Education & Training Plan

Student Name: ________________________________

Start & End Dates: ___/___/_____ to ___/___/_____

IT Cybersecurity Specialist Certificate Program

MyCAA Program Information
Tuition: $3,950
Course Code: AU-ITSS
Program Type: Certificate
Program Duration: 9 Months
Contact Hours: 540

This training program combines a 3 course training track:

- CompTIA Network+
- CompTIA Security+
- Cybersecurity

Computer security specialists configure access to computer systems as well as planning and coordinating information security protocols. The role of a computer security specialist usually includes some network monitoring tasks and the installation of security software on a company's computer terminals. Performing risk assessments, developing effective system-wide security plans and staying informed about the latest trends in computer virus and malware deployment are also principal components of the position.

The Job Outlook
Employment of information security analysts, web developers, and computer network architects is projected to grow 22 percent from 2010 to 2020, faster than the average for all occupations. Demand for information security analysts is expected to be very high. Cyber-attacks have grown in frequency and sophistication over the last few years, and many organizations are behind in their ability to detect these attacks. Analysts will be needed to come up with innovative ways to prevent hackers from stealing critical information or creating havoc on computer networks.

Prerequisites
Students taking this program should have either CompTIA A+ certification and nine months networking experience

**CompTIA Network + - 180 Hours**

**Overview**

The CompTIA Network+ certification is the sign of a qualified networking professional. Our course is designed to teach the CompTIA Network+ skills necessary to prepare for the N10-005 certification exam. CompTIA Network+ certification is vendor-neutral, validates technical competency in network technologies, installation and configuration, media and topologies, management, and security. CompTIA Network + is designed to ensure a common level of understanding for IT Professionals.

This course includes access to a hands-on Practice-Lab which will allow candidates to have training in the practical application of the course concepts without having to buy any additional software and will prepare them for success on the certification exam.

**Prerequisite(s):** We recommend candidates possess CompTIA A+ certification and networking experience. Students should have basic keyboarding and computer skills, and be comfortable navigating the internet.

By the end of this course, you will be able to:

- Comprehend the principles of networking including IP Addressing, Subnetting, Troubleshooting, Topology Selection, Backbones, and Segments
- Identify the steps for installing and configuring different network types
- Comprehend the principles of Ethernet and Networking Devices
- Identify methods for documenting, monitoring, and optimizing networks
- Identify Software, Hardware and Troubleshooting Tools

**Outline**

**CompTIA Network+ Module 1**

**Networking Concepts**

- Introduction to Networks
- Physical Network Topologies
- Topology Selection, Backbones, and Segments
- Open Systems Interconnection Specifications
- Internetworking Models
- OSI Reference Model
- Networking Topologies
- Connectors and Wiring Standards
- Physical Media
- Cable Properties
- Wiring Standards
- Installing Wiring Distributions

**CompTIA Network+ Module 2**

**Ethernet and Networking Devices**

- Current Ethernet Specifications
• Network Basics
• Ethernet and Data Link Layer
• Ethernet at the Physical Layer
• Common Network Connectivity Devices
• Specialized Devices
• Planning and Implementing a SOHO Network
• Network Segregation
• Internet Protocol
• TCP/IP
• Data Encapsulation

CompTIA Network+ Module 3
IP Addressing, Subnetting, and Troubleshooting

• IP Terminology
• Hierarchical IP Addressing Scheme
• IPv4 Address Types
• Internet Protocol Version 6 (IPv6)
• IP Subnetting Basics
• Troubleshooting IP Addressing
• Network Address Translation (NAT)
• IP Routing Basics
• IP Routing Processes
• Static and Dynamic Routing

CompTIA Network+ Module 4
Routing, Switching, and Wireless Protocols

• Routing Protocol Basics
• Distance Vector
• Link State Routing
• Switching and Virtual LANs
• Networking Before Layer 2 Switching
• Switching Services
• Spanning Tree Protocol
• VLAN Basics
• VLAN Trunking
• Wireless Technology
• Wireless Components
• Wireless Security

CompTIA Network+ Module 5
Authentication, Threats, and Network Security

• Authentication and Access Control
• Security Filtering
• Managing User Accounts and Password Security
• User-Authentication Methods
• Network Threats and Mitigation
• Recognizing Security Threats
• Understanding Mitigation Techniques
• Active Detection
• Physical and Hardware Security
• Defining Firewalls
• Firewall Technologies
• Scanning Services
• Intrusion Detection

CompTIA Network+ Module 6
Wide Area Networks and Troubleshooting

• WAN Terms
• T-Series Connections
• Transmission Media
• Broadband Services
• Wireless WAN Technologies
• WAN Protocols
• Troubleshooting Tools
• Protocol Analysis
• Using ipconfig and ifconfig
• Ping Utility
• Nslookup Utility
• Resolving Names with Hosts Table
• Using Mtr Command
• Using route Command
• File Transfer Protocol

CompTIA Network+ Module 7
Software, Hardware and Troubleshooting Tools

• Software and Hardware Tools
• Network Scanners
• Packet Sniffers
• Network Troubleshooting
• Narrowing Down the Problem
• Troubleshooting Steps
• Management, Monitoring, and Optimization
• Managing Network Documentation
• Monitoring the Network and Optimizing Its Performance
• Virtual Networking
• Exam Essentials and Review

Certifications:

Upon successful completion of this course, students will be prepared to sit for the CompTIA Exam N10-005: CompTIA Network+ certification exam.
Overview

CompTIA Security+ certification designates knowledgeable professionals in the field of security, one of the fastest-growing fields in IT. CompTIA Security+ is an international, vendor-neutral certification that demonstrates competency in Network Security, Compliance and Operational Security, Threats and Vulnerabilities, Application, Data and Host Security, Access Control and Identity Management Cryptography.

This course prepares for the Security+ certification exam SY0-401. Many corporations recommend or require the Security+ certification for their IT employees. Companies like Sun, IBM/Tivoli Software Group, Symantec, Motorola and Olympus Security Group know the value of a Security+ certification and recommend or require it of their IT employees.

This course includes access to a hands-on Practice-Lab which will allow candidates to have training in the practical application of the course concepts without having to buy any additional software and will prepare them for success on the certification exam.

Prerequisite(s): We recommend candidates possess CompTIA Network+ certification and two years of technical networking experience, with an emphasis on security.

After completing this course, you should be able to:

- Comprehend the principles of network security
- Identify the steps for compliance and operational security
- Identify Devices and Infrastructures
- Identify the steps for controlling access authentication, and authorization
- Identify the steps for protecting Wireless Networks

Outline

CompTIA Security+ Module 1
Risk, Monitoring, and Diagnosing Networks

- Risk related concepts
- Control Types
- False Positives and Negatives
- Risk Management
- Implementing Policies
- Understanding Control Types
- Alarms
- Alerts
- Trends
- Security Posture

CompTIA Security+ Module 2
Devices, Infrastructure, and Access Control

- Mastering TCP/IP
- OSI Resilience
- Working with TCP/IP Suite
• IPv4 and IPv5
• Encapsulation
• Protocols and Services
• Securing Workstations
• Access Control Basics
• Identity Management
• Network Access Control

CompTIA Security+ Module 3
Protecting the Wireless Networks and Securing the Cloud

• Wireless Systems
• Lightweight Extensible Authentication Protocol
• Wireless Attacks
• Access Points
• Classifying Information
• Private Cloud
• Security and the Cloud
• Host availability
• Sandboxing
• Cloud Storage

CompTIA Security+ Module 4
Host, Data, Cryptography and Application Security

• Application Hardening
• Fuzzing
• Secure Coding
• Host Security
• Database Technologies
• Cryptography Overview
• Modern Cryptography
• Rainbow Tables and Salt
• Key Stretching
• Wi-Fi Encryption

CompTIA Security+ Module 5
Malware, Vulnerabilities, Social Engineering and Threats

• Understanding Malware
• Surviving Viruses
• Types of Viruses
• Spoofing Attacks
• Understanding Social Engineering
• Types of Social Engineering Attacks
• What Motivates an Attack?
• The Principles Behind Social Engineering
• Social Engineering Attack Examples
• Understanding Physical Security

CompTIA Security+ Module 6
Security Administration and Disaster Recovery
• Understanding Physical Security
• Third-Party Integration
• Transitioning
• Understanding Business Continuity
• Impact Analysis
• The Health Insurance Portability and Accountability Act
• The Gramm-Leach-Bliley Act
• The Computer Fraud and Abuse Act
• Penetration Testing
• Vulnerability Scanning

Materials:
• *CompTIA Security+ Study Guide: SY0-401* by Emmett Dulaney and Chuck Easttom

Certifications:

Upon successful completion of this course, students will be prepared to sit for the CompTIA Exam SYO-401: CompTIA Security+ certification exam.

System Requirements:

Internet Access
• Broadband or high-speed internet access is required. Broadband includes DSL, cable, and wireless connections.
• Dial-Up internet connections will result in a diminished online experience. Moodle pages may load slowly and viewing large audio and video files may not be possible.

Hardware
• Windows hardware configurations and processors are acceptable
• Mac computers **MUST** have Microsoft Window Operating Systems over Bootcamp (Bootcamp is a free download from Apple's website)
• 1 GB RAM minimum recommended
• Operating Systems
  o Windows XP, 7, or 8 **and** Mac OS X 10 or higher with Windows
• Web Browsers
  o Google Chrome is highly recommended
  o Internet Explorer is not recommended as it may not display certain menus and links
• Cookies **MUST** be enabled
• Pop-ups **MUST** be allowed (Pop-up Blocker disabled)
• Kindle Reader App is needed for many of our courses (No special equipment needed. This can be downloaded onto your computer.)
• Adobe PDF Reader
• Media Plug-ins (These may be required depending on your course media.)
• Adobe Flash Player (Required for many of our career courses and ALL of our IT courses.)
• Adobe Acrobat Reader, Apple QuickTime, Windows Media Player, &/or Real Player
• PowerPoint Viewer (Use this if you don't have PowerPoint)

*Outlines are subject to change, as courses and materials are updated.*
Cybersecurity - 180 Hours

Overview
This course provides a comprehensive, trustworthy framework of practices for assuring information security. Students will learn how the various roles and functions within cybersecurity practice can be combined and leveraged to produce a secure organization. Concepts will not be presented as stagnant theory; instead, they are interwoven in a real world “adventure” story that runs throughout. This approach grabs students’ attention and assists them in visualizing the application of the content to real-world issues that they will face in their professional life. The content of the course is based on the Department of Homeland Security's Essential Body of Knowledge (EBK) for IT Security.

After completing this course, you should be able to:

- Comprehend information security and the latest trends in the industry
- Describe the roles and responsibilities of the Information Security Team
- Identify the Essential Body of Knowledge competency areas
- Describe access control methods and physical security guidelines
- Identify strategies for monitoring and managing an information security system

Outline

Cybersecurity Module 1
Overview of Information Security

- Importance of Information Security
- Essential Body of Knowledge (EBK)
- Finding an Appropriate Model
- Strategic Governing Process
- Global Roadmap for Security
- EBK Competency Areas
- Roles in EBK Framework
- Implementation and Adjustment
- Adapting Best Practice
- Developing Solutions from EBK
- Chief Information Security Officer (CISO)
- Context and Scope

Cybersecurity Module 2
Information Security Team

- Defining Executive Roles
- Role of CISO
- Architect’s Role
- Data Security Function
- Functional Security Roles
- Information Security Team
- IT Security Engineer
• Designing the Security Response
• Corollary Roles for Security
• Physical Security Professional
• Privacy Professional
• Procurement Professional

Cybersecurity Module 3
EBK Competencies

• Data Security
• Standard Models for Securing Data
• Cryptography
• Digital Forensics
• Ensuring Integrity
• Routine Evaluations
• Enterprise Continuity
• Successful Preparation
• Anticipating Disasters
• Incident Management
• Structured Response
• Consistent Execution

Cybersecurity Module 4
System Development and Maintenance

• Training and Awareness
• Ensuring Secure Behavior
• Build a Knowledgeable Workforce
• Effective Review Process
• IT Systems Operations and Maintenance
• Strategic Planning
• Controls Framework
• Maintaining Operational Capability
• Network and Telecommunications Security
• Managed Networks
• Boundaries of Trust
• Network Security Function

Cybersecurity Module 5
Controls and Regulations

• Personnel Security
• Screening and Hiring
• Formal Code of Conduct
• Physical Security
• Maintaining Secure Access
• Perimeter Controls
• Effective Procurement System
• Effective Supply Chains
• Identifying Trusted Suppliers
• Legal and Regulatory Compliance
• Role of Compliance Officer
• Evaluation Programs

Cybersecurity Module 6
Risk Management

• Risk Management Planning Process
• Risk Management Controls
• Targeting Security Controls
• Measuring Risk Management Process
• Strategic Management
• Defining Control Objectives
• Details of Implementation
• Making Informed Decisions
• System and Application Security
• Measuring Against Benchmarks
• Operational Framework
• Information-Based Management Process

Required Materials:

• CompTIA Network+ Deluxe Study Guide Recommended Courseware: Exam N10-005. By: Todd Lammle
• CompTIA Security+ Deluxe Study Guide Recommended Courseware: Exam SY0-301 By: Emmett Dulaney
• Cybersecurity: The Essential Body of Knowledge by Dan Shoemaker and Wm. Arthur Conklin

System Requirements:

Internet Access
• Broadband or high-speed internet access is required. Broadband includes DSL, cable, and wireless connections.
• Dial-Up internet connections will result in a diminished online experience. Moodle pages may load slowly and viewing large audio and video files may not be possible.

Hardware
• Windows hardware configurations and processors are acceptable
• Mac computers MUST have Microsoft Window Operating Systems over Bootcamp (Bootcamp is a free download from Apple’s website)
• 1 GB RAM minimum recommended
• Operating Systems
  o Windows XP, 7, or 8 and Mac OS X 10 or higher with Windows
• Web Browsers
  o Google Chrome is highly recommended
  o Internet Explorer is not recommended as it may not display certain menus and links
• Cookies MUST be enabled
• Pop-ups MUST be allowed (Pop-up Blocker disabled)
• Kindle Reader App is needed for many of our courses (No special equipment needed. This can be downloaded onto your computer.)
• Adobe PDF Reader
• Media Plug-ins (These may be required depending on your course media.)
• Adobe Flash Player (Required for many of our career courses and ALL of our IT courses.)
• Adobe Acrobat Reader, Apple QuickTime, Windows Media Player, &/or Real Player
• PowerPoint Viewer (Use this if you don't have PowerPoint)

**Outlines are subject to change, as courses and materials are updated.**