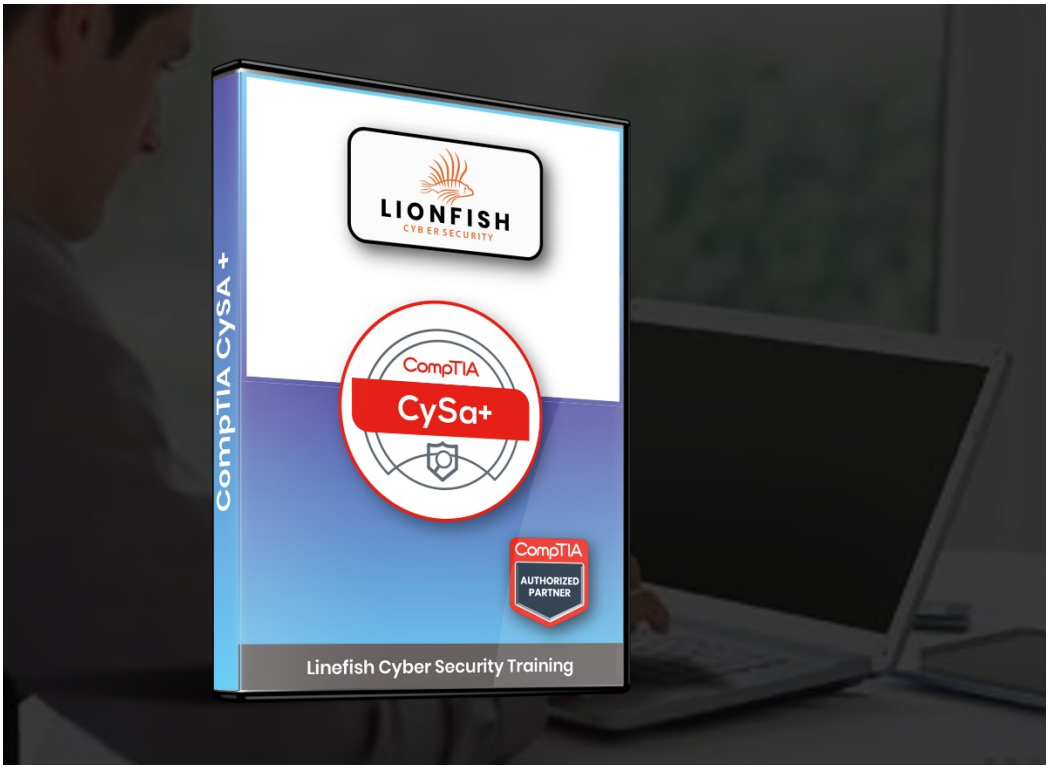
Lionfish Cyber Security Course Syllabus:

CompTIA CySA+ (CS0-001)

Interactive and entertaining talk-show style format presented by industry leading experts.

- 40+ hours of virtual training, practice exams, and study.
- Receive a Certificate of completion
- Presented by highly qualified, industry leading experts
- 12 Months Access *(Unless indicated otherwise)*



Description

www.LionfishCyberSecurity.com
877-732-6772 or info@lionfishcybersecurity.com
101 West Ohio Street, Suite 2000, Indianapolis, In 462041

CompTIA Cybersecurity Analyst (CySA+) is an IT workforce certification that applies behavioral analytics to networks and devices to prevent, detect and combat cybersecurity threats through continuous security monitoring.

Curriculum Overview

The CompTIA CySA (Cybersecurity Analyst) certification prep course is designed to help prepare candidates to sit for the CySA+ exam, as well as reinforce concepts for work roles such as Systems Security Analyst, Threat Analyst, and Vulnerability Assessment Analysts.

Objectives

- Apply environmental reconnaissance techniques like OS fingerprinting, e-mail harvesting, Netstat, and Syslog
- Analyze the results of network reconnaissance, and recommend or implement countermeasures
- Secure a corporate environment by scanning for vulnerabilities
- Respond to cyber incidents with a forensics toolkit, maintain the chain of custody, and analyze incident severity.

Prerequisites

- Know basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches, routers).
- Understand TCP/IP addressing, core protocols, and troubleshooting tools
- Identify network attack strategies and defenses.
- Know the technologies and uses of cryptographic standards and products
- Identify network- and host-based security technologies and practices.
- Describe the standards and products used to enforce security on web and communications technologies.

Target Audience

The CompTIA Cybersecurity Analyst (CySA+) examination is designed for IT security analysts, vulnerability analysts, or threat intelligence analysts. The exam will certify that the successful candidate has the knowledge and skills required to configure and use threat detection tools, perform data analysis, and interpret the results to identify vulnerabilities, threats, and risks to an organization with the end goal of securing and protecting applications and systems within an organization.

www.LionfishCyberSecurity.com
877-732-6772 or info@lionfishcybersecurity.com
101 West Ohio Street, Suite 2000, Indianapolis, In 462042

LIONFISH CYBER SECURITY™
Training Center

Syllabus

	CompTIA CySA+ Cybersecurity Analyst (CS0-001)
Episode	**Episode Name**
1	Promo
1	Introduction
Chapter 1 - Conducting Reconnaissance	
1	Thinking Like the Enemy
2	Tools of the Trade
Chapter 2 - Analyzing Reconnaissance Results	
1	Recon Results: Part 1
2	Recon Results: Part 2
3	Data Output
Chapter 3 - Responding to Network-Based Threats	
1	Protecting Your Territory
2	Hardening Strategies
Chapter 4 - Securing a Corporate Environment	
1	Pen Testing
2	Training
3	Reverse Engineering
4	Risk Evaluation
Chapter 5 - Vulnerability Management	
1	Requirements Identification
2	Scanning
3	Configuring and Executing Scans
4	Reporting and Remediating
Chapter 6 - Analyzing Vulnerabilities Scan Results	
1	Common Vulnerabilities: Part 1
2	Common Vulnerabilities: Part 2
Chapter 7 - Incident Response	
1	Incident Response Process
2	IR Roles and Responsibilities
Chapter 8 - Preparation Phase	
1	IR Active Preparation

www.LionfishCyberSecurity.com
877-732-6772 or info@lionfishcybersecurity.com
101 West Ohio Street, Suite 2000, Indianapolis, In 462043

2	Threat Trends

Chapter 9 - Forensic Tools

1	Digital Forensics
2	Seizure and Acquisitions
3	Forensics Acquisition Tools
4	Forensics Analysis: Part 1
5	Forensics Analysis: Part 2

Chapter 10 - Common Symptoms of Compromise

1	Network Symptoms
2	Host Symptoms
3	Application Symptoms

Chapter 11 - Incident Recovery and Post-Incident Response Process

1	Moving Forward: Part 1
2	Moving Forward: Part 2

Chapter 12 - Frameworks, Common Policies, Controls, and Procedures

1	Frameworks
2	Policies
3	Controls & Procedures
4	Verifications

Chapter 13 - Identity and Access Management

1	Context-Based Authentication
2	Identities
3	Managing Identities
4	Exploits

Chapter 14 - Defense Strategies

1	Data Analytics
2	Defense in Depth

Chapter 15 - Software Development Life Cycle (SDLC)

1	Secure Software Development Best Coding Practices

Chapter 16 - Tools and Technologies

www.LionfishCyberSecurity.com
877-732-6772 or info@lionfishcybersecurity.com
101 West Ohio Street, Suite 2000, Indianapolis, In 462044

1	Preventative Tools: Part 1
2	Preventative Tools: Part 2
3	Collective Tools
4	Vulnerability Scanning
5	Packet Capture
6	Connectivity Tools
7	Pen Testing Tools

Prepare for the CompTIA Network+ exam with the excellent practice tests. Enabling you to practice on test questions and assess your skill and knowledge of the material. Get certified the best way

- Applies to the current N10-007 exam
- Includes many practices questions
- Requires Windows, macOS, Chrome OS, or Linux (iOS and Android not supported)
- Single-user license

Learn includes:

- **Interactive learning with flashcards and performance-based questions.**
- **Videos that demonstrate key concepts and processes.**
- **Customizable learning plan.**
- **Easy self-assessments.**
- **Learning progress analytics and reporting.**

www.LionfishCyberSecurity.com
877-732-6772 or info@lionfishcybersecurity.com
101 West Ohio Street, Suite 2000, Indianapolis, In 462045

LIONFISH CYBER SECURITY™

Training Center

Sample Certificate upon completions of each course

To learn more, contact us at 877-732-6772 or info@lionfishcybersecurity.com

www.LionfishCyberSecurity.com

LIONFISH CYBER SECURITY™

101 West Ohio Street, Suite 2000, Indianapolis, In 46204

This institution is regulated by the Office for Career and Technical Schools - 10 N Senate Avenue, Suite SE 308, Indianapolis 46204 - OCTS@dwd.in.gov
http://www.in.gov/dwd/2731.htm

CMMC-AB Registered Provider Organization™