

[www.cyberspais.com](http://www.cyberspais.com)



## CyberSPAIS Certified SOC Engineer (CCSE)



## **CyberSP AIS Certified SOC Engineer (CCSE) – Overview**

### Who Is Eligible for This Course?

- Freshers looking to launch a career in cybersecurity.
- Working professionals planning to switch to cybersecurity.

### Course Duration

- 5 Months (200 Hours)

### Potential Job Roles Relevant to The Course

- Security Analyst, Security Engineer, Vulnerability Analyst, Penetration Tester, Red & Blue Teaming, Bug Bounty Hunting, Security Consultant, Cybersecurity Engineer, Network Engineer, Network Security Analyst, Server Administrator, Server Security Specialist, Cloud Specialist, Cloud Security Engineer, Threat Hunter, Cybersecurity Analyst, Application Security Analyst, Threat Intelligence Analyst, Security Consultant.

### Course Syllabus

- Module 1: Network & Communications Security - 40 Hours
- Module 2: Server & OS Security - 30 Hours
- Module 3: Cloud Security (AWS) - 30 Hours
- Module 4: Ethical Hacking (CEH) - 40 Hours
- Module 5: Penetration Testing & Red Teaming - 20 Hours
- Module 6: Security Operations Centre (SOC) - 40 Hours

### Potential Certifications Relevant to The Course

- CCNA, CompTIA Network+, CompTIA Security+, AWS Cloud Practitioner, AWS Certified Security, CEH, CPENT, CompTIA Pentest+, CSA, CySA+

### Why Training @CyberSP AIS?

- Job Oriented Industry Relevant Curriculum
- Based On Latest Cyber Security Topics & Trends
- 100% Assistance for Placements & Internships
- Industry Experienced & Certified Trainer
- Concepts Explained with Industry Scenarios
- Comprehensive Hands-on Sessions & Labs
- Regular Module Wise Assessments & Evaluations
- Cybersecurity Projects & Internships
- Thorough Preparation – Job Interview & Soft Skills
- Facility For Writing Certification Exams

## **CyberSPAIS Certified SOC Engineer (CCSE) – Syllabus**

### Module 1: Network & Communications Security (40 Hours) – Theory & Lab

- Security Fundamentals
- Identity & Access Management
- Data & Asset Security
- Practical Cryptography
- Networking Fundamentals
- Converged Protocols
- Multilayer Protocol
- Securing Network Devices
- Secure Routing Protocols
- Switching and Virtual LANs
- Firewall Architecture & Types
- Network Segmentation & Microsegmentation
- Intrusion Detection & Prevention Systems (IDS/IPS)
- Securing Edge & Fog Computing
- Wi-Fi, Cellular & Satellite Communications
- Wireless Attacks
- Wireless Network Security
- Content Distributed Networks (CDN)
- Network Access Control
- Port Based NAC
- Proxy Servers
- Content/URL Filter
- Endpoint Security (AV, EDR/XDR, HIDPS)
- Port Security
- DHCP Snooping
- Quality of Service (QoS)
- Secure Voice Communications
- Remote Access Security
- Authentication Protocols
- Virtual Private Networks (VPN) - IPSec
- Securing Multimedia Collaboration
- Network Monitoring
- Network Load Balancing
- Email Security
- MAC Flooding Attack
- MAC Cloning
- ARP Spoofing & Poisoning
- DHCP Security
- DNS Attacks
- DNS Security
- SNMP Security

- Kerberos Attacks
- Mobile Security
- IoT Security
- ICS/OT Security
- Securing WAN Technologies
- Circuit Switching
- Packet Switching
- Virtual Circuits
- Software Defined Networking (SDN)
- Assessment

 **Module 2: Server & OS Security (30 Hours) – Theory & Lab**

- Installing Linux & Windows Server OS
- Basic Commands & Administration (Linux, Windows)
- Server Hardening (Linux, Windows)
- Managing Users & Groups (Linux, Windows)
- Pluggable Authentication Module (PAM) (Linux)
- Configuring Secure Password Policy (Linux, Windows)
- Securing Active Directory (Windows)
- Configuring Group Policy (Windows)
- Privileged Account Management (Linux, Windows)
- File & Directory Permissions (Linux, Windows)
- Configuring RAID (Linux, Windows)
- Disk & File Encryption (Linux, Windows)
- Managing Backups (Linux, Windows)
- Secure Boot (Linux, Windows)
- Network Load Balancing & Clustering (Linux, Windows)
- Patch Management (Linux, Windows)
- Hardware Security Modules (TPM)
- Virtualization Security (Linux, Windows)
- Container Security (Linux, Windows)
- Endpoint Security (Linux, Windows)
- Linux Firewalls
- SELinux
- Assessment

 **Module 3: AWS Cloud Security (30 Hours)**

- Cloud Fundamentals
- Identity & Access Management
- Securing Elastic Compute Cloud (EC2)
- Elastic Load Balancing & Auto Scaling Groups (ELB & ASG)
- Cloud Monitoring (Cloud Watch)
- Amazon S3 Security

- Securing Route 53
- CloudFront
- Global Accelerator
- VPC & Networking Security
- SSL/TLS Encryption
- Key Management System
- Auditing & Logging (CloudTrail)
- Network Flow Capture
- Securing Messaging Services
- GuardDuty
- Security Incident Response
- AWS Security Tools
- Threat Detection and Incident Response
- Security Logging and Monitoring
- Infrastructure Security
- Identity and Access Management
- Data Protection Management
- Security Governance
- Assessment

 **Module 4: Ethical Hacking (CEH) (40 Hours)**

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography
- Assessment








 Module 5: Penetration Testing & Red Teaming (20 Hours)

- Planning a Penetration Test
- Introduction to Anonymity
- Reconnaissance & Information Gathering
- Open-Source Intelligence (OSINT)
- Scanning & Enumeration
- Vulnerability Mapping
- Exploitation & Gaining Access
- Social Engineering PenTest
- Wireless PenTest
- Network PenTest
- IAM PenTest
- System & AD PenTest
- Web Application PenTest
- Cloud PenTest
- Mobile, IoT & OT PenTest
- Post Exploitation Actions
- Cleanup & Restoration
- Penetration Test Reporting
- Red Teaming & Blue Teaming
- Assessment

 Module 6: Security Operations Centre (SOC) (40 Hours)

- SOC Fundamentals
- SOC Architecture & Processes
- SOC Roles & Responsibilities
- SOC Generations & Tools
- Security Information & Event Management (SIEM)
- Understanding SIEM Tools (Splunk)
- Asset & Media Protection
- Blacklisting & Whitelisting
- Configuration Management
- Change Management
- Patch Management
- Vulnerability Management
- CVE, CWE, NVD, SCAP, OWASP Top 10
- Botnets, DoS & DDoS Attacks
- DoS & DDoS Protection
- Firewall, IDS/IPS, DLP
- Malware Types
- Antimalware, EDR/XDR
- Honeypots & Honeynets
- Log Management & Protection

- User Entity Behavior Analytics (UEBA)
- Cyber Kill Chain
- Unified Kill Chain
- MITRE Attack Framework
- Threat Intelligence
- Threat Hunting
- Incident Management
- Automating Incident Response (SOAR)
- Security Investigations & Forensics
- Red & Blue Teaming
- Redundancy & Fault Tolerance
- Assessment

-  Project
-  Final Exam
-  Certification Preparation
-  Soft Skill Preparation
-  Interview Preparation
-  Issue Course Certificate
-  Placement Evaluation & Assistance