Microsoft Security Operations Analyst (SC-200T00)

ID SC-200T00 **Price** CHF 3,380.—(excl. VAT) **Duration** 4 days

Who should attend

The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Sentinel, Microsoft Defender XDR, Microsoft Defender for Cloud, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

This course is part of the following Certifications

Microsoft Certified: Security Operations Analyst Associate (MCSOAA)

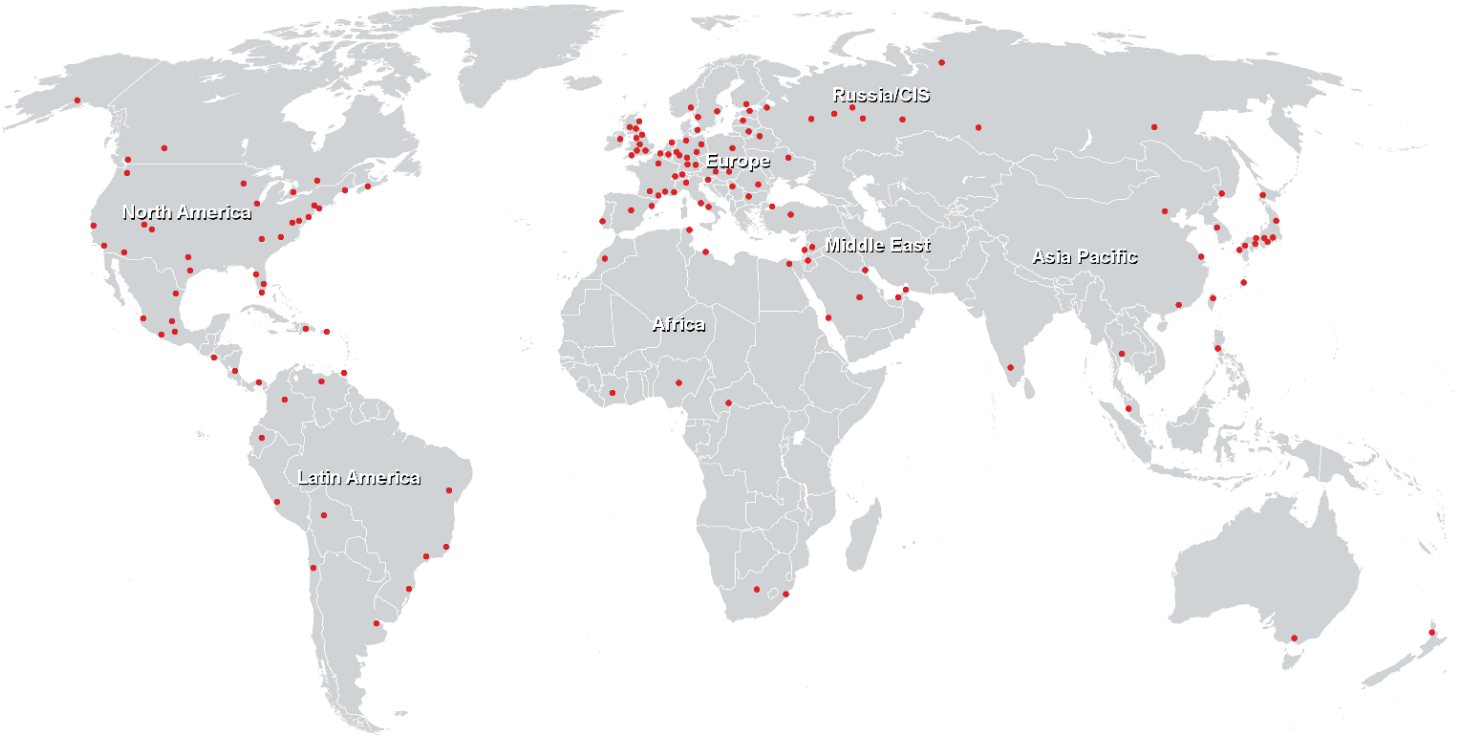
Course Content

- Mitigate threats using Microsoft Defender XDR
- Mitigate threats using Microsoft Copilot for Security
- Mitigate threats using Microsoft Purview
- Mitigate threats using Microsoft Defender for Endpoint
- Mitigate threats using Microsoft Defender for Cloud
- Create queries for Microsoft Sentinel using Kusto Query Language (KQL)
- Configure your Microsoft Sentinel environment
- Connect logs to Microsoft Sentinel
- Create detections and perform investigations using Microsoft Sentinel
- Perform threat hunting in Microsoft Sentinel

Microsoft Security Operations Analyst (SC-200T00)

Microsoft Solutions Partner
Microsoft Cloud Training Services

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch