Masterclass: SOC Operations & Threat Detection Mastery: Complete Training Program

Duration: 3 Days **Course Code: SOC** **Delivery Method: Virtual Learning**

Overview:

The course is dedicated for people who want to learn about Microsoft's cloud environment monitoring tools and framework. At the beginning, you will be introduced to the management of Entra ID, service auditing and logs, roles related to monitoring threats in the cloud, or the implementation of PIM and PAM services.
The next module is to walk you through the secure score functionality and how to improve it with cloud security configuration best practices, Azure Defender for servers and security standards recommendations.
During the course you will be able to configure an environment with EDR enabled, where we will try to attack endpoints and user identity and see how EDR behaves. Then we will go through security operations best practices and make hunting queries.
The implemented EDR solution and other components of the security stack will be linked within the Microsoft SIEM - Sentinel, which will allow monitoring and implementation of responses to threats.

Updated 17/7/2026

Target Audience:

SOC analysts, Enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security.

Objectives:

- By the end of this course, you will be able to:
- Monitor and manage Microsoft Entra ID operations, auditing, and security logs.
- Configure and improve Microsoft 365 security posture using Secure Score and Azure Defender.
- Deploy and manage Microsoft Defender for Endpoint (EDR).
- Perform threat detection, incident management, and advanced hunting using Kusto Query Language (KQL).
- Implement and operate Microsoft Sentinel for SIEM, threat monitoring, and automated response.
- Configure Microsoft Cloud App Security (MCAS) to monitor, protect, and control cloud applications.
- Integrate Microsoft security solutions to build an end-to-end SOC workflow.

Prerequisites:

- To attend this training, you should have a good hands-on experience in administering Windows infrastructure and basic knowledge of public cloud concepts (Office 365, Azure).

Testing and Certification

- Participants receive a lifetime-valid CQURE certification with no renewal fees.
- Virtual certificates are issued via Accredible.
- The certificate entitles participants to collect CPE points.

Follow-on-Courses:

None

Content:

Module 1: Monitoring Operations in Entra ID

- Entra ID Operations and Logs
- Entra ID Roles
- Identity Protection
- Audit Logs
- Red team perspective on Entra ID settings
- Privileged Identity Management (PIM)
- Office Management API
- Azure Policies
- Labs

Module 2: Microsoft 365 Security

- Secure Score and Security Center
- Improving Secure Score
- Azure Defender for Servers
- Security Benchmark Policy
- STIG ; CIS cloud security baseline
- Labs

Module 3: Microsoft 365 Defender for Endpoint (EDR)

- EDR configuration and deployment
- Security operations best practices
- Incident management
- Kusto Query Language (KQL)
- Advanced Hunting
- Partner APIs
- Malware evasion techniques
- Attack and remediation labs
- Microsoft Defender for Identity integration
- Microsoft Defender for Office 365 integration

Module 4: eXtended Detection and Response with Microsoft Sentinel

- Sentinel fundamentals
- Dashboards and Connectors
- Normalization
- Architecture
- Workbooks
- Incidents
- KQL hands-on labs
- Auditing and monitoring
- Integration with Microsoft Cloud security stack
- Fusion ML detections
- Automated notebooks
- Python customization
- Detection rule conversion
- Sentinel innovations
- Security Center investigations
- Anomaly detection
- GitHub monitoring
- Threat hunting
- Threat Intelligence
- End-to-end SOC scenario

Module 5: Microsoft Cloud App Security (MCAS)

- MCAS introduction
- Secure remote work
- App Discovery and Log Collector
- Real-time monitoring and controls
- Third-party application integration
- Microsoft Flow automation
- Conditional Access App Control
- Threat detection
- Information Protection
- MCAS Labs
- DLP deployment and monitoring with MCAS and Sentinel

Further Information:

For More information, or to book your course, please call us on 00 971 4 446 4987

training@globalknowledge.ae

www.globalknowledge.com/en-ae/

Global Knowledge, Dubai Knowledge Village, Block 2A,First Floor, Office F68, Dubai, UAE