CLOUD COMPUTING AND VIRTUALISATION

Microsoft SC-5001 - Configure SIEM Security Operations using Microsoft Sentinel

LENGTH
1 day

VERSION
A

MICROSOFT AZURE AT LUMIFY WORK

Lumify Work is your best choice for training and certification in any of Microsoft's leading technologies and services. We've been delivering effective training across all Microsoft products for over 30 years, and are proud to be Australia's and New Zealand's first and largest Microsoft Gold Learning Solutions Partner. All Lumify Work Microsoft Azure courses follow Microsoft Official Curriculum (MOC) and are led by Microsoft Certified Trainers. Join more than 5,000 students who attend our quality Microsoft courses every year.

Microsoft Solutions Partner
Microsoft Cloud
Training Services

WHY STUDY THIS COURSE

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.

Microsoft Applied Skills

For more than 30 years, Microsoft's industry-recognised certifications have provided proof of world-class technical proficiency for in-demand job roles. In today's ever-changing business environment, there are also times when you need verified project-specific skills. Microsoft Applied Skills is a new verifiable credential that validates that you have the targeted skills needed to implement critical projects aligned to business goals and objectives. Applied Skills gives you a new opportunity to put your skills center stage, empowering you to showcase what you can do and what you can bring to key projects in your organisation. Prepare for your Applied Skills credential with this one-day, instructor-led training course.

WHAT YOU'LL LEARN

After completing this course, students will be able to:

- Describe Microsoft Sentinel workspace architecture
- Install Microsoft Sentinel workspace
- Create and configure a Microsoft Sentinel workspace
- Connect Microsoft service connectors
- Explain how connectors auto-create incidents in Microsoft Sentinel
- Connect Azure Windows Virtual Machines to Microsoft Sentinel
- Connect non-Azure Windows hosts to Microsoft Sentinel
- Configure Log Analytics agent to collect Sysmon events

https://www.lumifywork.com/en-ph/courses/microsoft-sc-5001-configure-siem-security-operations-using-microsoft/

CLOUD COMPUTING AND VIRTUALISATION

Microsoft SC-5001 - Configure SIEM Security Operations using Microsoft Sentinel

- Explain the importance of Microsoft Sentinel Analytics
- Create rules from templates
- Create new analytics rules and queries using the analytics rule wizard
- Manage rules with modifications
- Explain automation options in Microsoft Sentinel
- Create automation rules in Microsoft Sentinel
- Deploy Microsoft Sentinel Content Hub solutions and data connectors
- Configure Microsoft Sentinel Data Collection rules, NRT Analytic rule and Automation
- Perform a simulated attack to validate Analytic and Automation rules

My instructor was great being able to put scenarios into real world instances that related to my specific situation.

I was made to feel welcome from the moment I arrived and the ability to sit as a group outside the classroom to discuss our situations and our goals was extremely valuable.

I learnt a lot and felt it was important that my goals by attending this course were met.

Great job Lumify Work team.

AMANDA NICOL
IT SUPPORT SERVICES MANAGER - HEALTH WORLD LIMITED

https://www.lumifywork.com/en-ph/courses/microsoft-sc-5001-configure-siem-security-operations-using-microsoft/

CLOUD COMPUTING AND VIRTUALISATION

Microsoft SC-5001 - Configure SIEM Security Operations using Microsoft Sentinel

COURSE SUBJECTS

- 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

Lumify Work
Customised Training

We can also deliver and customise this training course for larger groups saving your organisation time, money and resources.

For more information, please contact us on 02 8286 9429.

https://www.lumifywork.com/en-ph/courses/microsoft-sc-5001-configure-siem-security-operations-using-microsoft/

CLOUD COMPUTING AND VIRTUALISATION

Microsoft SC-5001 - Configure SIEM Security Operations using Microsoft Sentinel

WHO IS THE COURSE FOR?

- Security Engineers
- Security Operations Analysts

PREREQUISITES

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

https://www.lumifywork.com/en-ph/courses/microsoft-sc-5001-configure-siem-security-operations-using-microsoft/