CompTIA Cybersecurity Analyst (CYSA+)

ID CYSA+ **Price** on request **Duration** 5 days

Who should attend

This course is aimed at cyber security professionals with at least two to three years of on-the-job experience.

Prerequisites

Prior to attending the CompTIA Cybersecurity Analyst (CySA+), you are expected to have:

- The Network+ or Security+ certification - or equivalent knowledge
- A minimum of 4 years of hands-on information security or related experience

Course Objectives

On this accelerated CySA+ course you will focus on the following four cyber security domains:

- Threat Management
- Vulnerability Management
- Cyber Incident Response
- Security Architecture and Tool Sets

The training incorporates hands-on practical work in the form of virtual labs and software tools. This approach will accelerate your learning and will help retain your new found knowledge.

Course Content

Section 1: Threat Management

- Module 1: Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes
- Module 2: Given a scenario, analyse the results of a network reconnaissance
- Module 3: Given a network-based threat, implement or recommend the appropriate response and countermeasure
- Module 4: Explain the purpose of practices used to secure a corporate environment

Section 2: Vulnerability Management

- Module 1: Given a scenario, implement an information security vulnerability management process
- Module 2: Given a scenario, analyse the output resulting from a vulnerability scan
- Module 3: Compare and contrast common vulnerabilities found in the following targets

Section 3: Cyber Incident Response

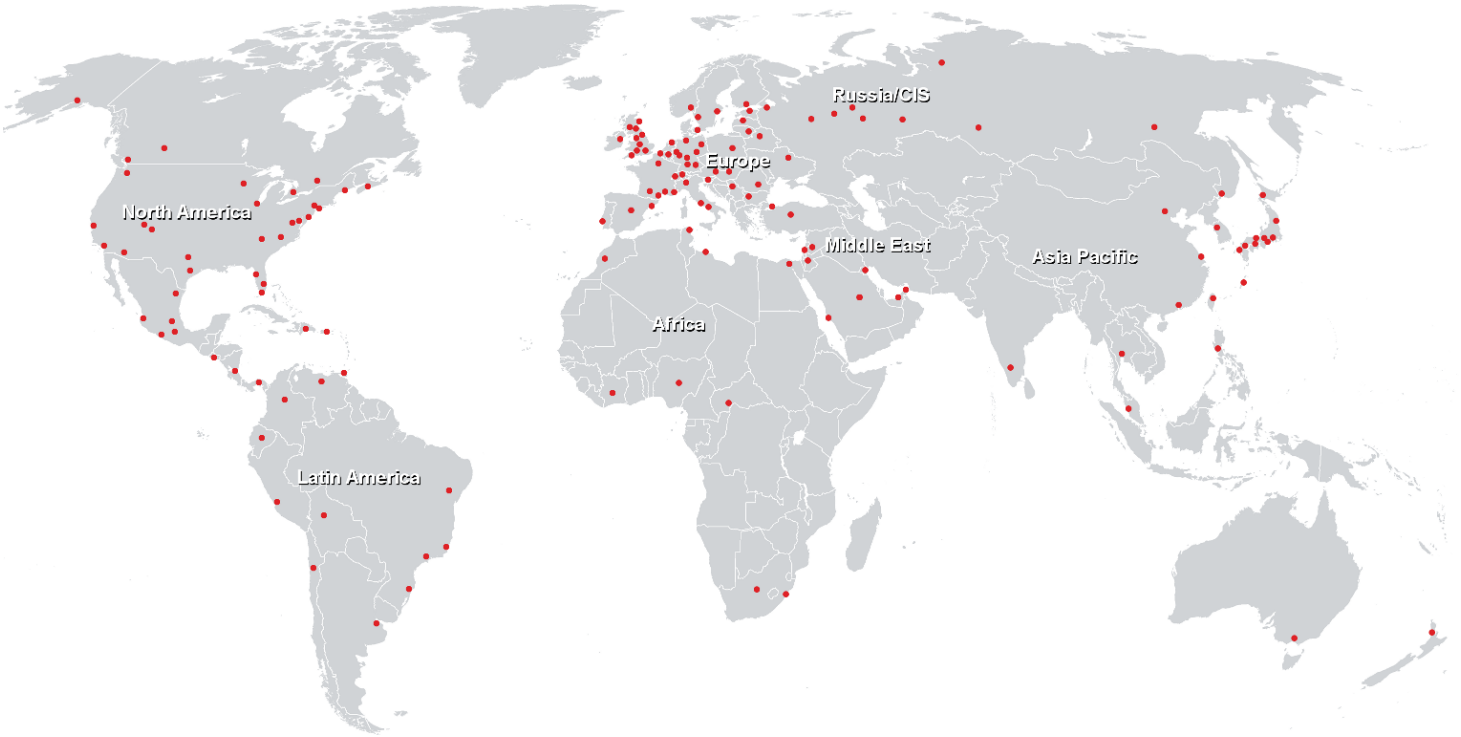
- Module 1: Given a scenario, distinguish threat data or behaviour to determine the impact of an incident
- Module 2: Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation
- Module 3: Explain the importance of communication during the incident response process
- Module 4: Given a scenario, analyse common symptoms to select the best course of action to support incident response
- Module 5: Summarise the incident recovery and post-incident response process

Section 4: Security Architecture and Tool Sets

- Module 1: Explain the relationship between frameworks, common policies, controls, and procedures
- Module 2: Given a scenario, use data to recommend remediation of security issues related to identity and access management
- Module 3: Given a scenario, review security architecture and make recommendations to implement compensating controls
- Module 4: Given a scenario, use application security best practices while participating in the Software Development Life Cycle (SDLC)
- Module 5: Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies

CompTIA Cybersecurity Analyst (CYSA+)

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