CERTCOP

CERTIFIED CYBER COP

Certcop - A Division of Secbay

Certified Cybercop Cybersecurity Engineer

CERTCOP

CERTIFIED CYBER SECURITY ENGINEER

CERTCOP
CERTIFIED CYBER COP

About Certcop

We combine the latest cyber tools with original in-house designs to develop customized and advanced cyber security programs to meet the client's requirements. CertCop offers training programs in the areas of pen testing using Kali Linux, Cyber Security Management, Incident Handling & Disaster Recovery, Application Security, Secure Coding, and customized SOC training programs according to client requirements.

- Certified and highly experienced instructors
- Certcop Flexible Scheduling (Days, evenings, weekends)
- Delivery Methods:
  Virtual Live/In-Class/On-site/
  1 on 1/ On-Demand
- Certcop Curriculum is of High Quality, Extensive, and Industry Standard.

CERTCOP
CERTIFIED CYBER COP

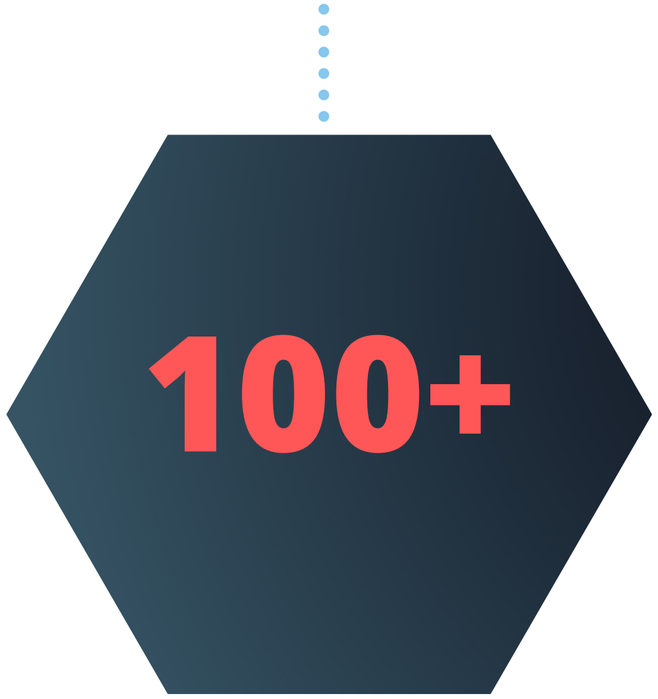
Proud to be one of the GLOBAL LEADERS in

Certcop Affiliation

Affiliated
Certification Vendors

Certcop Certcamps

Upcoming Cyber
Security Training



Certcop Trainings

Corporate and Govt.
Agencies Trained

CERTCOP
CERTIFIED CYBER COP

Partial List of Our Clients

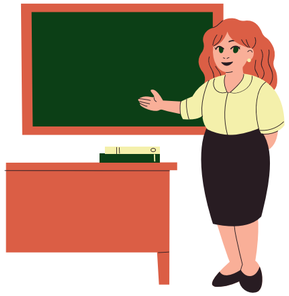
CERTCOP
CERTIFIED CYBER COP

OUR DELIVERY METHODS

Group Training

Individual Training

Instructor-Led Virtual live



Instructor-Led Classroom

On Demand

CERTCOP
CERTIFIED CYBER COP

About Program

Certcop's Cyber Security Engineer is designed to give you a foundational look at today's cybersecurity landscape and provide you with the tools to evaluate and manage security protocols in information processing systems.

A cybersecurity engineer is a professional who creates and executes secure network solutions that provide security against cyber-attacks, hackers, etc. They also regularly monitor and test those systems to ensure that the systems and networks are updated and functioning well.

CERTCOP
CERTIFIED CYBER COP

About Program

Target Audience

- 1. IT Professionals
- 2. Bounty Hunters
- 3. Entry Level Red Teamers
- 4. Pentesters
- 5. Cyber Security Analysts
- 6. Incident Responders

Requirements

- 1. Security & Network Basics
- 2. OWASP Top 10
- 3. Basic Incident Response Terminologies.

Skills Covered

- Cybersecurity fundamentals
- Threat actors attacks
- Mitigation
- Security policies
- Secure architecture
- Wireless networks
- Network security controls
- Risk management

CERTCOP
CERTIFIED CYBER COP

Exam Details

Course Name: Certified CyberCop – CCSE
Course Number: CertCopCCSE03
Required exam – CCSE-03
Number of questions – Maximum of 100
Types of questions – Multiple-choice and performance-based
Length of test – 180 minutes
Passing score – 70% – This test has no scaled score; it's pass/fail only.
Languages – English
Retirement – Usually three years after launch
Testing Provider – Online proctoring: ExamIT.com
Certification Exam Voucher – $395 USD

CERTCOP
CERTIFIED CYBER COP

Course Content

1.0 About the Program and Certification

- 1.1 About the Course
- 1.2 DoD Cybersecurity Workforce/8140/8570
- 1.3 Best Practices
- 1.4 About the Program: Certified Cybersecurity Engineer
- 1.5 Course Topics

2.0 Cybersecurity fundamentals -Network Essentials

- 2.1 History of Computing
- 2.2 Internet Timeline- ARPANET, DNS
- 2.3 Famous First
- 2.4 What is a computer?
- 2.5 Network Addresses, Network Interface Card
- 2.6 ARP commands
- 2.7 Windows Commands
- 2.8 CIA Triad, Network Essentials
- 2.9 Regional Internet Registries/Internet Assigned Number Authority (IANA)
- 2.10 Ports and Protocols
- 2.11 Network Topologies

CERTCOP
CERTIFIED CYBER COP

3.0 Network Fundamentals Design

- 3.1 Packet Capture and Replay
- 3.2 Packet Sniffer
- 3.3 Protocol Analyzers (a packet analyzer)
- 3.4 Wireshark
- 3.5 Who should use Wireshark?
- 3.6 Wireshark Demo
- 3.7 Tcpdump
- 3.8 Packet sniffer in the cloud
- 3.9 Writing a packet capture to a text file
- 3.10 Wireshark's cousin- tshark
- 3.11 Tcpreplay
- 3.12 Common Networking Protocols
- 3.13 DNS Tools- nslookup, dig
- 3.14 DNS Record Types
- 3.15 Querying multiple servers
- 3.16 DNS Poisoning
- 3.17 Session Hijacking
- 3.18 Wireless Networking-Wireless Access Point
- 3.19 Fat vs. Thin Access Point
- 3.20 WiFi Spectrum
- 3.21 MAC Filtering
- 3.22 Wireless Antennas
- 3.23 VLANs
- 3.24 DMZ- Screened Subnet
- 3.25 Virtual Private Network/VPN
- 3.26 Secure Protocols- DNSSEC, SSH, SMIME, SRTP, LDAPS, FTPS, SFTP, SNMP Version 3, HTTPS, IPSEC
- 3.27 Voice and Video Use Cases
- 3.28 Network Time Protocol (NTP)
- 3.29 Load Balancing
- 3.30 Out of Band Management

CERTCOP
CERTIFIED CYBER COP

- 3.31 Port Security
- 3.32 Network Appliances
- 3.33 Access Control Lists
- 3.34 Route Security
- 3.35 Implications of IPv6
- 3.36 Port Spanning
- 3.37 Port Mirroring
- 3.38 IP Addressing
- 3.39 Internet Protocol Purpose
- 3.40 Subnet Masking
- 3.41 Default Gateways
- 3.42 Makeup of IPv4 packet
- 3.43 IPv4 vs. IPv6
- 3.44 Binary to Decimal Conversion

4.0 Security Architecture

- 4.1 Packet Capture and Replay
- 4.2 Implement and Manage Engineering Processes using Secure Design Principles
- 4.3 Separation of Duties
- 4.4 Principle of Least Privilege (POLP)
- 4.5 Threat Modeling Methodologies
- 4.6 Security Models
- 4.7 Minimize Attack Surface
- 4.8 Defense in Depth
- 4.9 Understand Fundamentals of Security Models
- 4.10 Select Controls Based on System Requirements

CERTCOP
CERTIFIED CYBER COP

- 4.11 Understand Capabilities of Information Systems
- 4.12 Assess and Mitigate Security Vulnerabilities
- 4.13 Client Based Systems -Network Essentials
- 4.14 Server Based Systems Network Essentials
- 4.15 Database Systems 3nf, 2nf, 1f, SQL injection
- 4.16 Distributed Systems
- 4.17 Internet of Things
- 4.18 Industrial Control Systems

5.0 IDM (PAM, IAM)

- 5.1 Controlling Access to Assets
- 5.2 Comparing Identification and Authentication
- 5.3 Implementing Identity Management
- 5.4 Managing Identity and Access Provisioning Lifecycle
- 5.5 Remote Access Security Management
- 5.6 VPN – with respect to IAM/PAM
- 5.7 Information Systems Capabilities Cloud+
- 5.8 Working remotely from home

CERTCOP
CERTIFIED CYBER COP

6.0 Access Control

- 6.1 Access Control Models
- 6.2 Permissions, Rights, Privileges
- 6.3 Implicit Deny
- 6.4 Access Control Matrix
- 6.5 Constrained Interface
- 6.6 Content Dependent Control – CISSP- CDI
- 6.7 Context Dependent Control CISSP- UDI
- 6.8 POLP- Principle of Least Privilege
- 6.9 Separation Duties Privilege

7.0 Data Protection

- 7.1 Data in Transit
- 7.2 Data in Use
- 7.3 Data Retention
- 7.4 Data Remnants
- 7.5 Destruction
- 7.6 Backups -redundancy-
- 7.7 Purging
- 7.8 Wiping
- 7.9 Overwriting
- 7.10 Pulping

CERTCOP
CERTIFIED CYBER COP

8.0 Network Design

- 8.1 WAN, LAN, MAN, Campus LAN
- 8.2 PAN, WLAN
- 8.3 Network Essentials
- 8.4 Data Center.
- 8.5 Infrastructure.
- 8.6 Network management.
- 8.7 Network Security.
- 8.8 Networking careers.
- 8.9 IaC/Software Defined Networking, SDN

9.0 Cloud Security

- 9.1 Cloud Models
- 9.2 Cloud Organizations
- 9.3 Cloud Components
- 9.4 RMF- Risk Management Framework/CSF/NICE 2.0
- 9.5 Intro to FedRAMP
- 9.6 Intro to AI/ML
- 9.7 Differences between AI/ML
- 9.8 Current market uses – face detection, spam filtering, image recognition
- 9.9 Anaconda,
- 9.10 Cloud Security alliance
- 9.11 CIS Benchmarks
- 9.12 Frameworks and Guides- GDPR, PCI-DSS, NIST, CSF, ISO, SSAE
- 9.13 AI Tools

CERTCOP
CERTIFIED CYBER COP

10.0 Penetration Testing

- 10.1 Port Scanner
- 10.2 Nmap, ping, CLI
- 10.3 Packet Sniffing
- 10.4 tcpdump
- 10.5 Wireshark
- 10.6 SCAP
- 10.7 CVSS
- 10.8 NCP
- 10.9 Network Enumeration- SNMP enumeration
- 10.10 Burp Suite
- 10.11 Application Security
- 10.12 Fiddler
- 10.13 OpenVAS
- 10.14 Metasploit
- 10.15 Msfvenom
- 10.16 Core Impact
- 10.17 Cobalt Strike
- 10.18 Raspberry Pi
- 10.19 FPGA

CERTCOP
CERTIFIED CYBER COP

11.0 Compliance

- 11.1 Security Governance
- 11.2 Regulatory Compliance
- 11.3 Compliance
- 11.4 Strategic Plan
- 11.5 Tactical Plan
- 11.6 Operational Plan
- 11.7 Change Control Management
- 11.8 Security Standards, Baselines, Guidelines
- 11.9 Supply Chain Management

12.0 OSINT

- 12.1 Create an OSINT process
- 12.2 Conduct OSINT investigations in support of a wide range of customers
- 12.3 Understand the data collection life cycle
- 12.4 Create a secure platform for data collection
- 12.5 Analyze customer collection requirements
- 12.6 Capture and record data
- 12.7 Create sock puppet accounts- need to look into
- 12.8 Harvest web data
- 12.9 Perform searches for people
- 12.10 Access social media data
- 12.11 Assess a remote location using online cameras and maps- Shodan
- 12.12 Examine geolocated social media- metadata
- 12.13 Research businesses- open document search
- 12.14 Collect data from the dark web

CERTCOP
CERTIFIED CYBER COP

13.0 Risk Analysis

- 13.1 Risk Management
- 13.2 Threats
- 13.3 Manmade, Internal, External
- 13.4 Exploits
- 13.5 Quantitative Risk Management
- 13.6 Qualitative Risk Management
- 13.7 Risk Register
- 13.8 Supply Chain Management
- 13.9 Stakeholder Management
- 13.10 Risk Management Strategies
- 13.11 Risk Avoidance
- 13.12 Risk Mitigation
- 13.13 Risk Acceptance
- 13.14 Risk Outsourcing/Risk Transference
- 13.15 Resiliency
- 13.16 SLE=ALE x ARO CySA- Module 5.2
- 13.17 Malicious Human Threats
- 13.18 Accidental Human Threats
- 13.19 Environmental Threats
- 13.20 Threat assessment
- 13.21 Vulnerabilities
- 13.22 Default Configurations
- 13.23 Lack of Malware or updated definitions
- 13.24 Misconfigured or lack of firewalls

CERTCOP
CERTIFIED CYBER COP

14.0 Assessments and Audits

- 14.1 Security Audit vs Security Assessment
- 14.2 Password Audit
- 14.3 Compliance Audit
- 14.4 Information System Audit
- 14.5 internal Audit
- 14.6 External Audit
- 14.7 Best Practices
- 14.8 Physical Security Audit
- 14.9 Information Governance Audit
- 14.10 checklists for Audit
- 14.11 Virtual vs. Physical
- 14.12 STRIDE Model
- 14.13 DREAD Model
- 14.14 PASTA

15.0 Secure Application Development management

- 115.1 Software Development
- 15.2 Environment
- 15.3 Development
- 15.4 Test
- 15.5 Staging
- 15.6 Production
- 15.7 Quality assurance (QA)
- 15.8 Provisioning and de-provisioning
- 15.9 Integrity measurement
- 15.10 Secure coding techniques
- 15.11 Normalization
- 15.12 Stored procedures
- 15.13 Obfuscation/camouflage

CERTCOP
CERTIFIED CYBER COP

- 15.14 Code reuse/dead code
- 15.15 Server-side vs. client-side
- 15.16 Execution and validation
- 15.17 Memory management
- 15.18 Use of third-party libraries and
- 15.19 Software development kits (SDKs)
- 15.20 Data Exposure
- 15.21 Open Web Application
- 15.22 Security Project (OWASP)
- 15.23 Software Diversity
- 15.24 Compiler
- 15.25 Binary
- 15.26 Automation/scripting
- 15.27 Automated courses of action
- 15.28 Continuous monitoring
- 15.29 Continuous validation
- 15.30 Continuous integration (CI)
- 15.31 Continuous delivery (CD)
- 15.32 Continuous deployment (CD also?)
- 15.33 Elasticity
- 15.34 Scalability
- 15.35 Version control
- 15.36 Object Oriented Technology
- 15.37 Application Security
- 15.38 Input validation
- 15.39 Secure cookies
- 15.40 Hypertext Transfer

CERTCOP
CERTIFIED CYBER COP

- 15.41 Protocol (HTTP) headers
- 15.42 Code signing
- 15.43 Allow list
- 15.44 Block list/deny list
- 15.45 Secure coding practices
- 15.46 Static code analysis
- 15.47 Manual code review
- 15.48 Dynamic code analysis
- 15.49 Fuzzing

16.0 Cryptography

- 16.1 Brief History of Cryptography
- 16.2 Goals of Cryptography
- 16.3 Cryptographic Keys
- 16.4 Asymmetric Encryption
- 16.5 Secure Symmetric Encryption
- 16.6 Digital Signatures
- 16.7 Message Digest
- 16.8 Block Cipher vs. Stream Cipher
- 16.9 Block Cipher Modes
- 16.10 Symmetric Algorithms
- 16.11 Asymmetric Algorithms
- 16.12 PKI, RSA, Diffie Hellman

CERTCOP
CERTIFIED CYBER COP

- 16.13 AES, Twofish, Blowfish, IDEA,
- 16.14 Enigma
- 16.15 Caesar Cipher/Substitution Ciphers
- 16.16 Kerchoff's Principle
- 16.17 Logical Operations – AND, OR, NOR, NOT, XOR
- 16.18 Boolean Mathematics
- 16.19 Modulus Function
- 16.20 One-Way Functions
- 16.21 Nonce
- 16.22 Cryptographic Keys

17.0 Biometrics

- 17.1 Fingerprint
- 17.2 Retina modality video
- 17.3 Iris – iris recognition
- 17.4 Facial
- 17.5 Voice
- 17.6 Vein
- 17.7 Gait
- 17.8 Efficacy
- 17.9 False Acceptance Rate (FAR)
- 17.10 False Rejection Rate (FRR)

CERTCOP
CERTIFIED CYBER COP

18.0 Working Remote-WFH-COVID-19

- 18.1 Working Remotely Intro
- 18.2 Remote Work Studies
- 18.3 What companies are saying
- 18.4 Unsecured Public WIFi
- 18.5 Gelocations/Smartphones
- 18.6 Work From Home Tools
- 18.7 Private Browsing/VPNs
- 18.8 Mixing Personal and Company Data
- 18.9 Which OS Should I choose
- 18.10 Chromebooks
- 18.11 Smartphone Security
- 18.12 Dangerous Malicious Mobile Apps

CERTCOP
CERTIFIED CYBER COP

Clients Testimonials

Got certified in Cybercop Red Team tutors are just great. They are very practical in their approach and help you learn things faster.
Bark - Security Analyst

The instructor was great and had amazing energy throughout. He also added a lot of additional material and customized the class. I really got what I needed out of this course.
AutoDesk

I enjoyed the Red Team course and want to stick with you guys for more training in the near future for Reconisense, Cloud Security, and Report Writing.
Marcus - Managing Director

CERTCOP
CERTIFIED CYBER COP

50+ Certcamp Location Across the Globe

Certcop - A Division of Secbay

info@certcop.com

CertCop, A Secbay Company
11710 Plaza America Drive Suite 2000
Reston, VA - USA