CompTIA Cybersecurity Analyst (CYSA+)

LANTEC
CORPORATE TRAINING

Duration: 5 days

Prerequisites: This course assumes that you have some applied knowledge of computers, TCP/IP networks, and cybersecurity principles. Knowledge equivalent to the CompTIA Security+ certification is helpful but not necessary.

Audience: Students will benefit most from this course if they intend to take a CompTIA CySA+ exam.

Description: The **CompTIA Cybersecurity Analyst (CySA+)** course provides the knowledge to analyze, monitor, and protect computer and network systems using a vendor-neutral format. It includes threat intelligence, active security, vulnerability management, network reconnaissance and monitoring, secure operations, and incident response. This course maps to the CompTIA CySA+ certification exam.

OUTLINE:

CHAPTER 1: UNDERSTANDING THREATS

Module A: Threats and vulnerabilities
Module B: Attack strategies

CHAPTER 2: PROACTIVE SECURITY

Module A: Threat intelligence
Module B: Attack methodology
Module C: Active defenses

CHAPTER 3: OPERATIONAL SECURITY

Module A: Controls and procedures
Module B: Automation and process improvement

CHAPTER 4: VULNERABILITY MANAGEMENT

Module A: Vulnerability testing
Module B: Vulnerability management programs
Module C: Vulnerability remediation

CHAPTER 5: SECURITY TESTING PROCEDURES

Module A: Vulnerability assessment tools
Module B: Analyzing scan results

CHAPTER 6: SECURE INFRASTRUCTURE

Module A: Infrastructure comparisons
Module B: Secure network infrastructure
Module C: Identity systems

CHAPTER 7: SECURE HOSTS AND DATA

Module A: Secure operating systems
Module B: Data protection

CHAPTER 8: SECURE SOFTWARE

Module A: Application exploits
Module B: Secure development
Module C: Software testing

CHAPTER 9: THREAT ANALYSIS

Module A: Threat detection techniques
Module B: Detection and analysis tools

CHAPTER 10: INCIDENT RESPONSE

Module A: Incident response planning
Module B: Incident response procedures
Module C: Digital forensics