COURSE SYLLABUS:

SECURITY+

Course Details:

Course Code: IT-5011
Course Title: Security+
Course Hours: 96 (6 Weeks)
Course Prerequisites: None
Method of Delivery: Online

Type of Instruction:

This course is delivered via Remote Mentored Learning (RML). Students view video-based instruction and access course materials from anywhere with a high-speed internet connection and have access to a team of Student Success Specialists, Advisors, and Coordinators who provide ongoing support throughout the course. This course is designed to be completed within a prescribed amount of time, with responsibilities for each course thoroughly outlined to pace the program effectively. Students learn through a variety of media, including video lecture, animations, simulations, games and activities, and more. Students are engaged in skill-building labs and real-world exercises designed to translate what is learned into critical skill-building and preparation for entering a new career. This multi-sensory learning method allows the student to control their learning schedule, the content covered, and the pace of the training while receiving personalized support, guidance, and motivation from a dedicated Student Success team.

Method of Evaluation and Grading:

This MedCerts course is considered PASS/FAIL. At the end of each chapter (lesson), students must pass a mandatory review quiz to proceed to the next chapter, with a final exam at the end of the course. Quiz and final exam grades are available immediately after completion of the quiz/exam. Each may be re-taken until a satisfactory score is achieved. This is to ensure that the student is more easily able to identify difficult/challenging areas where improvement may be needed, re-focus efforts on these areas, and then re-assess for mastery of content. To receive a PASS grade for the course, students must view all video chapters as assigned, access all required activities within the Learning Management System (LMS), and pass each chapter review quiz and the final exam with a minimum score of 80%.

Offline Supplements, Instruction & Review:

This course includes additional learning materials provided as a supplement the core training components. While students are not required to read/review or submit completed activities or assignments that are provided within these supplements, MedCerts strongly encourages students to utilize these additional resources as they will allow for a more comprehensive learning experience and will increase the likelihood of subject matter retention, and better prepare students for certification success.

Instructional Content, Text, and Training Materials:

Security+ (TotalSEM)
Recorded Video-Based Lecture/Instruction

Mike Meyers' CompTIA Security+ Certification Guide (Mike Myers & Scott Jernigan)
2nd Edition Textbook – Exam SYO-501

SY0-501 Security+ (2017) Certification Study Package (Kaplan IT Training)

Course Objectives:

- Identify the fundamental concepts of computer security.
- Identify security threats and vulnerabilities.
- Examine network security.
- Manage application, data and host security.
- Identify access control and account management security measures.
- Manage certificates.
- Identify compliance and operational security measures.
- Manage risk.
- Manage security incidents.
- Develop business continuity and disaster recovery plan

Course Description:

IT-5011 Security+ is the primary course students will need in order to gain the skills and knowledge required to gain Security+ Certification. This course is targeted toward the information technology (IT) professional who has networking and administrative skills in Windows-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks and familiarity with other operating systems, such as Mac OS X, Unix, or Linux, and who wants to further a career in IT by acquiring a foundational knowledge of security topics. In this course, students will build on knowledge and experience with security fundamentals, networks, and organizational security as they acquire the specific skills required to implement basic security services on any type of computer network. This course also provides the broad-based knowledge necessary to prepare for further study in specialized security fields.

Course Outline:

WEEK 1

Chapter 1 – Risk Management

The CIA of Security
What is Risk?
Threat Actors

Managing Risk
Using Guides for Risk Assessment
Security Controls
Interesting Security Controls
Defense in Depth
IT Security Governance
Security Policies
Frameworks
Quantitative Risk Calculations
Business Impact Analysis
Organizing Data
Security Training
Third-Party Agreements

Chapter 2 – Cryptography

Cryptography Basics
Cryptographic Methods
Symmetric Cryptosystems
Symmetric Block Modes
RSA Cryptosystems
Diffie-Hellman
PGP/GPG
Hashing
HMAC
Steganography
Certificates and Trust
Public Key Infastucture
Cryptographic Attacks

WEEK 2

Chapter 3 – Identity and Access Management

Identification
Authorization Concepts
Access Control List
Password Security
Linux File Permissions
Windows File Permissions
User Account Management
AAA
Authentication Methods
Single Sign-On

Chapter 4 – Tools of the Trade

OS Utilties, Part 1
OS Utilties, Part 2
Network Scanners
Protocol Analyzers
SNMP
Logs

WEEK 3

Chapter 5 – Security Individual Systems

Denial of Service
Host Threats
Man-in-the-Middle
System Resiliency
RAID
NAS and SAN
Physical Hardening
RFI, EMI, and ESD
Host Hardening
Data and System Security
Disk Encryption
Hardware/Firmware Security
Secure OS Types
Securing Peripherals
Malware
Analyzing Output
IDS and IPS
Automation Strategies
Data Destruction

Chapter 6 – The Basic LAN

LAN Review
Network Topologies Review
Network Zone Review
Network Access Controls
The Network Firewall
Proxy Servers
Honeypots
Virtual Private Networks
IPSec
NIDS/NIPS
SIEM (Security Information and Event Management)

WEEK 4

Chapter 7 – Beyond the Basic LAN

Wireless Review
Living in Open Networks
Vulnerabilities with Wireless Access Points
Cracking 802.11, WEP
Cracking 802.11, WPA and WPA2
Cracking 802.11, WPS
Wireless Hardening
Wireless Access Points
Virtualization Basics
Virtual Security
Containers
Infrastucture as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Deployment Models
Static Hosts

Mobile Connectivity
Deploying Mobile Devices
Mobile Enforcement
Mobile Device Management
Physical Controls
HVAC
Fire Suppression

Chapter 8 – Secure Protocols

Secure Applications and Protocols
Network Models
Know Your Protocols - TCP/IP
Know Your Protocols - Applications
Transport Layer Security (TLS)
Internet Service Hardening
Protecting Your Servers
Secure Code Development
Secure Deployment Concepts
Code Quality and Testing

WEEK 5

Chapter 9 – Testing Your Infrastructure

Vulnerability Scanning Tools
Vulnerability Scanning Assessment
Social Engineering Principles
Social Engineering Attacks
Attacking Applications
Attacking Web Sites
Exploiting a Target
Vulnerability Impact

Chapter 10 – Dealing with Incidents

Incident Response
Digital Forensics
Contingency Planning
Backups

WEEK 6

Conclusion

Course Recap

Course Final Exam