

QUOTATION

Sir/Madam,

Sub: Quotation for **Center for Futuristic Learning – Cyber Security** Training Program

Greetings from SIX PHRASE – Edutech Private Limited

In line with the discussion we had with you we have here with detailed the program details along with the cost for conducting the **Center for Futuristic Learning – Cyber Security** Training Program. Please find below the program details.

Program Duration:	I to IV Year Integrated Mode - 72 Hours per Semester (1 to 8 Semesters) III Year Bootcamp Mode – 300 Hours
Target Audience:	BE Students
Program Type:	Center for Futuristic Learning – Cyber Security
Value Additions:	<ul style="list-style-type: none"> ✓ Online Hands On Training Sessions with Technology Experts from Corporate and from IITs. (30% of Course Duration). ✓ 3 Interactive Webinar sessions per semester with CEOs and Technology Heads from Corporate. ✓ Real World Projects certified by PWC. ✓ Cloud Labs Tools & Softwares
Placement & Internship Assistance:	<ul style="list-style-type: none"> ✓ Access to 30+ Product Companies: Marquee Companies: >20 LPA; Super Dream Companies: 10-20 LPA; Dream Companies: 5-10 LPA ✓ Abroad Internships & Placements ✓ Study Abroad Programs with Placements

Syllabus:

Cyber Security - Curriculum

Course	Modules
Module 1 - Operating Systems	<ul style="list-style-type: none"> - Introduction to Linux - Virtual Environment Setup - Command line operations - Linux file systems - Filters - Kali Linux - Kali Linux Tools - Cybersecurity Tool Disciplines - Advanced Packet Tool - APT Key Management Utility - Management tools - Domain of protection - Access Matrix - Access control - Language based protection - Multics - Firewalls - Security in operating systems
Module 2 - Computer Networking	<ul style="list-style-type: none"> - Types of Network - Network Topologies - Cabling - Ethernet - IP Address - MAC - Address Resolution Protocol - Subnetting - The OSI Model - Internet Models - TCP - UDP - Internet Protocols: FTP, HTTP, HTTPS, DHCP - Network Security Technologies
Module 3 - Cryptography	<ul style="list-style-type: none"> - What is Cryptography? - Encryption and Decryption - Cryptanalysis - Symmetric Ciphers - Classic Encryption Techniques - DES and AES - Block Cipher - Asymmetric Ciphers - Number Theory - RSA algorithm - Diffie-Hellman Key exchange - Cryptosystem - Pseudo Random Number Generators (PRNG)

	<ul style="list-style-type: none"> - Introduction to Blockchain Technology - Cryptography in Blockchain - Blockchain Security Fundamentals - Threats and Attacks in Blockchain
<p>Module 4 - Infrastructure Security</p>	<ul style="list-style-type: none"> - Security Attacks - Services and Mechanism - Models for Network Security - Kerberos - Remote Access Security - VPN, SSH, IPSEC - Wireless Networks - Wireless Vulnerabilities - Network Monitoring - Security Topologies - VLANS - Network- and Host-Based IDS - Honey pots and Honeynets - Incident Response
<p>Module 5 - Application Security</p>	<ul style="list-style-type: none"> - Input Validation - Attack Surface Reduction - Authentication - Two Factor and Three Factor Authentication - Web Application Authentication - Authorization - Custom Authorization Mechanism - Client Side Attacks - Session Management - SSL and HTTPS - Introduction to Web Security - SSL & HTTPS - Insecure Direct Object Reference - Directory Traversal - Mobile security - Secure Development Methodologies
<p>Module 6 - Information Security and Ethical Hacking</p>	<ul style="list-style-type: none"> - Information Security Overview - Information Security Threats and Attack Vectors - Hacking Concepts - Information Security Controls - Types of Security Policies - Physical Security - Incident Management - Vulnerability Assessment - Information Security Laws and Standards - Anonymity - Footprinting Concepts - Maltego Tool Overview - Recon-ng Overview - Overview of Network Scanning

	<ul style="list-style-type: none"> - Scanning Methodology - Enumeration - Techniques for Enumeration - Vulnerability Assessment
Module 7 - Wireless and Device Hacking	<ul style="list-style-type: none"> - System Hacking Methodologies - Rainbow Table - Wireless Encryption - Wireless Threats - Wireless Hacking Methodology - Bluetooth Hacking - Wireless Security Tools - Hacking Wi-Fi - DDOS - Sniffing - MAC Attacks - ARP Poisoning - Spoofing Attack - DNS Poisoning - What is IoT? - IoT Architecture - IoT Attacks and threats
Module 8 - Penetration Testing	<ul style="list-style-type: none"> - Web server Attacks - Attack Methodology - DDOS - Web App Hacking Methodology - Countermeasures - MITM - Bruteforce - OWASP Top Vulnerabilities - Introduction to SQL injection - SQL Injection Concepts - SQL Injection Methodology - Evasion Techniques - Blind SQL Injection - Validating and Escaping Inputs - Session Hijacking - Social Engineering Concepts - Social Engineering Techniques - Identity Theft

<p>Module 9 - Generative AI in Cyber Security</p>	<ul style="list-style-type: none"> - Introduction to <i>Generative AI in Cyber Security</i> - Role of <i>Generative AI</i> in cybersecurity and ethical hacking - Applications of <i>Generative AI</i> in security tasks - Fundamentals of <i>Generative AI</i> - Understanding <i>Generative Adversarial Networks (GANs)</i> - <i>Generating Malicious and Benign Content</i> - Using <i>GANs</i> to generate malware samples - <i>Generating benign content for data augmentation</i> - <i>Generative AI for Evasion</i> - <i>Phishing Campaign Generation</i> - <i>Limitations and Ethical Considerations</i>
<p>Module 10 - Development and Scripting in Cybersecurity</p>	<ul style="list-style-type: none"> - Introduction to <i>Scripting and Automation in Cybersecurity</i> - Benefits of automation in security tasks - Programming Fundamentals for Scripting - Variables, data types, operators - Control structures (if statements, loops) - Functions and modules - Scripting with Python - Basics of Python programming - Automating tasks with Python scripts - Scripting with Bash - Basics of Bash scripting - Creating Bash scripts for automation - Using Nmap scripting engine (NSE) - Vulnerability Assessment Automation - Automating vulnerability scans - Automating tasks during security incidents
<p>Module 11 - Cloud Security</p>	<ul style="list-style-type: none"> - Importance of cloud security - Cloud Deployment Models - Cloud Security Risks and Vulnerabilities - Misconfigurations - inadequate access controls - Securing Cloud Infrastructure - Identity and access management - Encryption and key management - Network security in the cloud - Third-party security tools - Threat Detection - Incident response planning for cloud breaches - Cloud Security Assessments - Implementing strong authentication - Data classification and encryption - Cloud Compliance and Regulations

<p>Module 12 - Digital Forensics</p>	<ul style="list-style-type: none"> - Introduction to Digital Forensics - Objective of Digital Forensics - Media Devices - The Computer Investigation Process - Recovering Deleted Files and Deleted Partitions - Data Acquisition and Duplication - Boot Processes - Investigating Email Crimes and Violations - Tracing Email - Introduction to Malware Analysis - Malware Characteristics and Behavior - Malware Delivery and Infection Methods - Static and Dynamic Malware Analysis - Malware Reverse Engineering - Memory Analysis for Malware
<p>Capstone Project</p>	<ul style="list-style-type: none"> - Vulnerability assessment and exploitation - Network security - Web application security - Ethical Hacking - Social engineering - Malware analysis - Forensics - Incident response