



SECURE THE DIGITAL



CYBER A1 CERTIFIED CYBER SECURITY EXPERT

1 Year Training / 200 Hour Training

An ISO 9001 - 2015 Certified Company

Copyright © 2021 by Cyber A1 Global Solutions LLP
All rights reserved.



Overview of **CYBER A1 CERTIFIED CYBER SECURITY EXPERT**

We foresee that our future is in the hands of young, technologically advanced and interconnected cyber world. To prepare our cyberspace against more advanced and highly malicious cyber-attacks we are hunting for Cybersecurity and Ethical Hacking enthusiasts who have the will to be in the Cybersecurity frontiers of the future.

Our Cyber A1 Certified Cyber Security Expert program looks to fish for geniuses who need discovery and nurturing by the right Cybersecurity and Hacking masters to take their potential to the next level of excellence.

CCSE was built to incorporate a hands-on environment and systematic process across every ethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to perform the job of a Cyber Security Expert. You will be exposed to an entirely different posture towards the responsibilities and measures required to be secure

HIGHLIGHTS OF THE Learning Path

200+ Hours of Training



5-8 Students in a Batch

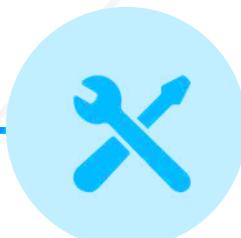
1:1 Mentoring also available

Soft skills along with technical trainings.



Learn from Industry Experts

40GB + Lab Material And Tools



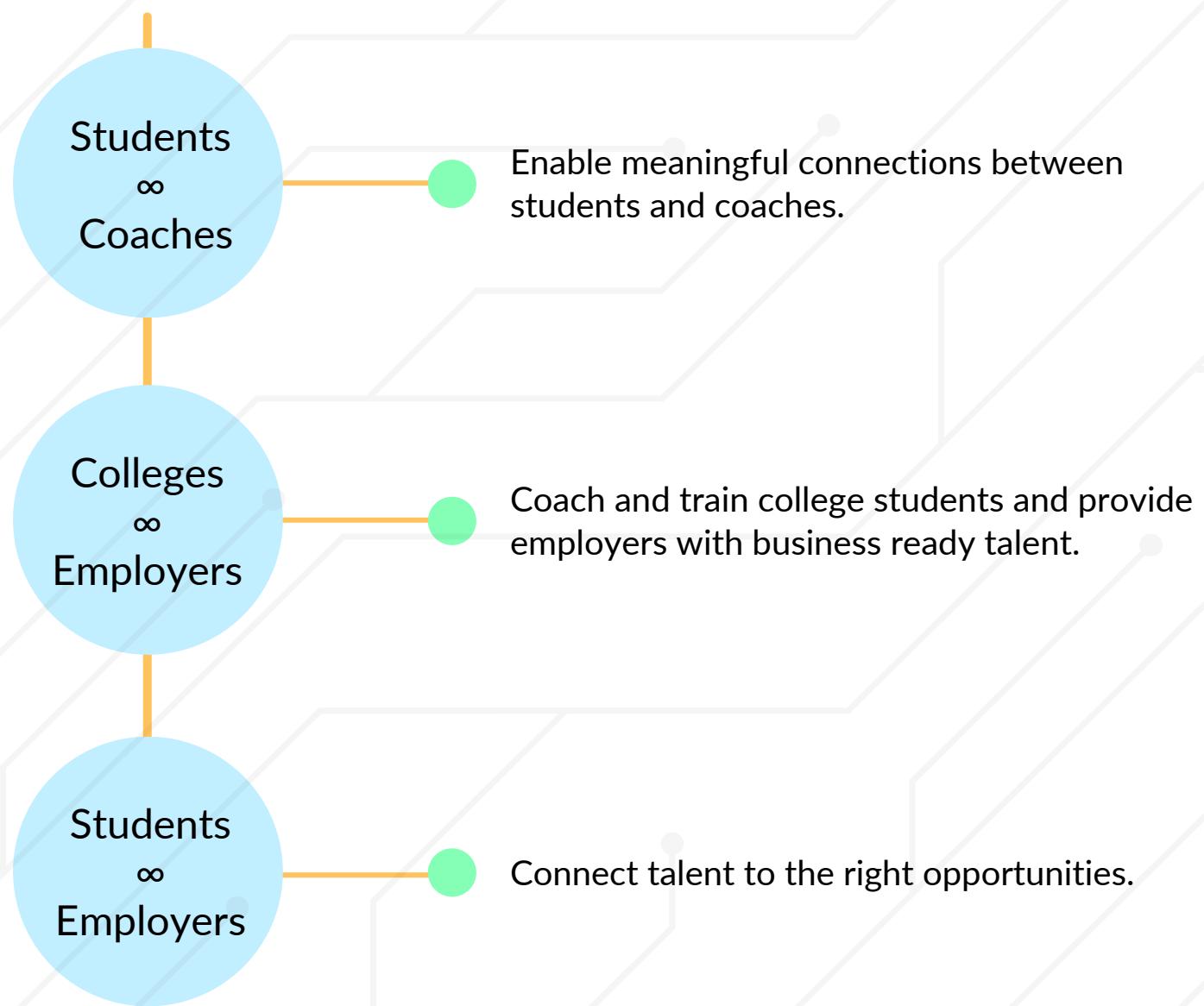
WHO WE ARE?

Cyber A1 Global Solution LLP provides quality trainings in field of Ethical Hacking, Bug Bounties, Network Security, and Cyber Forensics.

Innovative and real-time experience courses tailored for the Industry for hands-on and practical exposure We believe and have a vision to educate and make professionals ready for the future.

We build real-world simulated environment to train students in the field of cyber security

OUR OBJECTIVES?



Top 07 Reasons To Learn Cybersecurity

7. Cybersecurity – An Evergreen Industry
6. Travel the World with Cybersecurity
5. A Chance to Work with Secret Agencies
4. Unlimited Potential for Personal Growth
3. A Variety of Industries to Choose
2. A Job that Never Gets Boring
1. Fat Pay Cheques

Eligibility Criteria for CCEH

- **Background and Education Requirements**

Currently, there is no standard education requirement to be a white hat hacker. But a bachelor's degree or diploma in IT security system and computer science subject is an additional opportunity.

Additionally, relevant job experience is also a plus for recruitment.

- **Stay Legal**

It's important to make one mind in the early stages to never engage in "black hat" hacking activities. Undeniably, it is, totally unethical to engage in someone else's network without their permission. Engaging in other networks is an illegal activity, which can ruin your ethical hacking career and even put you behind the bars.

Before hiring an ethical hacker every organization requires security clearance from the government and if the candidate has any criminal background then it can reject its application



Course Contents

Course Duration - 200 Hrs

Network Essential

- 01** Explain the concept of network communication.
- 02** Explain the basic requirements for getting online.
- 03** Create a simulated network using Cisco Packet Tracer.
- 04** Build a simple home network.
- 05** Explain the importance of standards and protocols in network communications.
- 06** Explain how communication occurs on Ethernet networks.
- 07** Create a fully connected LAN.
- 08** Explain the features of an IP address.
- 09** Explain the DHCP address assignment process.
- 10** Firewall And IDS ,IPS

Course Contents

Course Duration - 200 Hrs

Linux

- 01 Linux Fundamentals
- 02 Linux Background
- 03 Install Linux
- 04 Basic Commands
- 05 Linux File System
- 06 Command Flag or Switch
- 07 Permissions
- 08 General Useful Utilities
- 09 Maintain your system automation
- 10 System logs

Course Contents

Course Duration - 200 Hrs

Programming (BASH)

01 Introduction

02 What is bash?

03 First Bash Scripting

04 Variable

05 Parameters

06 Arrays

07 Conditions

Course Contents

Course Duration - 200 Hrs

Ethical Hacking

- 01 Introduction to Ethical Hacking
- 02 Footprinting and Reconnaissance
- 03 Scanning Networks
- 04 Enumeration
- 05 Vulnerability Analysis
- 06 System Hacking
- 07 Malware Threats
- 08 Sniffing
- 09 Social Engineering
- 10 Denial-of-Service

Course Contents

Course Duration - 200 Hrs

Ethical Hacking

- 11 Session Hijacking
- 12 Evading IDS, Firewalls, and Honeypots
- 13 Hacking Web Servers
- 14 Hacking Web Applications
- 15 SQL Injection
- 16 Hacking Wireless Networks
- 17 Hacking Mobile Platforms
- 18 IoT and OT Hacking
- 19 Cloud Computing
- 20 Cryptography

Course Contents

Course Duration - 200 Hrs

BLUE TEAMING & CYBER SOC

- 01 Introduction to SIEM & SOC
- 02 NextGen SOC
- 03 SOC & SIEM Architecture and Deployment
- 04 Logs, Events Collection and Event Correlation
- 05 Incident Management & Understanding Logs
- 06 Incident Response Methodology
- 07 Building SOC
- 08 Developing use cases and associated correlation rules
- 09 Detection and Prevention

Course Contents

Course Duration - 200 Hrs

WEB AND ANDROID APPLICATION SECURITY

- Web Application Penetration Testing
- Android Penetration Testing

Active Directory Penetration Testing

COURSE FEE AND REGISTRATION

Paid in Installment

₹80,000 INR

Paid one time

₹ 60.000 INR



Duration of the Course

1 Year or 200 Hour training



How to Register

Call at +91-9091192906

or mail us at

support@cybera1.com



Payments Mode

Credit/Debit Card, Bank Transfer or Cheque



EMI

no cost EMI

HACK YOUR CAREER WITH



SECURE THE DIGITAL

www.cybera1.com

support@cybera1.com

+91 9091192906

All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or DE compilation is strictly prohibited without the prior written consent of Cyber A1.

No part of this document may be reproduced in any form or by any means without the prior written authorization of Cyber A1. While every precaution has been taken in the preparation of this document, Cyber A1 assumes no responsibility for errors or omissions.