Configure SIEM Security Operations Using Microsoft Sentinel (SC-5001)

COURSE OVERVIEW

Get started with Microsoft Sentinel security operations by configuring the Microsoft Sentinel workspace, connecting Microsoft services and Windows security events to Microsoft Sentinel, configuring Microsoft Sentinel analytics rules, and responding to threats with automated responses.

WHO WILL BENEFIT FROM THIS COURSE?

Students wishing to configure SIEM security operations using Microsoft Sentinel.

PREREQUISITES

- Fundamental understanding of Microsoft Azure
- Basic understanding of Microsoft Sentinel
- Experience using Kusto Query Language (KQL) in Microsoft Sentinel

COURSE OBJECTIVES

- Create and manage Microsoft Sentinel workspaces
- Connect Microsoft services to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Threat detection with Microsoft Sentinel analytics
- Automation in Microsoft Sentinel
- Configure SIEM security operations using Microsoft Sentinel

COURSE OUTLINE

Module 1: Create and manage 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.

Module 2: Connect Microsoft services to Microsoft Sentinel

- Learn how to connect Microsoft 365 and Azure service logs to Microsoft Sentinel.

Module 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.

Module 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.

Module 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.

Module 6: Configure SIEM security operations using Microsoft Sentinel

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

WHY TRAIN WITH SUNSET LEARNING INSTITUTE?

Sunset Learning Institute (SLI) has been an innovative leader in developing and delivering authorized technical training since 1996. Our goal is to help our customers optimize their technology Investments by providing convenient, high quality technical training that our customers can rely on. We empower students to master their desired technologies for their unique environments.

What sets SLI apart is not only our immense selection of trainings options, but our convenient and consistent delivery system. No matter how complex your environment is or where you are located, SLI is sure to have a training solution that you can count on!

Premiere World Class Instruction Team

- All SLI instructors have a four-year technical degree, instructor level certifications and field consulting work experience
- Sunset Learning has won numerous Instructor Excellence and Instructor Quality Distinction awards since 2012

Enhanced Learning Experience

- The goal of our instructors during class is ensure students understand the material, guide them through our labs and encourage questions and interactive discussions.

Convenient and Reliable Training Experience

- You have the option to attend classes live with the instructor, at any of our established training facilities, or from the convenience of your home or office
- All Sunset Learning Institute classes are guaranteed to run – you can count on us to deliver the training you need when you need it!

Outstanding Customer Service

- You will work with a dedicated account manager to suggest the optimal learning path for you and/or your team
- An enthusiastic student services team is available to answer any questions and ensure a quality training experience

Interested in Private Group Training?

Contact Us