Course 843 – CompTIA Cybersecurity Analyst+ (CySA+)

Duration: 5 days

What You Get:

- CompTIA CySA+ (CS0-002) Exam Voucher
- 5 days of high quality classroom or live online training
- Access to ActiveLearning's Virtual Labs
- CompTIA CySA+ Accredited Instructor
- More than 120 end of chapter drill questions with answer keys
- Mock exam with answer key
- Online access to CompTIA CySA+ learning resources
- Official CompTIA CySA+ Digital Courseware
- Certificate of Attendance
- Exam Prep Guarantee
- Lunch, morning and afternoon refreshments
- Unlimited course refresher for 1 year (Note: exams are not included)

You Will Learn How To

- Assess and respond to security threats and operate a systems and network security platform.
- Collect and use cybersecurity intelligence and threat data.
- Identify modern cybersecurity threat actors types and tactics, techniques, and procedures.
- Analyze data collected from security and event logs and network packet captures.
- Respond to and investigate cybersecurity incidents using forensic analysis techniques.
- Assess information security risk in computing and network environments.
- Implement a vulnerability management program.
- Address security issues with an organization's network architecture.
- Understand the importance of data governance controls.
- Address security issues with an organization's software development life cycle.
- Address security issues with an organization's use of cloud and service-oriented architecture

Course Benefits

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.

CompTIA CySA+ is the only cybersecurity analyst certification with both hands-on, performance-based questions and multiple-choice questions.

In this training, you will be able to proactively capture, monitor, and respond to network traffic findings. You also learn about application security, automation, threat hunting, and IT regulatory compliance, which affects the daily work of security analysts.

Who Should Attend

This course is designed for those who are seeking the CompTIA CySA+ CS0-002 certification ~~exam~~ and who are aiming for job roles such as:

- Security Operations Center Analyst
- Vulnerability Analyst
- Cybersecurity Specialist
- Intelligence Analyst
- Security Engineer
- Cybersecurity analyst

Prerequisites

- At least 2 years experience in network security
- Familiarity with TCP/IP protocols such as IP, ARP, ICMP, DNS, DHCP, HTTP, etc.
- Familiarity with common safeguards in network environments, such as firewalls, IPS, NAC, and VPNs.

About the Exam

- Maximum of 85 questions
- Multiple choice and performance-based
- 165 minutes
- Passing Score: 750 (scale of 100 - 900)
- Testing Provider: Pearson Vue Testing Centers or Online Testing

Course Content

Explaining the Importance of Security Controls and Security Intelligence

- Identify Security Control Types
- Explain the Importance of Threat Data and Intelligence

Utilizing Threat Data and Intelligence

- Classify Threats and Threat Actor Type
- Utilize Attack Frameworks and Indicator Management
- Utilize Threat Modeling and Hunting Methodologies

Analyzing Security Monitoring Data

- Analyze Network Monitoring Output
- Analyze Appliance Monitoring Output
- Analyze Endpoint Monitoring Output
- Analyze Email Monitoring Output

Collecting and Querying Security Monitoring Data

- Configure Log Review and SIEM Tools
- Analyze and Query Logs and SIEM Data

Utilizing Digital Forensics and Indicator Analysis Techniques

- Identify Digital Forensics Techniques
- Analyze Network-related IoCs
- Analyze Host-related IoCs
- Analyze Application-Related IoCs

- Analyze Lateral Movement and Pivot IoCs

Applying Incident Response Procedures

- Explain Incident Response Processes
- Apply Detection and Containment Processes
- Apply Eradication, Recovery, and Post-Incident Processes

Applying Risk Mitigation and Security Frameworks

- Apply Risk Identification, Calculation, and Prioritization Processes
- Explain Frameworks, Policies, and Procedures

Performing Vulnerability Management

- Analyze Output from Enumeration Tools
- Configure Infrastructure Vulnerability Scanning Parameters
- Analyze Output from Infrastructure Vulnerability Scanners
- Mitigate Vulnerability Issues

Applying Security Solutions for Infrastructure Management

- Apply Identity and Access Management Security Solutions
- Apply Network Architecture and Segmentation Security Solutions
- Explain Hardware Assurance Best Practices
- Explain Vulnerabilities Associated with Specialized Technology

Understanding Data Privacy and Protection

- Identify Non-Technical Data and Privacy Controls
- Identify Technical Data and Privacy Controls

Applying Security Solutions for Software Assurance

- Mitigate Software Vulnerabilities and Attacks
- Mitigate Web Application Vulnerabilities and Attacks
- Analyze Output from Application Assessments

Applying Security Solutions for Cloud and Automation

- Identify Cloud Service and Deployment Model Vulnerabilities
- Explain Service-Oriented Architecture
- Analyze Output from Cloud Infrastructure Assessment Tools
- Compare Automation Concepts and Technologies

About ActiveLearning, Inc.

ActiveLearning is the Philippines' leading provider of Information Technology and Project Management education, where thousands of students take courses from Application Development to Project Management to Network Security, and much more. Our courses are taught by expert instructors, and learning is enhanced through a blend of in-depth

lectures, workshops, and hands-on exercises.