Understanding Cisco Cybersecurity Operations Fundamentals (CCNACBR)

ID CCNACBR **Price** CHF 4,495.—(excl. VAT) **Duration** 5 days

Who should attend

- Associate-Level Cybersecurity Analysts

This course is part of the following Certifications

Cisco Certified Cybersecurity Associate (CCNA CYBERSECURITY)

Prerequisites

There are no formal prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- Familiarity with Ethernet and TCP/IP networking
- Working knowledge of the Windows and Linux operating systems
- Familiarity with basics of networking security concepts

These skills can be found in the following Cisco Learning Offering:

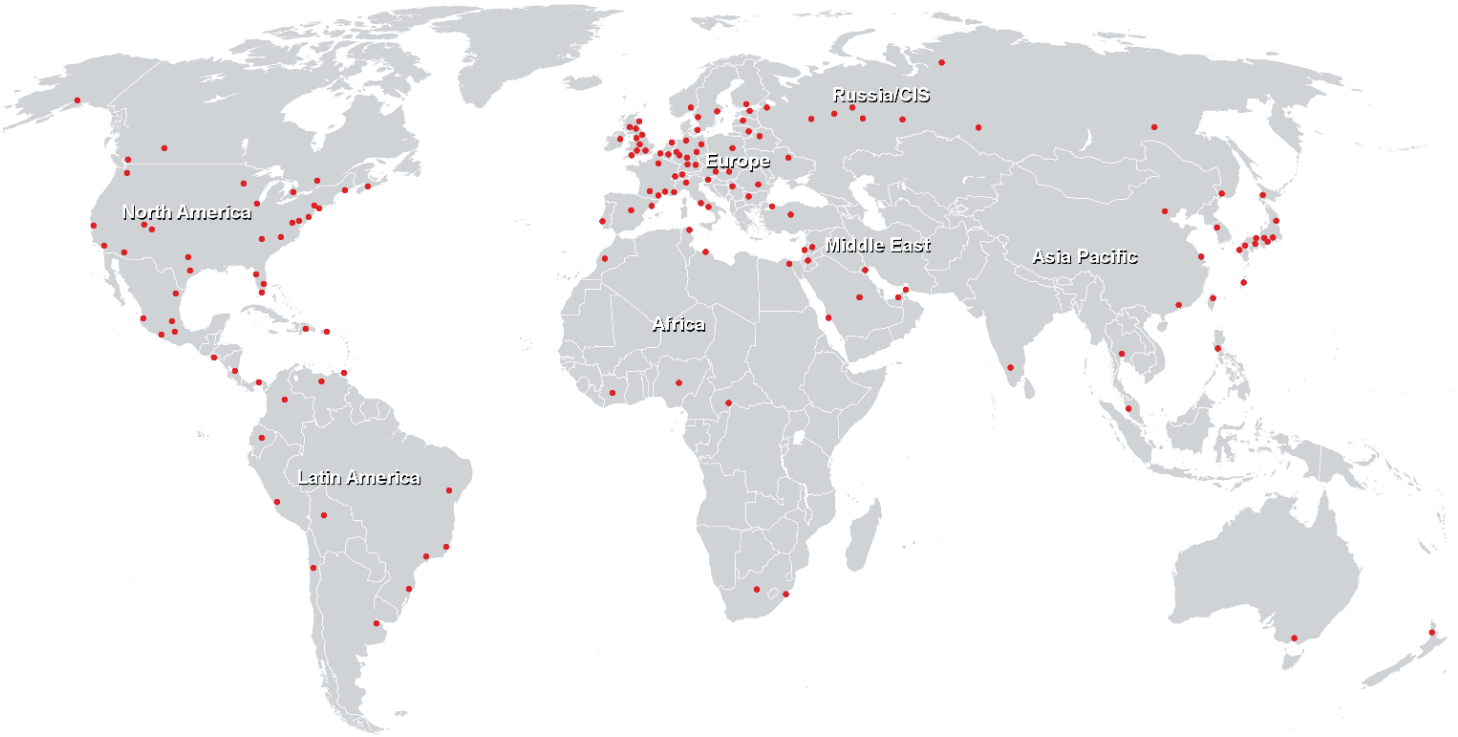
- Implementing and Administering Cisco Solutions (CCNA)

Course Objectives

- Explain the foundational aspects of SOCs, including their types, key roles, and essential metrics for measuring effectiveness
- Apply foundational security principles and risk management concepts to assess and protect organizational assets
- Compare and apply various access control models to secure network resources and enforce organizational policies
- Differentiate between various cloud deployment and service models and explain the shared responsibility for security in cloud environments
- Explain the fundamental concepts of cryptography, differentiate between various cryptographic algorithms, and explain how cryptographic principles are applied in real-world protocols and systems, including key exchange, digital signatures, and SSL/TLS
- Identify and describe the fundamental components and operational aspects of the Windows operating system for security analysis
- Identify and describe the fundamental components and operational aspects of the Linux operating system for security analysis
- Utilize Command Line Interfaces (CLIs) for basic system interaction, file management, and security-related tasks in both Windows and Linux environments
- Explain the operations and identify the security implications of foundational network protocols
- Describe and differentiate various network security controls and their application in protecting network infrastructure
- Differentiate between various Intrusion Detection and Prevention Systems (IDS/IPS) and interpret their output for security monitoring
- Describe and compare various endpoint security solutions and their effectiveness against common threats
- Identify and categorize various cyber threat actors based on their motivations, capabilities, and common tactics
- Explain the phases of the Classic Cyber Kill Chain model and identify adversary actions within each phase
- Apply the MITRE ATT&CK Framework to analyze and map cyber threats, explain its structure and application, and leverage it to enhance threat detection, incident response, and communication within a security operations environment
- Identify and describe various social engineering attack vectors, including those enhanced by generative AI
- Describe fundamental network attack techniques that exploit protocol vulnerabilities
- Describe advanced attack vectors and emerging threats in the current cybersecurity landscape
- Identify and explain various types of Network Security Monitoring (NSM) data and their role in incident investigation
- Identify and interpret various log data sources from operating systems, network devices, and security tools
- Explain NetFlow operations and its application as a security tool for network monitoring and anomaly detection
- Describe common web application attacks and their exploitation methods
- Apply advanced log analysis techniques to interpret security data and identify patterns of suspicious behavior
- Perform packet capture analysis and apply digital forensics

processes to investigate security incidents. Focus on the 5-tuple and timestamps to correlate with other logs, as this is your primary tool for network forensics
- Explain malware analysis outputs and apply threat intelligence frameworks for security investigations
- Explain the architecture, core functions, and best practices for implementing SIEM solutions for effective security monitoring
- Explain the features and common use cases of SOAR platforms for automating and streamlining incident response
- Explain the Cisco XDR platform, its core functions, features, and components for unified threat detection and response
- Differentiate between the legacy and modern NIST incident response guidance (NIST SP 800-61 Rev 2 and NIST SP 800-61 Rev 3 special publications), describe core IR components aligned with the NIST CSF 2.0 framework, and identify how these practices satisfy CMMC requirements for the Defense Industrial Base (DIB)
- Describe the roles, categories, and operational services of Computer Security Incident Response Teams (CSIRTs)
- Explain the concept of security monitoring playbooks and their components for standardizing incident response
- Apply various threat hunting methodologies to proactively identify and mitigate hidden threats within a network

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