Current Technologies
Computer Learning Centers

CompTIA

6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: http://www.ctclc.com

CompTIA Cybersecurity Analyst+ (CySA+)

This course provides the basic knowledge needed to analyze, monitor, and protect cybersecurity resources in a vendor-neutral format. It includes threat intelligence, vulnerability management, network reconnaissance and monitoring, secure policies and procedures, host and network security, identity management systems, and incident response.

How you'll benefit

This class will help you:

- Learn how to analyze, monitor, and protect critical infrastructures using threat-detection and threat-analysis tools.

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10%
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs Run up to Date Code for all our courses

Objectives

Upon completing this course, the student will be able to meet these objectives:

- Explain the Importance of Security Controls and Security Intelligence
- Utilize Threat Data and Intelligence
- Analyze Security Monitoring Data
- Collect and Query Security Monitoring Data
- Utilize Digital Forensics and Indicator Analysis Techniques
- Apply Incident Response Procedures
- Apply Risk Mitigation and Security Frameworks
- Perform Vulnerability Management
- Apply Security Solutions for Infrastructure Management
- Understand Data Privacy and Protection
- Apply Security Solutions for Software Assurance
- Apply Security Solutions for Cloud and Automation

Course Duration

5 day

Course Price

$2,895.00

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

Certification Exam

CS0-002

2022 Current Technologies CLC

6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: http://www.ctclc.com

CompTIA Cybersecurity Analyst+ (CySA+)

Who Should Attend

The job roles best suited to the material in this course are:

- This course is designed for IT professionals such as PC, desktop, and help desk technicians who have experience supporting PC hardware who wish to make the transition to become server hardware and support specialists.
- IT Security Analyst
- Security Operations Center (SOC) Analyst
- Vulnerability Analyst
- Cybersecurity Specialist
- Threat Intelligence Analyst
- Security Engineer

Perquisites

To fully benefit from this course, you should have the following knowledge:

- Knowledge equivalent to the CompTIA Security+ certification
- At least two years (recommended) of experience in computer network security technology or a related field.
- The ability to recognize information security vulnerabilities and threats in the context of risk management.
- Foundation-level operational skills with some of the common operating systems for computing environments.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in computing environments. Safeguards include, but are not limited to, basic authentication and authorization, resource permissions, and anti-malware mechanisms.
- Foundation-level understanding of some of the common concepts for network environments, such as routing and switching.
- Foundational knowledge of major TCP/IP networking protocols including, but not limited to, TCP, IP, UDP, DNS, HTTP, ARP, ICMP, and DHCP.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in network environments. Safeguards include, but are not limited to, firewalls, intrusion prevention systems, and VPNs.

2022 Current Technologies CLC

6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: http://www.ctclc.com

CompTIA Cybersecurity Analyst+ (CySA+)

Outline

Module 0: Introduction

- Course setup

Module 1: Understanding threats

- Threats and vulnerabilities
- Threat intelligence
- Automation technologies

Module 2: Policy design

- Security policies
- Controls and procedures

Module 3: Vulnerability management

- Risk management programs
- Vulnerability assessment
- Vulnerability management programs

Module 4: Recognizing vulnerabilities

- Attack strategies
- System vulnerabilities
- Application exploits

Module 5: Network threats

- Network vulnerabilities
- Cloud vulnerabilities

Module 6: Reconnaissance

- Reconnaissance techniques
- Active reconnaissance
- Analyzing scan results

2022 Current Technologies CLC

CompTIA Cybersecurity Analyst+ (CySA+)

Module 7: Network security systems

- Network security systems
- Logging and monitoring

Module 8: Network defense techniques

- Data analysis
- Threat hunting

Module 9: Secure infrastructure management

- Data protection
- Hardening networks
- Cryptographic security
- Identity systems

Module 10: Secure system design

- Hardware assurance
- Hardening hosts and devices
- Software assurance

Module 11: Incident Response

- Incident response planning
- Incident response procedures
- Forensic toolkits

2022 Current Technologies CLC