CCE - CNS - Program Description Document

Course Name	**Certified Cyber Engineer – Computer & Network Security**
Course Name as on Certificate	**Certified Cyber Engineer – Computer & Network Security (CCE-CNS)**
Certificate Type	Certificate of Completion by IIT-MADRAS & NASSCOM – (**NASSCOM QP - REFERENCE ID:** SSC/Q0917)
Certificate Issued by	IIT MADRAS
Course Objectives	It is a course to learn the most effective steps to prevent attacks and detect adversaries with actionable techniques for Computer and Network, that one can directly apply when they get to work. As Certified Cyber Engineer, 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. CCE-CNS along with two more specialization viz. Certified Cyber Engineer – Software Engineering and Secure Coding (SESC) Certified Cyber Engineer – Cloud Security & Devops (CS&D) Will make the students to be ready for a career in Infosec domain, where there is a huge shortfall of trainined manpower.
Eligibility	• Must be a bonafide student of any college and must have completed Year 1 of any course. • For Indian Participants – Pursuing a Graduate degree programme, after 1st year or finished Diploma Holders (10+2+3) from a recognized university (UGC/AICTE/DEC/AIU/State Government) in any discipline. • 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	Students in the colleges who have finished year 1 in any stream and fresh graduate students aspiring to have a career in Cyber Security can enroll for this programme. Anyone who wish to work in security & is interested in security, or has to understand security should take this course, including: • Information Security / Cyber Security as career • Anyone new to information security with some background in information systems and networking.
Course Content	**Module 1 - Introduction to Computer Network Security:** Introduction, securing the computer networks- hardware/software, forms of protection, security standards; Sources of vulnerabilities and its assessment (4 hrs) **Module 2 - Security challenges, Assessment, Analysis and Assurance:** Sources of security threats, threat motives, management and correlation and security threat awareness; System security policy, Building a security policy, security requirement specification, Threat Identification and analysis, Vulnerability identification and assessment and security monitoring and auditing; Disaster Management, Resources for disaster planning and recovery (6hrs). **Module 3 - Access Control, Authorization and Authentication:** Access - Rights, Control systems; authorization- mechanisms, types, principles, and granularity; Authentication - factors and effectiveness, elements, types, methods and policy (4 hrs). **Module 4 - Cryptography:** Symmetric Encryption, public key encryption, enhancing security and Key management; Public key Infrastructure, hash function and digital signatures (4 hrs).

	Module 5 - System Intrusion Detection and Prevention: Intrusion detection mechanism, systems, types; Response to system intrusion, challenges to intrusion detection systems and implementations; Intrusion prevention systems (4 hrs). **Module 6 - Computer and Network Forensics:** Computer forensics, network forensic and forensics tools (2 hrs). **Module 7 - Firewall, Virus and Content Filtering:** Firewall- types, configuration, implementations and limitations; Scanning, Filtering and blocking; Virus filtering and content filtering (4 hrs). Computer Network Security Protocols: Application Level Security, Security in the Transport Layer, Network layer, Link layer and over LANs (6 hrs). **Module 8 - Security in Wireless Network and Devices:** WLAN security concerns and best practices for WI- FI security (4 hrs). **Module 9 - Security in sensor networks:** Challenges, vulnerabilities and attacks, security mechanisms and best practices for sensors (4 hrs).
Pedagogy	The primary method of instruction for theory will be through recorded sessions and reading materials. Hands-on will be LIVE demonstration 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 completion of assignments / assessments, 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 Advisor and Mentor** **Professor Kamakoti, IIT – Madras** **Department of Computer Science and Engineering,** **Member, National Security Advisory Board, Government of India.** **Programme Director:** **Mr. Mohan Ram C, MD, FISST** **Programme Coordinator:** **Professor K. Mangala Sunder, IIT - Madras** **Head, Digital Skills Academy** **Lead Academic Faculty Members:** **Professor Noor Mahammad SK – IIIT D&M – Kancheepuram** **Professor Harish Ramani – Visiting Faculty @IIIT-B & Sri City** **Professor Mohan Ram C – Adjunct Faculty @ IIIT-B & Sri City**
Duration	LMS (Self-learning from Video and reading materials – to be completed before hands-on – every week) – 20 hours (mainly theory on Computer & Networking fundamentals) Hands-on - Live delivery by instructors with hands-on demo – 20 hours (4 weeks x 5 hrs per week)

<table>
<tr><td></td><td colspan="2">Tools and Hands-on exercises – 15 hours (students try the tools demonstrated themselves & report)
<b>TOTAL = 55 Hours (40 hours of instruction / teaching)</b></td></tr>
<tr><td><b>Class Schedule</b></td><td colspan="2">Week days – between 6 and 8.30 PM – 2 days per week for 4 weeks</td></tr>
<tr><td><b>Programme Highlights/USPs</b></td><td colspan="2"><b>Course Benefits to Participants</b>
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 next year, 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)
<b>About Cyber Security trainings so far</b> – FISST has conducted awareness cum certification of working professionals in India and Dubai & formal electives subject to students @ IIIT-B to the <b><u>tune of 2320+ participants</u></b>. The number is growing rapidly with more corporate and colleges opting to this course. Participants for certification programmes include IT professionals from leading banks like <b>SBI, Vijaya Bank, Canara Bank, Axis Bank, IDFC Bank, HDFC Bank, Deutsche Bank, Royal Bank of Scotland (RBS), Manapuram Gold Loan</b> etc. and several leading IT consulting and services organisations like <b>Deloitte, HCL, Infosys, Wipro, Cognizant, TCS</b> etc. Also, top notch professionals big corporates like <b>Oracle, Microsoft, Shell, Cisco, Honeywell, Schneider</b> etc. and PSU like <b>IRCTC, Railtel, NLC India, Dredging Corporation</b> etc. have attended the courses. Also, officers from various Govt. departments like <b>DRDO, MHA, DRDO and CEG – Govt. of Karnataka</b> have participated<b>.</b>
On successful completion of the programme, you will be able to
• Apply what you learnt directly to your job when you get 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.
• 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.
Other benefits to participants include
• Opportunity to earn a Certificate from IIT Madras along with NASSCOM
• Lectures imparted by eminent academicians and practicing industry experts.
• Convenient schedules
• 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"><b>Total Fees</b></td><td></td><td><b>Total Fees (Rs.)</b></td></tr>
<tr><td>Total Programme Fee</td><td><b>INR 8400 + 18% GST (Total - Rs. 9912/-)</b>
USD 250 for overseas enrollment</td></tr>
</table>