MARYLAND RANGE
Cyber Security Training & Simulation Center

SSCP CBK Training Seminar

The SSCP CBK Training Seminar is the ideal course for fresh graduates or IT professionals who wish to prepare for SSCP certification by honing their technical skills and provides them with practical, hands-on security knowledge in operational IT roles. It is tailored to aid participants in preparation for certification by affirming their technical ability to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability.

Course Overview

Maryland CSTR is the only Official Training Provider for SSCP CBK Training Seminars in the USA, which offers SSCP CBK curriculum integrated with **Practical Hands-on Training**. It provides a comprehensive review of information security concepts and industry best practices, covering the 7 domains of the SSCP CBK. All the training seminars are led by authorized instructors. The SSCP domains are drawn from various information security topics.

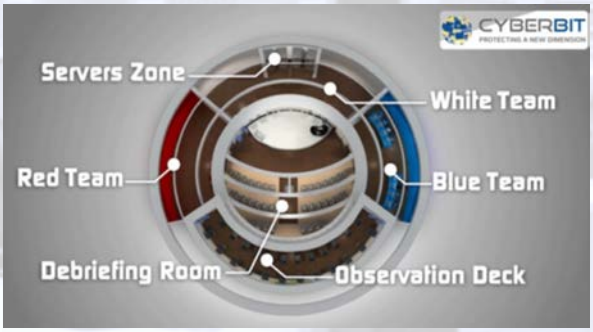
The domains include:

- Access Controls
- Security, Operations and Administration
- Risk Identification, Monitoring and Analysis
- Incident Response and Recovery
- Cryptography
- Network and Communications Security
- Systems and Application Security

The integration of the practical hands-on training increases knowledge retention and application. These activities include open ended questions from the instructor to the students, matching and poll questions, group activities, open/closed questions, group discussions, and expose to real-life cyber-attack scenarios.

The course features:

- Official (ISC)² courseware
- Taught by authorized instructors
- Student handbook
- Real-world cyber-attack scenarios
- Certificate of Completion



Training Benefits

- Integrated SSCP CBK training curriculum with realistic hands-on practical exercises
- A comprehensive review of information security concepts and industry best practices
- Confirm your breadth and depth of hands-on technical knowledge expected by employers
- Provide a career differentiator, enhancing your credibility and marketability for desirable opportunities in information security industry

Who Should Attend

The training seminar is ideal for fresh graduates or IT professionals who are looking to develop their knowledge and practical skills with the added incentive of cyber-attack scenario-based training. For individuals who do not possess the required work experience to become certified SSCPs after passing the exam, they can apply to be Associates of (ISC)² while working towards fulfilling the requirements to become certified SSCPs. The training seminar is ideal for those working in positions such as, but not limited to:

- Network Security Engineer
- Systems/Network Administrator
- Security Analyst
- Systems Engineer
- Security Consultant/Specialist
- Security Administrator
- Systems/Network Analyst
- Database Administrator

Course Structure

Day One		Day Four	
a.	**Access Controls** ▪ Implement Authentication Mechanisms ▪ Operate Internetwork Trust Architectures (e.g., extranet, third-party connections, federated access) ▪ Participate in the Identity-Management Lifecycle ▪ Implement Access Controls (e.g., subject-based,	a.	**Systems and Application Security** ▪ Identify and Analyze Malicious Code and Activity ▪ Implement and Operate Endpoint Device Security (e.g., virtualization, thin clients, thick clients, USB devices) ▪ Operate and Configure Cloud Security ▪ Secure Big Data Systems
b.	**Security Operations and Administration** ▪ Understand and Comply with Codes of Ethics ▪ Understand Security Concepts ▪ Document and Operate Security Controls ▪ Participate in Asset Management ▪ Implement and Assess Compliance with Controls ▪ Participate in Change Management ▪ Participate in Security Awareness and Training ▪ Participate in Physical Security Operations (e.g., security assessment, cameras, locks)	b.	**Practical Exercises** ▪ Introduction to Task Manager | Process Explorer | Process Monitor | Linux Commands
c.	**Practical Exercises** ▪ Introduction to Network Setup | Firewall Rules and Configurations		
Day Two		**Day Five**	
a.	**Risk Identification, Monitoring and Analysis** ▪ Understand the Risk Management Process ▪ Perform Security Assessment Activities	a.	**Incident Response and Recovery** ▪ Participate in Incident Handling ▪ Understand and Support Forensic Investigations
b.	**Practical Exercises** ▪ Introduction to Windows and Linux Logs | Network Monitoring System | SIEM	b.	**Cryptography** ▪ Understand and Apply Fundamental Concepts of Cryptography
		c.	**Practical Exercises** ▪ Incident Response Plan
Day Three		**Day Six**	
a.	**Networks and Communications Security** ▪ Understand Security Issues Related to Networks ▪ Protect Telecommunications Technologies ▪ Control Network Access ▪ Manage LAN-based Security ▪ Operate and Configure Network-Based Security Devices ▪ Implement and Operate Wireless Technologies	a.	**Cyber Range Exercises** ▪ Application of the knowledge gained on the 7 CBK® domains ▪ Develop detection and response skills through cyber range exercises ▪ Exposure to real-world cyber-attack scenarios
b.	**Practical Exercises** ▪ Network Topology		