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, we will introduce you to the management of Azure Active Directory, service auditing and logs, roles related to monitoring threats in the cloud, or the implementation of PIM and PAM services.
In the next module we will walk through cloud security configuration best practices with secure score, Azure Defender for servers or 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, which will allow monitoring and implementation of responses to threats.

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

Testing and Certification

- What is wonderful about our certification is that it is lifetime valid with no renewal fees – the technology changes, but fundamentals and attitude remain mostly the same. Our Virtual Certificates, which entitle you to collect CPE Points, are issued via Accredible.

Content:

Module 1: Monitoring operations in Azure AD

1. Azure Active Directory Operations and Logs

2. Azure AD Roles

3. Identity Protection – Roles, Review access, alerts, Discovery and Insights

4. How to deal with Audit Log

5. Challenging Azure AD settings in Azure and Office from red team perspective

6. Privileged Identity Management – JITA, Discover and Monitor

7. Office Management API – Logs around Office 365

8. Microsoft Azure Policies – getting started, compliance, remediation, assignments, blueprints

9. Labs

Module 2: Microsoft 365 security

1. Secure Score and Security Center

2. Best Practices for Improving Your Secure Score

3. Azure Defender for Servers

4. Security Benchmark Policy

5. Labs

6. STIG ; CIS – cloud security baseline

Module 3: Microsoft 365 Defender for Endpoint – EDR

1. Intro 101 (configuration, device inventory,

3. How to manage Incidents

4. Kusto language 101 – basic and advanced queries

5. Advanced Hunting

6. Partner ; APIs

7. Hacker ways to hide malware and bypass EDR

8. Attacks examples and remediation labs

9. EDR Integration with Microsoft Defender for Identity

10. EDR Integration with Microsoft Defender for Office 365

Module 4: Extended Detection and Response with Sentinel

1. Sentinel 101 - Azure Sentinel Dashboards, Connectors

2. Understanding Normalization in Azure Sentinel

3. Cloud ; on-prem architecture

4. Workbooks deep dive - Visualize your security threats and hunts

5. Incidents

6. KQL intro (KQL hands-on lab exercises) and Optimizing Azure Sentinel KQL queries performance

7. Auditing and monitoring your Azure Sentinel workspace

8. Sentinel configuration with Microsoft Cloud stack, EDR and MCAS

12. Best Practices for Converting Detection Rules from Splunk, QRadar, and ArcSight to Azure Sentinel Rules

13. Deep Dive into Azure Sentinel Innovations

14. Investigating Azure Security Center alerts using Azure Sentinel

15. Customizable Anomalies and How to Use Them

16. Introduction to Monitoring SAP with Azure Sentinel for Security Professionals

17. Hunting in Sentinel

18. Deep Dive on Threat Intelligence

19. End-to-End SOC scenario with Sentinel

Module 5: Microsoft Cloud App Security

1. Intro do MCAS

2. Enabling Secure Remote Work

3. App Discovery and Log Collector Configuration

4. Extending real-time monitoring ; controls to any app

5. Connecting 3rd party Applications

6. Automation and integration with Microsoft Flow

7. Conditional Access App Control

8. Threat detection

9. Information Protection

10. Labs: Protect Your Environment Using

concept, Report, alerts) and EDR deployment

2. Security Operations best practices with Microsoft EDR

9. Fusion ML Detections with Scheduled Analytics Rules

10. Streamlining your SOC Workflow with Automated Notebooks

11. Customizing Azure Sentinel with Python

MCAS

11. DLP in Microsoft stack – how to deploy and monitor using MCAS and Sentinel

Additional Information:

Exercises
All exercises are based on Windows Server 2016 and 2019, Windows 10, Kali Linux and Azure Cloud. During the course our finest specialists will use their unique tools, over 100 pages of exercises and presentations slides with notes.

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK