Masterclass:

SOC Analyst Course

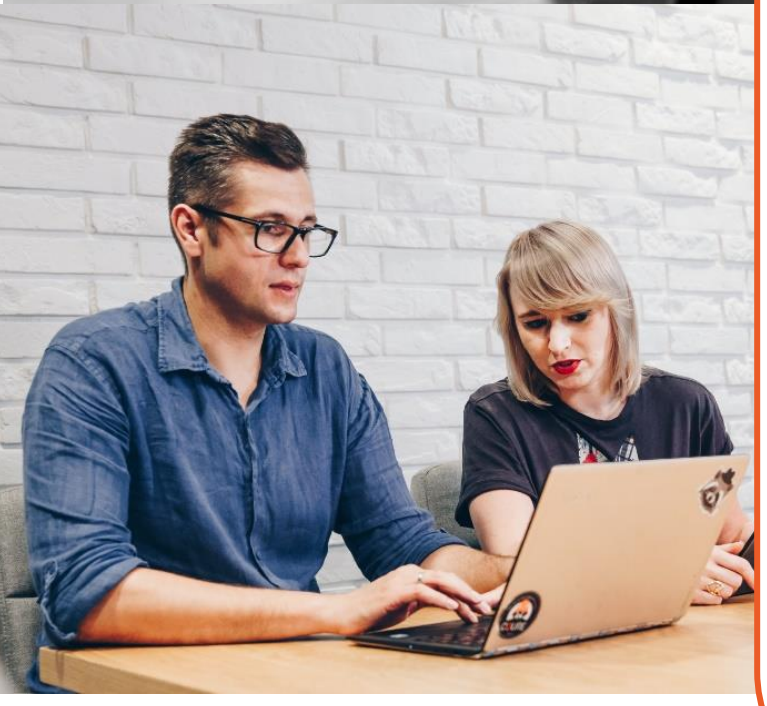
Duration: 5 days

Live Virtual Class

CQURE

info@cqure.pl

www.cqure.pl
www.cqureacademy.com



Mike Jankowski-Lorek, Ph.D. is a is a cybersecurity expert, solution architect, consultant, penetration tester and developer with more than 18 years of experience in the field. He designs and implements solutions for organization identity and access, databases, network and security monitoring and management, mainly working in Microsoft ecosystem for medium to enterprise-level organizations.

CQURE has been providing cybersecurity services and trainings since it was set up in Warsaw in 2008. Throughout the years, our services have reached a wide range of clients around the world, which allowed us to open new offices in New York (2013), Dubai (2014), and Zug (2016).

CQURE Academy is primarily a training program consisting of over 40 high-quality technical workshops and seminars, and providing certification to specialists. Additionally, in October 2016 CQURE has successfully launched online and subscription-based trainings.

CQURE Experts speak at the international events and engage in multiple cybersecurity projects – they bring their knowledge and experience from the field to the trainings. CQURE Academy also involves R&D – that is why CQURE Team is so recognizable in the cybersecurity field.

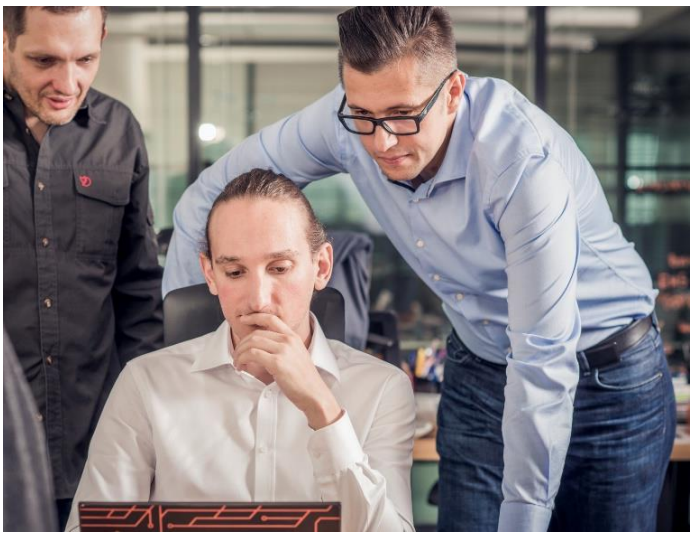
SOC Analyst Course

This is an international Live Virtual Class, which means you will share the learning experience in a group of IT pros from around the world! The class is taught in English by CQURE Cybersecurity Experts! Remember that this course is limited to 12 participants total to ensure the highest quality and unique learning experience! During this course you will have an opportunity to interact with the instructor and get their help with any problems you might encounter, just as if it was a regular class.

About The Course

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 Azure Active Directory, 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.

Duration: 5 days (35 hours)
Running hours: 9AM – 4PM (CET)

Loads of Knowledge

The course is an intense workshop! During these 5 days we recommend a good cup of coffee – this course is really intense and in order not to miss a thing you MUST stay awake!

Exercises

All exercises are based on **O365 and Azure Cloud**. During the course our finest specialists will use their unique tools, practical exercises and presentations slides with notes.

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.

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).

Agenda

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, concept, Report, alerts) and EDR deployment
2. Security Operations best practices with Microsoft EDR
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
9. Fusion ML Detections with Scheduled Analytics Rules
10. Streamlining your SOC Workflow with Automated Notebooks
11. Customizing Azure Sentinel with Python
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 GitHub 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 MCAS
11. DLP in Microsoft stack – how to deploy and monitor using MCAS and Sentinel

CQURE ACADEMY