using Microsoft Sentinel management.

Key Learnings

- Describing, installing and managing Microsoft Sentinel workspace architecture
- Connecting Microsoft service connectors, Azure Windows Virtual Machines and non-Azure Windows hosts to Microsoft Sentinel
- Configuring Log Analytics agent to collect Sysmon event
- Explaining the importance of Microsoft Sentinel Analytics and different types of analytics rules
- Creating rules from templates, new analytics rules and queries
- Managing rules with modifications.
- Explaining and creating automation options in Microsoft Sentinel
- Creating and configuring a Microsoft Sentinel workspace
- Deploying Microsoft Sentinel Content Hub solutions and data connectors
- Configuring Microsoft Sentinel Data Collection rules, NRT Analytic rule and Automation
- Performing a simulated attack to validate Analytic and Automation rules

Target audience

This course is aimed at Security Operations Analysts.

Additional information

This workshop is integrated into the course AZ-500: Microsoft Azure Security Technologies.

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-digital-transformation-technologies/cloud/microsoft-azure/course-configure-siem-security-operations-using-microsoft-sentinel-intensive-training