DEVLUSTRO
Empowering Talent ▲ Enabling Careers

QUOTATION

Sir/Madam,

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

Greetings from DEVLUSTRO – 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:	✓ 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:	✓ 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	- 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	- 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	- 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 - Cyrptosystem - Pseudo Random Number Generators (PRNG) - Introduction to Blockchain Technology - Cryptography in Blockchain

	- Blockchain Security Fundamentals - Threats and Attacks in Blockchain
Module 4 - Infrastructure Security	- 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 - Honeypots and Honeynets - Incident Response
Module 5 - Application Security	- 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
Module 6 - Information Security and Ethical Hacking	- 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 - Scanning Methodology - Enumeration - Techniques for Enumeration - Vulnerability Assessment

Module 7 – Wireless and Device Hacking	- 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	- 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
Module 9 - Generative AI in Cyber Security	- Introduction to Generative AI in Cyber Security - Role of Generative AI in cybersecurity and ethical hacking - Applications of Generative AI in security tasks - Fundamentals of Generative AI - Understanding Generative Adversarial Networks (GANs) - Generating Malicious and Benign Content - Using GANs to generate malware samples - Generating benign content for data augmentation - Generative AI for Evasion - Phishing Campaign Generation - Limitations and Ethical Considerations
Module 10 - Development and Scripting in Cybersecurity	- Introduction to Scripting and Automation in Cybersecurity - 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
Module 11 - Cloud Security	- 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

Module 12 - Digital Forensics	- 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
Capstone Project	- Vulnerability assessment and exploitation - Network security - Web application security - Ethical Hacking - Social engineering - Malware analysis - Forensics - Incident response