AZ-301T02-A: Designing a Data Platform Solution

Duration- 1 days

Course Overview

This course establish the basic knowledge need for any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Securi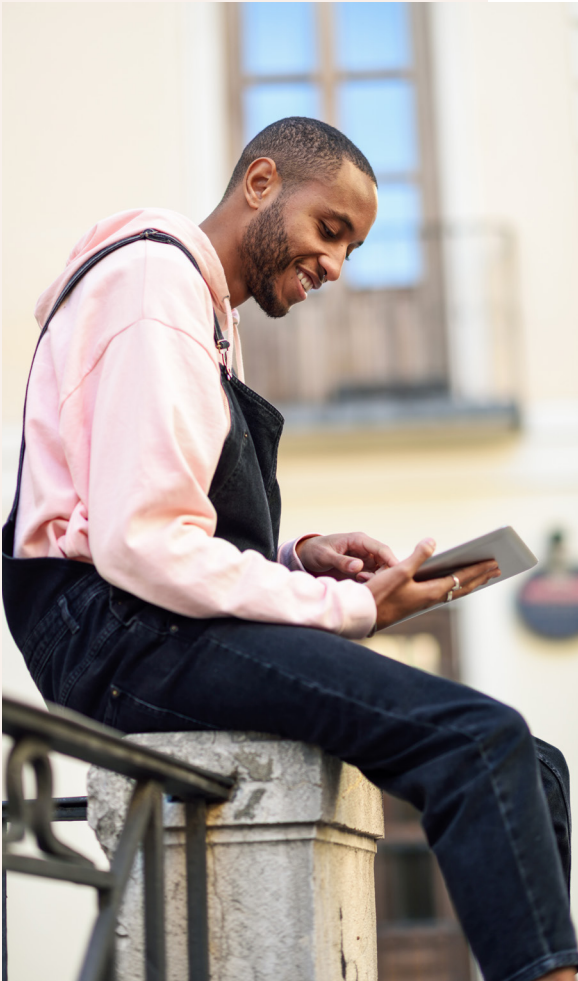ty+ incorporates best practices in hands-on trouble-shooting to ensure security professionals have practical security problem-solving skills.

What you will learn.

This course will teach you how to:

- Examine network security.
- Identify compliance and operational security measures.
- Manage risk
- Identify security threats and vulnerabilities.
- Manage security incidents.
- Manage application, data and host security.
- Develop business continuity and disaster recov-

LASU CBT 18

administrator, systems administrator and network administrator.

Prerequisites

Students should have taken CompTIA Network+ certification course and exam, together with 24 months experience in networking support/IT administration.

Module 1: Security Fundamentals

- Information Security Cycle
- Information Security Controls
- Authentication Methods
- Cryptography Fundamentals
- Security Policy Fundamentals

Module 2: Security Threats and Vulnerabilities

- Social Engineering
- Physical Threats and Vulnerabilities

ery plans.
- Identify access control and account management security measures.

Who is this course for?

The course is for an individual who want to have the knowledge on security architect, security engineer, security consultant/specialist, information assurance technician, security

- Network-Based Threats
- Wireless Threats and Vulnerabilities
- Software Based Threats

Module 3: Network Security

- Network Devices and Technologies
- Network Design Elements and Components
- Implement Networking Protocols
- Apply Network Security Administration
- Principles
- Secure Wireless Traffic

Module 4: Managing Application, Data and Host

- Security
- Establish Device/Host Security
- Application Security
- Data Security
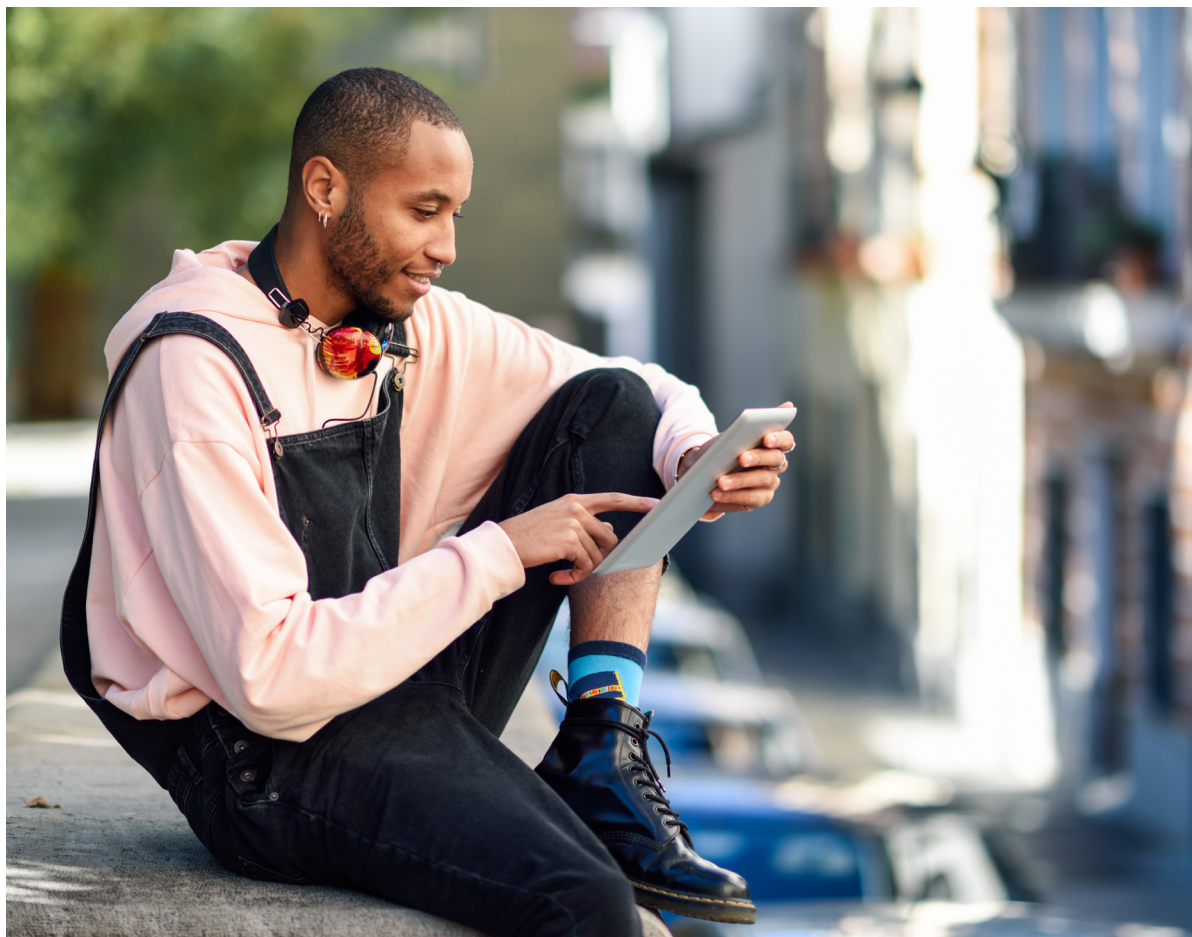
- Mobile Security

Module 5: Access Control, Authentication, and
- Account Management
- Access Control and Authentication Services
- Implement Account Management Security
- Controls

Module 6: Managing Certificates
- Install a Certificate Authority (CA)
- Hierarchy
- Enroll Certificates
- Secure Network Traffic by Using
- Certificates
- Renew Certificates
- Revoke Certificates
- Back Up and Restore Certificates and Private Keys
- Restore Certificates and Private Keys

Module 7: Compliance and Operational Security
- Physical Security
- Legal Compliance
- Security Awareness and Training

Module 8: Risk Management
- Risk Analysis
- Implement Vulnerability Assessment Toolsand Techniques
- Scan for Vulnerabilities
- Mitigation and Deterrent Techniques

Module 9: Managing Security Incidents
- Respond to Security Incidents
- Recover from a Security Incident

Module 10: Business Continuity and Disaster
- Recovery Planning
- Business Continuity
- Plan for Disaster Recovery
- Execute Disaster Recovery Plans and
- Procedures

Pages 4