# CCW - Program Description Document

| | |
|---|---|
| **Course Name** | **Certified Cyber Warrior** |
| **Course Name as on Certificate** | **Certified Cyber Warrior v3.0** |
| **Certificate Type** | Certificate of Completion by IIT-MADRAS |
| **Certificate Issued by** | IIT MADRAS |
| **Course Objectives** | It is comprehensive course to learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that one can directly apply when they get back to work. As Certified Cyber Warrior, the participant will learn tips and tricks from the best of the experts from a mix of industry & academia, so that they can win the battle against the wide range of cyber adversaries that want to harm the enterprises' IT environment. |
| **Eligibility** | • For Indian Participants - Graduates or Diploma Holders (10+2+3) from a recognized university (UGC/AICTE/DEC/AIU/State Government) in any discipline.<br>• For International Participants - Graduation or equivalent degree from any recognized University or Institution in their respective country. |
| **Pre Requisites** | Basic understanding of technology, networks and security, while not mandatory, will be an added advantage. |
| **Target Segment** | Working professionals and fresh graduate students aspiring to have a career in Cyber Security can enroll for this programme. Anyone who works in security, is interested in security, or has to understand security should take this course, including:<br>• Security professionals who want to fill the gaps in their understanding of technical information security.<br>• Managers who want to understand information security beyond simple terminology and concepts.<br>• Operations personnel who do not have security as their primary job function but need an understanding of security to be effective.<br>• IT engineers and supervisors who need to know how to build a defensible network against attacks.<br>• Administrators responsible for building and maintaining systems that are being targeted by attackers.<br>• Forensic analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs.<br>• Anyone new to information security with some background in information systems and networking. |
| **Course Content** | **MODULE 1 – INTRODUCTION SESSION**<br><br>Details: This session explain about the need of the program, how it is been design and how it is expected to drive as a certification program in coordination with IIT Madras<br><br>Technical Information: Introduction about IIT Madras, FISST and about students<br><br>**MODULE 2 – INTRODUCTION & OVERVIEW TO CYBER SECURITY**<br><br>Details: This session provide an overview of Cyber Security, its domains, its necessity in the modern digital era and mindset to drive this program until the end<br><br>Technical Information:<br>• Introduction to Cyber Security,<br>• Introduction to Information Security,<br>• Overview of Cyber Security,<br>• Domain Information of Cyber Security,<br>• Types of Security,<br>• Branches of Cyber Security |

**MODULE 3 – DIGITAL FORENSICS - AN OVERVIEW**

Details: This session is been split into two as theory and practical. The theoretical part of this session shall explain about the concepts of digital forensics and how an investigation is performed after a breach. The practical session drives you to the world of forensics with state-of-the-art forensics tool handling extended to the bootcamp session

Technical Information:

- Digital Forensics concepts,
- Digital forensic methods,
- Digital forensic tools,
- Sample data for analysis,
- Digital forensic process and identification

Tools:

- Autopsy,
- FTK imager,
- CAINE,
- Bulk Extractor,
- DEFT,
- Xplico,
- Plainsight,
- X-Way Forensics,
- EnCase

**MODULE 4 – IT & CYBER LAW - AN OVERVIEW**

Details: This session explain about the way how Cyber Law is designed for the hacking era with practices and solutions to follow while using internet and internet related technologies

Technical Information:

- Cyber law concepts,
- IT law sections,
- Do's and Don’ts in cyber environment,
- Cyber etiquette,
- How to perform lawful activity

**MODULE 5 – CRYPTOGRAPHY - AN OVERVIEW**

Details: This session is been split into two as theory and practical. The theoretical part of this session shall explain about the concepts of cryptography used in passwords and other methodological ways. The practical session helps to understand basic tools of cryptography on how to design tough password and safeguard your digital assets

Technical Information:

- Cryptography basic concepts,
- Types of cryptography,
- Message authentication,
- Encryptions algorithms,
- Hashing algorithms,
- Steganography,
- Digital certificates

Tools:

- hash calc,
- Quickstego,
- Disk crypto,
- AES Crypt,
- Our secret

**MODULE 6 – PHYSICAL SECURITY AND IMPORTANCE**

Details: This session provide an understanding and need for strong Physical security and how assets containing digital data to be stored a safe environment. Some of the interesting way of physical hacking that help hackers to steal invaluable data shall be handled during the bootcamp session

Technical Information:

- Physical security introduction
- Perimeter security
- Cyber physical security
- Command and control system
- Overview of IoT devices and security concerns

Tools:

- Rubber Ducky
- WiFi Pineapple
- Aircheck
- LAN Turtle
- HackRF One
- Lockpicks
- Keylogger

**MODULE 7 – Governance & Compliance - An Overview**

Details: This session explain about the Cyber Security governance and compliance requirements required to be followed by organisations, governments along with details of modern standards and policies

Technical Information:

- Cyber Security Governance
- Cyber Security Compliance
- Best practice standards
- Compliance for corporate

**MODULE 8 – Cyber Risk and Cyber Insurance Best Practices**

Details: This session talks about Cyber risk and how to mitigate it using Cyber Insurance and best practices in keeping your data and process in the digital environment

Technical Information:

- Cyber Risk assessment
- Risk management
- Risk matrix and methodology
- Cyber insurance framework
- How to achieve Cyber Insurance for an organisation

**MODULE 9 – Network Security - The Corporate Culture**

Details: This session explains about the latest requirements of Networks Security to be followed by every organisation and performing Vulnerability Assessment and Penetration Testing with state-of-the-art tools extended to the bootcamp for real world incident access

Technical Information:

- Network Security basics for organization
- Penetration testing methodology
- Ports and services of modern networks
- Types of hacks using networking
- Network devices
- Linux commands and techniques

Tools:

- Log analyzer
- Wireshark
- Nessus

- Aircrack
- Snort
- John the Ripper
- tcpdump

**MODULE 10 – Offensive Security - Hackers Mind**

Details: This session explains about the mindset of a hacker and how the hacker think, plan, strategize, work with modern concepts, techniques and tools to hack into a network towards stealing information from individuals, organisations and government.

Technical Information:
- Hacking concepts
- Hacking types
- Hacking methodology
- Hacking techniques and tools

Tools:
- Metasploit
- Acunetix
- App Scan
- Cain & Abel
- Password cracker
- Ettercap
- HPWebinspect
- L0phcrack

**MODULE 11 – Mobile Security - Common Man Vulnerability**

Details: This session explains about the vulnerabilities that exist in today's mobile operating systems and how to understand, identify and eliminiate those vulnerabilities with available tools and techniques extended to boot camp sessions

Technical Information:
- Mobile Security basics
- Operating System level vulnerability
- Mobile Vulnerability Assessment basics

Tools:
- Zed attack proxy
- Kiuwan
- Android debugger

**MODULE 12 – Cloud Security - The Global Problem**

Details: This session talks about the risks and issues of migrating to cloud, managing cloud environment and various vulnerabilities present in cloud environments

Technical Information:
- Cloud Security basics
- Cloud Control Matrix
- OWASP top 10 Cloud vulnerability
- Auditing Cloud environment

**MODULE 13 – Dark web and Deep web - Does it really exist**

Details: This session unveils about how dark web and deep web is helping hackers in gathering data about an individual, an organisation and governments to penetrate into an environment with smart commands and techniques

Technical Information:
- Deep web and Dark web overview and basics
- ToR browser and its utility
- The black market and its data
- Ransomware

Tools:

- ToR browser
- Online tools
- Commands and installations

**MODULE 14 – Risk Management - It is very important?**

Details: This session deals with the importance of risk management and how to identify an organisation's risk and ascertain the mitigation methodology from a third eye angle and support with mitigation steps

Technical Information:

- Risk management basics
- Risk management concepts
- Risk matrix methodology
- Risk identification and risk treatment

**MODULE 15 – Security Operation Centre - Need of the hour**

Details: This session talks about the need for Security Operation Centre (SOC) for an organisation and how it will help to proactively identity the risk that may be posted by malicious threats.

Technical Information:

- What is SOC
- SOC concepts
- SOC methodology
- SOC identification and how to use

Tools:

- SIEM
- IDS
- Configurations and live lookup

**MODULE 16 – Application Security - Every organisation's Real Problem**

Details: This session talks about top vulnerabilities persistent in applications and how to identify using the command and tools available with state of the art incident based real world lab providing you the concept oriented explanation

Technical Information:

- Application security concepts
- Web Vulnerability Assessment and Penetration Testing
- Identifying OWASP top 10 vulnerabilities

Tools:

- Acunetix
- Netsparker
- GHDB, etc.

**MODULE 17 – Cyber Security Design and Maintaining Resilience & Best Practices**

Details: This session explain about modern cyber security design and how to maintain the environment with best practices, standards, procedures and methods

Technical Information:

- Cyber Security Network and best practice design
- Cyber security resilience
- Best Practices of Cyber security in organisations

**MODULE 18 – Malware Analysis - An Overview**

Details: This session talks about the latest malware and how to detect, analyse, disect a malware identified in systems using tools and techniques within specific timeframe and support further elimination

Technical Information:

- Basics of Malware Analysis
- Malware identification
- Malware analysis
- Reverse Engineering concepts

Tools:

- APK Tool
- Ollydbg
- Malware Analyzer
- REMnux Malware Analysis

**MODULE 19 – 20 Critical Security components - Discussion**

Details: This session explain about the 20 critical security controls and its components designed for professional everyday utility and a discussion based on other concepts handled

Technical Information:

- 20 Critical Security Components

**MODULE 20 – Incident Management – an overview**

Details: This session talks about the steps and procedures of an incident management process and what to follow post an incident/breach in a detailed manner to prepare for worst time

Technical Information:

- Incident management as process
- Incident management concept and steps
- Performing incident analysis

**Boot Camp – 30 Hours – 3 Days – 52 Tools**

- The boot camp comprises of 30 packed hours exhibiting state-of-the-art cyber security tools to try and practice is real world Cyber Environment created for learning purpose.
- The boot camp has teams to practice red teaming, blue teaming and white teaming exercise to plan, execute, protect, detect and support features.
- All the following tools will be used for understanding real world cyber threats and prepare on how to mitigate it.

| | | | |
|---|---|---|---|
| Autopsy | Our secret | John the Ripper | ToR browser |
| FTK imager | Rubber Ducky | tcpdump | Online tools |
| CAINE | WiFi Pineapple | Metasploit | Commands |
| Bulk Extractor | Aircheck | Acunetix | SIEM |
| DEFT | LAN Turtle | App Scan | IDS |
| Xplico | HackRF One | Cain & Abel | Configurations and live lookup |
| Plainsight | Lockpicks | Password cracker | Acunetix |
| X-Way Forensics | Keylogger | Ettercap | Netsparker |
| EnCase | Log analyzer | HPWebinspect | GHDB, etc. |
| hash calc | Wireshark | L0phcrack | APK Tool |
| Quickstego | Nessus | Zed attack proxy | Ollydbg |
| Disk crypto | Aircrack | Kiuwan | Malware Analyzer |
| AES Crypt | Snort | Android debugger | REMnux Malware Analysis |

**Pedagogy**

The primary method of instruction will be through LIVE lectures that will be delivered online via internet to participant desktops/laptops or classrooms. The lectures will be delivered by eminent academicians and practicing industry experts. The programme will be primarily taught though a combination of lectures, discussions, exercises and labs. All enrolled students will be provided access to our FISST Whizard Cloud Campus through which students may access other learning aids, reference materials, assessments and assignments as appropriate. Throughout the duration of the course, students will have the flexibility to reach out to the Professors, real time during the class or offline via the FISST Whizard Cloud Campus to raise questions and clear their doubts.

| | |
|---|---|
| **Assessment** | There are periodic evaluation components built in as a part of the program. These maybe in the form of a quiz, assignment or other objective/subjective assessments as relevant and applicable to the program. A minimum of 70% attendance to the LIVE lectures and participation in the 3 Day on-campus boot-camp, is a prerequisite for the successful completion of this program. Participants who satisfy the attendance criteria and successfully clear the evaluation components will be awarded a certificate of completion. |
| **Programme Faculty** | **Programme Director:** Mr. Mohan Ram C from FISST<br><br>Mohan has nearly 33 years of professional experience after an M.Tech from IIT-Roorkee, as IT leader specializing in Cyber Security and related physical surveillance for critical infrastructure including refinery, nuclear power plants and mission critical IT infrastructure etc. Mohan is currently pioneering Cyber Education space in India to create awareness and fill the gap in skills to tackle potential damages due to cybercrimes in partnership with leading academic institutions across India.<br><br>**Professor Kama Koti, IIT – Madras, Program Advisor and Mentor**<br>**Lead Academic Faculty Members:**<br>**Professor Noor Mahammad SK – IIIT D&M – Kancheepuram**<br>**Professor Masilamani V – IIIT D&M – Kancheepuram**<br>**Professor Tricha Anjali from IIIT-B (LMS)**<br>**Professor Ashish Choudhury from IIIT-B (LMS)**<br>**Professor Harish Ramani – Visiting Faculty @IIIT-B**<br>**Professor Mohan Ram – Adjunct Faculty @ IIIT-B**<br>**And other industry experts from a pool of consultants / experts.** |
| **Duration** | Live delivery (Virtual) by instructors with hands-on demo – 56 hours (14 weeks x 4 hrs per week)<br>LMS (Self-learning) – 9 hours (mainly Cryptography and Maths behind it & Networking fundamentals)<br>Project work (self-learning by web research) – 10 hours (to be submitted before campus visit)<br>Tools and Hands-on exercises – 15 hours (students try the tools demonstrated themselves & report)<br>Campus – Hands-on / Boot camp style – 30 hours (@ IIT-Madras campus – followed by Graduation ceremony)<br>TOTAL = 120 Hours |
| **Class Schedule** | Twice a week on on Saturdays & Sundays from 10.00 a.m. to 12.00 p.m. |
| **Programme Highlights/USPs** | **Course Benefits to Participants**<br><br>Build a lucrative and futuristic career in the field of Cyber Security. According to NASSCOM, the estimated demand for security workforce to rise globally to six million by 2019, up from 4 million in 2015, with projected shortfall of 1.5 million (https://www.gadgetsnow.com/tech-news/Cybersecurity-to-create-1million-jobs-Nasscom/articleshow/51884133.cms)<br><br>**About CCW so far** – FISST has conducted awareness cum certification of working professionals in India and Dubai & formal electives subject to students @ IIIT-B to the **tune of 2240+ participants**. The number is growing rapidly with more corporate and colleges opting to this course.<br><br>Participants for certification programmes include IT professionals from leading banks like **SBI, Vijaya Bank, Canara Bank, Axis Bank, IDFC Bank, HDFC Bank, Deutsche Bank, Royal Bank of Scotland (RBS), Manapuram Gold Loan** etc. and several leading IT consulting and services organisations like **Deloitte, HCL, Infosys, Wipro, Cognizant, TCS** etc.<br><br>Also, top notch professionals big corporates like **Oracle, Microsoft, Shell, Cisco, Honeywell, Schneider** etc. and PSU like **IRCTC, Railtel, NLC India, Dredging Corporation** etc. have attended the courses.<br><br>On successful completion of the programme, you will be able to |

<table>
<tr><td></td><td colspan="3">

- Apply what you learnt directly to your job when you get back to work.
- Design and build a network architecture using VLANs, NAC, and 802.1x based on advanced persistent threat indicators of compromise.
- Run Windows command line tools to analyze the system looking for high-risk items.
- Run Linux command line tools (ps, ls, netstat, etc.) and basic scripting to automate the running of programs to perform continuous monitoring of various tools.
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems.
- Create an effective policy that can be enforced within an organization and design a checklist to validate security and create metrics to tie into training and awareness.
- Identify visible weaknesses of a system using various tools (mostly free or minimal subscription – without large investment) and, once vulnerabilities are discovered, cover ways to configure the system to be more secure.
- Build a network visibility map that can be used for hardening of a network - validating the attack surface and covering ways to reduce that surface by hardening and patching.
- Sniff open protocols like telnet and ftp and determine the content, passwords, and vulnerabilities using WireShark and many more relevant tools.

Other benefits to participants include

- Opportunity to earn a Certificate from IIT Madras.
- Lectures imparted by eminent academicians and practicing industry experts.
- Get exposure to contemporary and sought after areas like IOT device security, Blockchain, Cryptocurrencies etc.
- Gain comprehensive understanding of applicable Cyber Laws.
- 3 days On Campus "Bootcamp" style workshop module covering hands on exposure to lab sessions on Cyber Threats and Cryptography etc.
- Certification ceremony on campus at the completion of the programme
- Fully Online Course with LIVE online interactive lectures that provides a "real" classroom experience in a "virtual" environment. No isolated learning experience.
- Seamless technology that can transmit lecture videos effectively at home broadband connection of 512 kbps.

- User friendly and easy to use technology interface. No expensive and time consuming software/hardware installations required at your end.
- Virtual classrooms that allow for active interactions with other fellow students and faculty.
- Convenient weekend schedules
- In the event that students miss attending the LIVE lecture on the Virtual Classroom for some reason, students will be granted access to the recorded sessions for a specified number of days/times.
- FISST Whizard Cloud Campus – Students on our virtual social learning platform are provided access to course presentations, projects, case studies, assignments and other reference materials as applicable for specified courses. Students can raise questions and doubts either real time during the live class or offline through the Cloud Campus.
- Learn from Anywhere – No need to travel to an institute or training center. Learning continues even if you are traveling or not available at any specific location. You may also learn from the comfort of your home.

</td></tr>
<tr><td rowspan="2">Total Fees</td><td></td><td>Total Fees (Rs.)</td><td></td></tr>
<tr><td>Total Programme Fee</td><td>INR 120,000 + 18% GST / USD 2500 for overseas enrollment</td><td></td></tr>
</table>