CERTCOP

CERTIFIED CYBER COP

Certcop - A Division of Secbay

Certified Cybercop Blue Team

CERTCOP

BLUE TEAM CERTIFIED - DEFENSIVE SECURITY

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

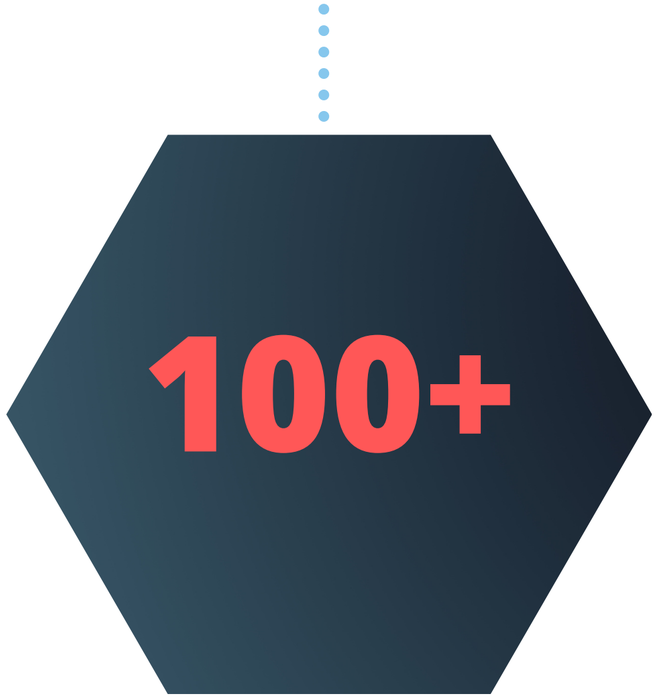
Proud to be one of the GLOBAL LEADERS in

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

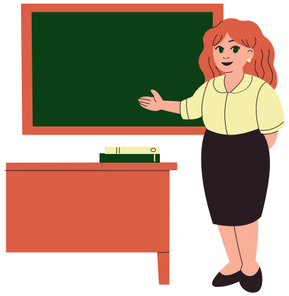
CERTCOP
CERTIFIED CYBER COP

OUR DELIVERY METHODS

Group Training

Individual Training

Instructor-Led Virtual live



Instructor-Led Classroom

On Demand

CERTCOP
CERTIFIED CYBER COP

About Program

The Certified Cybercop Blue Team program is designed to teach and evaluate real defensive security abilities across a wide variety of blue-team disciplines, making it ideal for newcomers to the sector as well as seasoned security professionals.

Target Audience

- Security/Network Defenders
- Security enthusiasts
- Students
- Entry-level Cybersecurity Positions

Prerequisite

This course requires a basic familiarity with TCP/IP and operating system principles. It's a plus if you're familiar with the Linux command line, network security monitoring, and SIEM technologies. Some fundamental security concepts are expected at this level.

CERTCOP
CERTIFIED CYBER COP

Exam Details

Course Name : Certified CyberCop – Blue Team
Course Number : CertCopBT01
Required exam – CCBT-E002
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 Blue Team Methodology

- 1.1 Intro what is the blue team
- 1.2 Why do we need the blue team?
- 1.3 What is blue teaming and how is it different?
- 1.4 What organizations should use Blue Teaming?
- 1.5 What does a Blue Team Do?
- 1.6 Purpose of Blue Team Exercise?
- 1.7 Blue Team Use Cases/Misuse Cases?
- 1.8 What kind of person should be on a Blue Team?
- 1.9 What to test in Blue Team?
- 1.10 Difference between Red Team and Blue Team
- 1.11 Example of Blue Team?
- 1.12 What is the goal of a blue team?

2.0 Intro to Linux

- 2.1 Introduction to Linux
- 2.2 UNIX Architecture
- 2.3 Advantages of Linux
- 2.4 Linux Basic Commands
- 2.5 Unix / Linux - File Management
- 2.6 Linux - File Permission / Access Modes

3.0 Identity and Access (IAM)

- 3.1 What is identity and access management?
- 3.2 Why do we need IAM?
- 3.3 How does IAM Work?
- 3.4 IAM Functionality
- 3.5 Difference between identity management and access management
- 3.6 AWS identity and access management
- 3.7 Tools to implement identity and access management
- 3.8 Identity and Access Management Technologies

4.0 Vulnerability Scanning

- 4.1 Vulnerability Scanning
- 4.2 Vulnerability Scanning Vs. Penetration Testing
- 4.3 How Vulnerability Scanning Works
- 4.4 Types of Vulnerability Scanners
- 4.5 External Vs Internal Vulnerability Scans
- 4.6 Authenticated Vs. Unauthenticated Vulnerability Scans

5.0 Linux Firewalls

- 5.1 firewall
- 5.2 How do Firewalls Work
- 5.3 Types of Firewalls
- 5.4 IP Tables
- 5.5 IP Tables – Tables and Chains
- 5.6 IP Tables and Rules
- 5.7 Uncomplicated Firewall

6.0 Security Information and Event Management (SIEM)

- 6.1 security information and event management (SIEM)
- 6.2 Legacy Siem vs. Modern Siem
- 6.3 NIST Requirements for Security Tools
- 6.4 Log Aggregation
- 6.5 Log Deduplication
- 6.6 Log Forensics
- 6.7 Event Correlation and Alerting
- 6.8 Real-Time Alerting
- 6.9 File Integrity Monitoring
- 6.10 Log Analysis with Dashboards
- 6.11 Privileged User Monitoring
- 6.12 Compliance Audits
- 6.13 Archiving Data
- 6.14 SIEM Tools

7.0 Incident Response Toolkit

- 7.1 Incident Response Toolkit
- 7.2 How IR Management Tools Work
- 7.3 IR Management Tool Features
- 7.4 Types of Incident Response Toolkits
- 7.5 Cyber Incident Response Toolkits in Industrial Spaces
- 7.6 Know Environmental Safety Protocols
- 7.7 What does an Incident Response team do?
- 7.8 Incident Response Plan Management
- 7.9 Indicators of Compromise (IOC)
- 7.10 Incident Response Tools

8.0 Digital Forensics

- 8.1 Digital Forensics
- 8.2 History of Digital Evidence
- 8.3 Objectives of Computer Forensics
- 8.4 Process of Digital Forensics
- 8.5 What Tools Are Used For Digital Forensics?
- 8.6 Types of Digital Evidences
- 8.7 What are the Main Challenges in Digital Forensics?
- 8.8 Advantages of Digital Forensics
- 8.9 Disadvantages of Digital Forensics

9.0 SOAR – Security Orchestration Automation Response

- 9.1 SOAR
- 9.2 Common Themes in Security
- 9.3 Essential Soar Characteristics
- 9.4 Runbooks
- 9.5 Machine Learning
- 9.6 Soar Relation to Incident Response

10.0 Digital Forensics

- 10.1 Risk Mitigation
- 10.2 Cybersecurity Risk Mitigation
- 10.3 Conducting a Risk Assessment to Determine Vulnerabilities
- 10.4 Establish Network Access Controls
- 10.5 Implement Firewalls and Antivirus Software
- 10.6 Creating a Patch Management Schedule
- 10.7 Continuously Monitor Network Traffic
- 10.8 Build an Incident Response Plan
- 10.9 Research and Development in Cybersecurity

11.0 Software Development Life Cycle (SDLC)

- 11.1 Software Development Life Cycle
- 11.2 Software Development Security
- 11.3 Data Warehousing
- 11.4 SEI-CMMI

12.0 Setting Localization Options

- 12.1 Localization
- 12.2 Setting Environment Variables
- 12.3 Change Environment Variables Manually

13.0 Sifting through Services

- 13.1 Linux Server
- 13.2 Important Server Commands
- 13.3 What is a Kernel
- 13.4 Serving up the Basics

14.0 Threat and Vulnerability Management

- 14.1 Threat and Vulnerability Management
- 14.2 4 Major Elements
- 14.3 Threat and Vulnerability Management-Baseline
- 14.4 Threat and Vulnerability Analysis
- 14.5 Vulnerability Enumeration
- 14.6 Remediation Planning
- 14.7 Vulnerability Lifecycle Management

15.0 Cryptography and PKI

- 15.1 Cryptography
- 15.2 Cryptography Techniques
- 15.3 Types of Cryptography
- 15.4 Cryptography Tools
- 15.5 cryptography algorithms
- 15.6 Applications of Cryptography
- 15.7 Public Key Infrastructure
- 15.8 What makes up a PKI?
- 15.9 What is a Digital Certificate?
- 15.10 What is Electronic Identity?
- 15.11 PKI Authentication
- 15.12 PKI Digital Signing
- 15.13 PKI Encryption and Decryption of Data

16.0 Package Management and Repositories

- 16.1 Introduction
- 16.2 APT AND DPKG
- 16.3 Understanding the Sources. List File
- 16.4 Kali Repositories
- 16.5 Initializing APT
- 16.6 Installing Packages
- 16.7 Upgrading Kali Linux
- 16.8 Apt Cache Command
- 16.9 Dpkg Log File
- 16.10 Reinstalling Packages With Apt -- Reinstall and Aptitude Reinstall
- 16.11 Gnome Package Manager
- 16.12 KDE Discover
- 16.13 Snap Installer
- 16.14 Other Package Managers

17.0 Mobile Device Hacking

- 17.1 Mobile Device Hacking
- 17.2 OWASP Mobile Top 10 Risks
- 17.3 Mobile Application Attack Vectors
- 17.4 Anatomy of Mobile Attack
- 17.5 Types of Attacks
- 17.6 Android Device Hacking
- 17.7 IOS Device Hacking
- 17.8 IOS Jail Breaking

18.0 Kali Linux Bash Scripting

- 18.1 Bash Scripting
- 18.2 Shell Comparison
- 18.3 Other Shells
- 18.4 Started With a Shell
- 18.5 Bashrc File

19.0 Recruiting Blue Team Members

- 19.1 Blue Team Roles
- 19.2 skills required for blue team members
- 19.3 Personality Traits Required for Blue Team Members
- 19.4 Outsourcing vs. Developing In House
- 19.5 Soft Skills required for blue team members
- 19.6 Interpersonal Skills
- 19.7 Project Management
- 19.8 Be a Team Player
- 19.9 Leadership

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