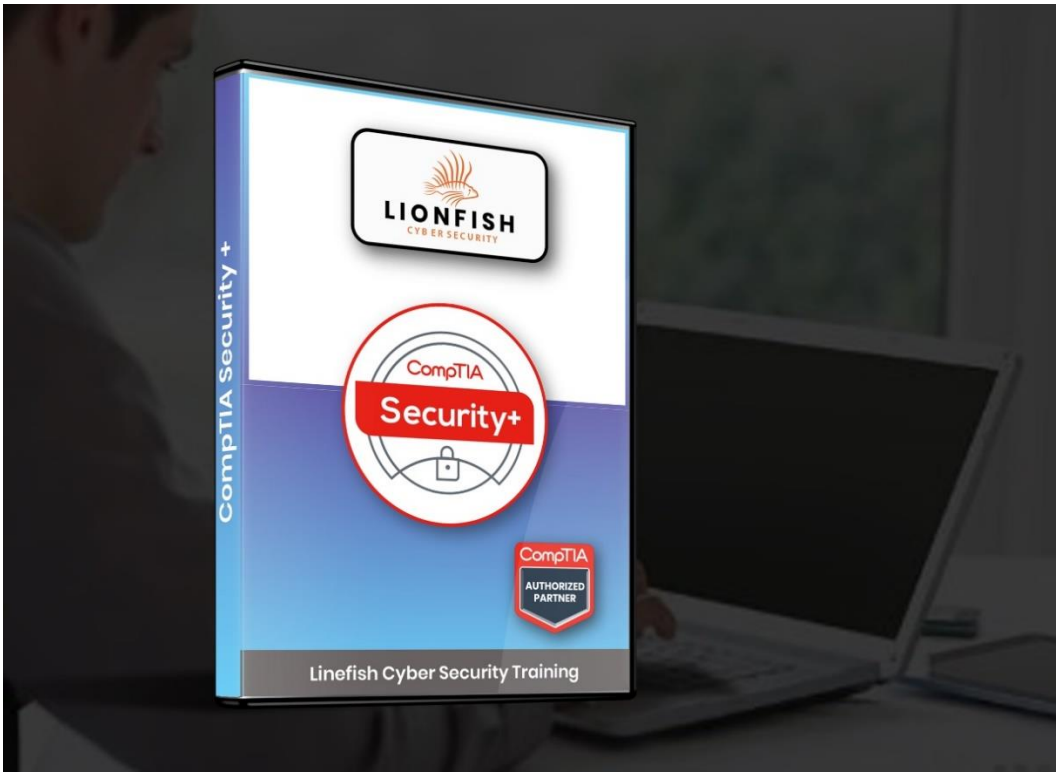
Lionfish Cyber Security Course Syllabus:

CompTIA Security+

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)*
- * The CompTIA bundle comes with practice exams.



LIONFISH CYBER SECURITY™

DESCRIPTION

CompTIA Security+ focuses in on the latest trends in risk management, risk mitigation, threat management, and intrusion detection. This certification will allow you to demonstrate your cybersecurity skills and abilities to employers.

CURRICULUM

Overview

CompTIA Security+ is the certification globally trusted to validate foundational, vendor-neutral IT security knowledge and skills. As a benchmark for best practices in IT security, this certification covers the essential principles for network security and risk management – making it an important steppingstone of an IT security career.

CompTIA Security+ is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on troubleshooting to ensure security professionals have practical security problem-solving skills. Cybersecurity professionals with Security+ know how to address security incidents – not just identify them. Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.

Objectives

- Provide operational, information, application and infrastructure level security
- Secure the network to maintain availability, integrity, and confidentiality of critical information
- Operate within a set of rules, policies, and regulations wherever applicable
- Comprehend Risk identification and mitigation

Prerequisites

IT security professionals with a minimum of two years' experience in IT administration with a focus on security; users with basic day-to-day technical information security experience; those interested in gaining a broader and deeper knowledge of security concerns and implementation; and learners preparing for the Security+ exam

Target Audience

- The series is intended for aspiring IT security professionals entering into security.
- The professionals who are Systems Administrator Network Administrator Security Administrator Junior IT Auditor/Penetration Tester

CURRICULUM Syllabus

CompTIA Security+	
#	**Episode Name**
1	Promo
2	Introduction to Security+ SY0-501
	Chapter 1 - Risk Management
1	The CIA of Security
2	What is Risk?
3	Threat Actors
4	Managing Risk
5	Using Guides for Risk Assessment
6	Security Controls
7	Interesting Security Controls
8	Defense in Depth
9	IT Security Governance
10	Security Policies
11	Frameworks
12	Quantitative Risk Calculations
13	Business Impact Analysis
14	Organizing Data
15	Security Training
16	Third-Party Agreements
	Chapter 2 - Cryptography
1	Cryptography Basics
2	Cryptographic Methods
3	Symmetric Cryptosystems
4	Symmetric Block Modes
5	RSA Cryptosystems
6	Diffie-Hellman
7	PGP/GPG
8	Hashing
9	HMAC
10	Stenography
11	Certificates and Trust
12	Public Key Infastucture
13	Cryptographic Attacks
	Chapter 3 - Identity and Access Management

1	Identification
2	Authorization Concepts
3	Access Control List
4	Password Security
5	Linux File Permissions
6	Windows File Permissions
7	User Account Management
8	AAA
9	Authentication Methods
10	Single Sign-On

Chapter 4 - Tools of the Trade

1	OS Utilties, Part 1
2	OS Utilties, Part 2
3	Network Scanners
4	Protocol Analyzers
5	SNMP
6	Logs

Chapter 5 - Securing Individual Systems

1	Denial of Service
2	Host Threats
3	Man-in-the-Middle
4	System Resiliency
5	RAID
6	NAS and SAN
7	Physical Hardening
8	RFI, EMI, and ESD
9	Host Hardening
10	Data and System Security
11	Disk Encryption
12	Hardware/Firmware Security
13	Secure OS Types
14	Securing Peripherals
15	Malware
16	Analyzing Output
17	IDS and IPS
18	Automation Strategies
19	Data Destruction

Chapter 6 - The Basic LAN

1	LAN Review
2	Network Topologies Review

3 Network Zone Review
4 Network Access Controls
5 The Network Firewall
6 Proxy Servers
7 Honeypots
8 Virtual Private Networks
9 IPSec
10 NIDS/NIPS
11 SIEM (Security Information and Event Management)

Chapter 7 - Beyond the Basic LAN

1 Wireless Review
2 Living in Open Networks
3 Vulnerabilities with Wireless Access Points
4 Cracking 802.11, WEP
5 Cracking 802.11, WPA and WPA2
6 Cracking 802.11, WPS
7 Wireless Hardening
8 Wireless Access Points
9 Virtualization Basics
10 Virtual Security
11 Containers
12 Infrastucture as a Service (IaaS)
13 Platform as a Service (PaaS)
14 Software as a Service (SaaS)
15 Deployment Models
16 Static Hosts
17 Mobile Connectivity
18 Deploying Mobile Devices
19 Mobile Enforcement
20 Mobile Device Management
21 Physical Controls
22 HVAC
Fire Suppression

Chapter 8 - Secure Protocols

1 Secure Encryption Applications and Protocols
2 Network Models
3 Know Your Protocols - TCP/IP
4 Know Your Protocols - Applications

5	Transport Layer Security (TLS)
6	Internet Service Hardening
7	Protecting Your Servers
8	Secure Code Development
9	Secure Deployment Concepts
10	Code Quality and Testing

	Chapter 9 - Testing Your Infrastructure
1	Vulnerability Scanning Tools
2	Vulnerability Scanning Assessment
3	Social Engineering Principles
4	Social Engineering Attacks
5	Attacking Applications
6	Attacking Web Sites
7	Exploiting a Target
8	Vulnerability Impact

	Chapter 10 - Dealing with Incidents
1	Incident Response
2	Digital Forensics
3	Contingency Planning
4	Backups

Overview

Prepare for the CompTIA Security+ exam with the excellent TotalTester Online practice tests. The 1000+ questions mirror the questions you'll see on the real exam; enabling you to practice on test questions and assess your skill and knowledge of the material. Get certified the best way, the TotalTester way!

- Applies to the current SY0-501 exam
- Includes over 1000 questions
- Requires Windows, macOS, Chrome OS, or Linux (iOS and Android not supported)
- Single-user license
-

Question Pool Sources

- Multiple (4+) McGraw-Hill publications

TotalTester Features

Testing Modes

- Practice Mode: tests with hints and answer explanations
- Exam Mode: just like the real thing, no help, just you and the questions
- Results graded by topic for easy review

Customized Tests

- Filter questions by exam objectives
- Choose whether or not to include hints and answer explanations
- Choose the number of questions on your practice test
- Set your own time limit

Test History

- See the date you took each test
- View final score for each test
- See number of questions answered correctly by objective
- Review each question, see your answer, the correct answer, and explanations

LIONFISH
CYBER SECURITY™

Sample Certificate upon completions of each course.

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

Lionfish Cyber Security has partnered with Instructor Mike Myers & Total Seminars to bring you best in class training, Labs and Practice exams.