CompTIA Cybersecurity Analyst (CYSA+)

ID CYSA+ **Preis** auf Anfrage **Dauer** 5 Tage

Zielgruppe

Der Kurs eignet sich für Cybersecurity-Professionals mit mindestens zwei bis drei Jahren Praxiserfahrung.

Voraussetzungen

Für die CySA+ Schulung werden folgende Vorerfahrungen erwartet:

- Eine Network+ oder Security+ Zertifizierung oder äquivalente Kenntnisse
- Mindestens 2-3 Jahre Praxiserfahrungen in der Informationssicherheit oder verwandten Bereichen

Kursziele

In dieser CySA+-Schulung konzentrieren Sie sich auf folgende vier Cybersecurity-Bereiche:

- Threat Management
- Vulnerability Management
- Reaktion auf Cybersecurity Vorfälle
- Security Architektur und Tool Sets

Im Training sind praktische Aufgaben in Form von virtuellen Labs und Softwaretools enthalten, um den Lernvorgang zu beschleunigen und das erlangte Wissen zu festigen.

Kursinhalt

1. Threat Management

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

2. Vulnerability Management

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

3. Cyber Incident Response

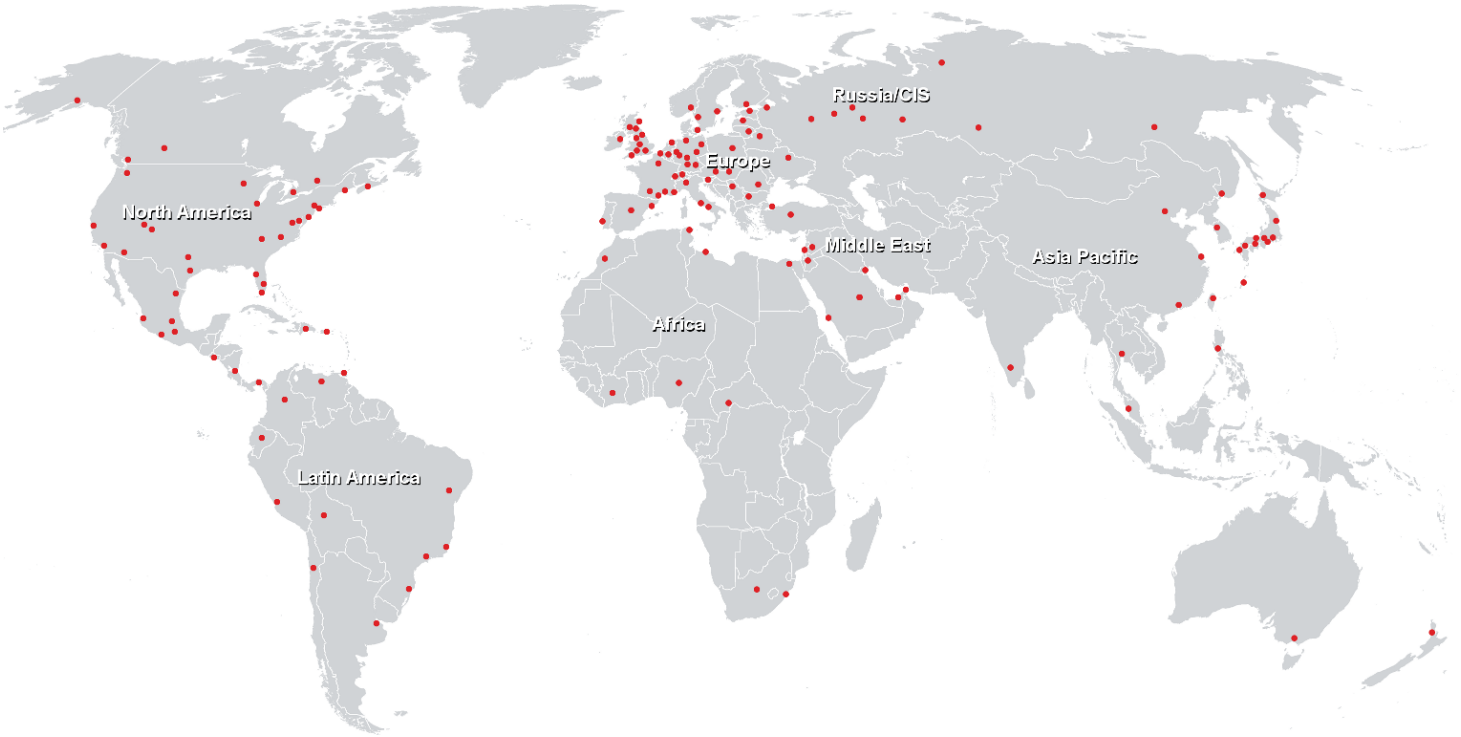
- Given a scenario, distinguish threat data or behaviour to determine the impact of an incident
- Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation.
- Explain the importance of communication during the incident response process.
- Given a scenario, analyse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

4. Security Architecture and Tool Sets

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

CompTIA Cybersecurity Analyst (CYSA+)

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer GmbH

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

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