**COURSE: WIIT - 7410 Cyber Security I – ISC2 SSCP**

**DESCRIPTION OF COURSE**

This course provides a core understanding of cyber security concepts and practices. It aligns with the ISC2 SSCP Certification and a student who completes both Cyber Security I & II is prepared to take the SSCP Certification exam. This course covers the SSCP domains of Cyber Security fundamental concepts, Infrastructure & Security, Security Operations, Security Management & Compliance.

**SOFTWARE**

Software tools used in the course are for free download.

**TEXTBOOK, MANUALS, REFERENCES, AND OTHER READINGS**

The ISC2 SSCP Course Content is provided for free in blackboard.

**UNITS OF INSTRUCTION & CLASS CALENDAR**

**Core Security Concepts**

* Understanding Security Concepts
  + Confidentiality/Integrity/Availability
  + Threats vs. Vulnerabilities
  + Principle of Least Privilege
  + Resources and Prioritization
* Understanding Risk Management
  + Frameworks
  + Vulnerability Identification
  + Monitor Risks
  + Risk Responses
    - Risk Avoidance
    - Risk Acceptance
    - Transfer Risk
    - Reduce/Mitigate Risk
* Risk Assessment
  + Intentional/Unintentional Threats
  + Likelihood/Impact
  + Risk Profiles
    - Terminology (SLE, ARO, ALE)
    - Qualitative vs. Quantitative
    - Risk Determination
    - Qualitative Assessments
    - Risk Visibility
    - Risk Tolerance
  + Cost/Benefit Analysis
* Risk Remediation
  + Residual Risk
  + Controls Evaluation
  + Evaluate and Identify New Vulnerabilities

**Infrastructure & Security**

* Security Controls
  + Reactive Controls
  + Compensating Controls
  + Implementation and Assessment
  + Access Controls
    - Identity Lifecycle Overview
    - Role-based
    - Rule-based
    - Mandatory
    - Discretionary
    - Privileged Access
* System Architecture/Interoperability
  + Architectural Vulnerabilities
  + Architectural Design
* Configuration Management
  + Understand Asset Management
    - Hardware
    - Software
    - Data/Information Ownership
  + Change Management
  + Patch Management
  + Detecting Unauthorized Change
* LAN-based Security Principles/Wireless
  + Overview: Routers, Switches, Firewalls, Segmentation
  + Access control monitoring (NAC)
  + Authentication (Radius/TACACS)
  + DNS and DHCP
  + Network Attacks

**Security Operations**

* Identify and Analyze Malicious Code and Activity
  + Types of Malware
  + Attackers
  + Web Application Vulnerabilities
  + Anti-Malware Tools
* Operate and Maintain Monitoring Systems
  + Sensors and Continuous Monitoring
    - Network IDS
    - Network IPS
    - Host-based IDS
    - Host-based IPS
  + Event Logs
  + Application Logs
  + SEIM
* Vulnerability Assessment and Penetration Testing
  + Security Assessments
  + Testing Strategy
  + Vulnerability Assessments
  + Penetration Testing

**Security Management & Compliance**

* Incident Response
  + Overview
  + Discovery
  + Escalation
  + Countermeasures
  + Forensics and Legal Aspects
* Audit Findings
  + Audit Standards
  + Compliance
  + Audit Reports
* Continuity Planning
  + Principles and Overview
  + BCP
  + BIA
  + Plan Testing
  + Restoration