Kelly Technologies

CYBER SECURITY

CYBER SECURITY EXPERT PROGRAM

EXCEL IN YOUR CAREER WITH OUR CYBER SECURITY SOC MASTER PROGRAM

What is Cyber Security?

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from unauthorized digital access and malicious attacks. It's also known as information technology security or electronic information security.

Cyber security refers to every aspect of protecting an organization and its employees and assets against cyber threats. As cyber attacks become more common and sophisticated and corporate networks grow more complex, a variety of cyber security solutions are required to mitigate corporate cyber risk.

Why is Cyber Security important?

Business continuity is the single and main reason why cyber security is important.

At an individual level, a cyber security attack can result in everything from identity theft to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning. Imagine what can happen over corporate level.

Why do we need this course?

Here are the 10 top reasons why you should consider learning cyber security:

High Demand

Cyber security experts are in high demand. As mentioned earlier, there are about 35 lakh cyber security job openings globally, making it an exciting career opportunity.

Job Opportunities Across Industries

With cyber security skills, you can work across many industries, and this includes the government, banking, business, education, and healthcare sectors.

Kelly Technologies

CYBER SECURITY

Great Salary Benefits

Cyber security offers fantastic earning opportunities. According to Glassdoor, the average salary of a fresher is 5-8 lakhs and highest annual salary for a cyber security engineer is 1.3 crores and expected to grow more in future.

Working with Top Organizations

Many big companies are on the lookout for cyber security experts. Mastering the required skill set can make you qualified to work with organizations such as Google, Meta, Apple, and Microsoft.

Empowering Businesses and Employees

Learning cyber security can provide knowledge and skills to secure the organization's data and reduce potential cyber attack threats.

Reduced Cost

Investing in cyber security courses can help you learn ways to detect and contain data breaches and reduce the cost of damages.

Reducing Response Time

Human error is one of the main causes of cyber breaches. By learning cyber security, you can understand and identify potential threats and contain them on time.

Retain Customer Trust

Learning cyber security will strengthen business security and protect customers' data. A strong cyber security system will promote trust and retain customers.

Staying Updated with New Threats

As cyber attacks are growing more and more sophisticated, constantly learning and sharpening your skills in the field has become paramount.

Learn Cyber Security Any Time

Whether you are a beginner or changing your field, cyber security can provide lucrative opportunities to advance your career.

Different types of Cyber Security roles:

Vulnerability Assessment and Patch Management – Qualys and Rapid7

Kelly Technologies

CYBER SECURITY

Penetration Testing – Kali Linux, Metasploit, Burp Suite, Nessus, Wireshark, Nmap Etc

SOC (MSSP) – Firewalls, SIEM, EDR, SOAR, XDR, NDR, Proxy, Email Gateway, UEBA, Threat Intelligence, Threat Hunting.

Cyber Security SOC Master Course

This course will cover the below topics during the training and will provide comprehensive knowledge of how to handle an attack and mitigate it in real time.

Cyber Security & Ethical Hacking

- What is Hacking
- Who is a Hacker
- Skills of a Hacker
- Types of Hackers
- Reasons for Hacking
- Who are at the risk of Hacking attacks
- Effects of Computer Hacking on an organization
- Network Security Challenges
- Elements of Information Security: Confidentiality, Integrity &
- Availability
- The Security, Functionality & Usability Triangle
- What is Ethical Hacking
- Why Ethical Hacking is Necessary
- Scope & Limitations of Ethical Hacking
- What is Penetration Testing
- What is Vulnerability Auditing
- Cyber Security Fundamentals
- Enterprise Architecture and Components
- Information System Governance and Risk Assessment

- Incident Management
- Setting up Virtual machines
- Social Engineering attack
- Case studies on recent frauds
- CIA Traid
- Why you need security
- Send Self destructive messages
- Cyber Security as a career
- Top Cyber Security Certifications
- Top cyber security jobs, Requirements & salary
- Some Famous hacking events

Computer and Network Basics:

- Hacking
- Internet protocol
- Types of IP
- Port
- Protocol
- Protocol service
- Vulnerability
- What are Networks and what is networking
- Network topologies
- How the Networking devices communicate?
- Vulnerable Hacking environments
- Window/Linux commands
- Introduction of kali

CYBER SECURITY

Malware Threats

- What is malware
- Types of malware
- Virus
- What is a virus program
- What are the properties of a virus program
- How does a computer get infected by virus
- Types of virus
- Virus making tools
- How to defend against virus attacks
- Worm
- What is a worm program
- How worms are different from virus
- Trojan
- What is a Trojan horse
- How does a Trojan operate
- Types of Trojans
- Identifying Trojan infections
- How to defend against Trojans
- Spyware
- What is a spyware
- Types of spywares
- How to defend against spyware
- Rootkits
- What is a Rootkit
- Types of Rootkits
- How does Rootkit operate
- How to defend against Rootkits

Kelly Technologies

CYBER SECURITY

Phishing and Social engineering

- What is Phishing
- How Phishing website is hosted
- How victims are tricked to access Phishing websites
- How to differentiate a Phishing webpage from the original webpage
- How to defend against Phishing attacks
- Advance Phishing

DOS : Denial of Service

- What is a DOS attack
- What is a DDOS attack
- Symptoms of a Dos attack DoS attack techniques
- What is a Botnet
- Defending DoS attacks

Session Hijacking

- What is session hijacking.
- Dangers of session hijacking attacks
- Session hijacking techniques
- Cross-Site scripting attack
- Session hijacking tools
- How to defend against session hijacking.
- How to defend against web server hacking

SQL Injection

- What is SQL Injection
- Effects of SQL Injection attacks
- Types of SQL Injection attacks
- SQL Injection detection tools

Kelly Technologies

CYBER SECURITY

Cryptography

- What is Cryptography
- Types of cryptography
- Cipher algorithms
- Public key infrastructure
- What is a Hash
- Cryptography attacks

Security Operations Center (SOC)

Installation of Kali Linux

- Obtaining Kali Linux Installation Media
- System Requirements for Kali Linux Installation
- Preparing for Installation (Backup, Partitioning, etc.)
- Creating a Bootable USB Drive or DVD
- Booting from Installation Media
- Starting the Installation Process
- Choosing Installation Options (Language, Keyboard Layout, etc.)
- Selecting Installation Type (Graphical or Text-Based)
- Partitioning the Disk (Manual or Guided)
- Installing the Base System
- Configuring Network Settings
- Setting Up Users and Passwords
- Post-Installation Setup (Updates, Additional Software, etc.)

Active Directory – Basics

- Introduction to Active Directory
- Purpose and Benefits of Active Directory
- Components of Active Directory
- Domains, Trees, and Forests

- Domain Controllers
- Active Directory Users and Groups

What is CIA Traid

- Confidentiality
- Integrity
- Availability

Identity Theft

- Definition of Identity Theft
- Types of Identity Theft
- Methods Used in Identity Theft
- Impact of Identity Theft
- Common Targets of Identity Theft
- Prevention Measures
- Detection and Response Strategies
- Legal and Regulatory Considerations
- Identity Theft Protection Services
- Emerging Trends in Identity Theft

Risk Assessment

- Definition of Risk Assessment
- Importance and Purpose of Risk Assessment
- Steps in the Risk Assessment Process
- Identification of Assets and Risks
- Threat Identification and Analysis
- Vulnerability Assessment
- Risk Analysis and Evaluation
- Risk Treatment and Mitigation Strategies
- Risk Acceptance and Transference

- Documentation and Reporting

SOC ANALYST

- Introduction to Security Operations Center
- Understanding SMTP / Telnet / SSH / FTP
- Brute force Attacks
- OWASP TOP 10
- Splunk Installation
- Introduction to Splunk
- SOC Process
- Splunk Components
- SOC Roles & Responsibilities
- What is SIEM
- SIEM Architecture
- Architecture of Splunk
- Splunk User Interface
- Basic Searching
- Creating Alerts
- Creating Reports & Dashboards
- Uploading Demo Logs to Splunk & Firewall log analysis
- Understanding Firewall Logs
- IDS Log Analysis
- Understanding Antivirus Logs
- Understanding Windows Event Logs
- SIEM Use cases
- Malware Outbreak analysis
- Incident Handling Stages

Kelly Technologies

CYBER SECURITY

Introduction Threat Hunting

- Threat Hunting – Scanning attack on Web server
- Threat Hunting – Brute Force Attacks
- Email Header Analysis
- Introduction to Symantec Endpoint protection
- Introduction to DLP (Data Loss Prevention)
- Security Incident Response procedure
- Security Incident Response
- Importance and Purpose of Incident Response
- Incident Classification and Prioritization
- Incident Detection and Reporting
- Incident Triage and Initial Assessment
- Activation of Incident Response Team
- Escalation Procedures
- Containment and Mitigation Measures
- Evidence Collection and Preservation
- Investigation and Root Cause Analysis
- Communication and Notification Protocols
- Remediation and Recovery Actions
- Post-Incident Review and Lessons Learned
- Documentation and Reporting Requirements
- Continuous Improvement and Updates to Incident Response Plan.

DIFFERENT TYPES OF ATTACKS AND IR/IM PROCESS

- Malware
- Phishing
- Ransomware
- Social engineering
- Man in the Middle Attacks

- DoS and DDoS
- Injection based attacks
- Broken Access Control
- Cryptographic Failures
- Identification and Authentication Failures

In addition to above we will train how to write policies, create runbooks, playbooks, implementing finetuning and whitelisting.

VULNERABILITY ASSESSMENT and PATCH MANAGEMENT.

A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

How does a vulnerability assessment work?

There are three primary objectives of a vulnerability assessment.

1) Identify vulnerabilities ranging from critical design flaws to simple misconfigurations.
2) Document the vulnerabilities so that developers can easily identify and reproduce the findings.
3) Create guidance to assist developers with remediating the identified vulnerabilities.

Vulnerability testing can take various forms. One method is Dynamic Application Security Testing (DAST). A dynamic analysis testing technique that involves executing an application (most commonly a Web application), DAST is performed specifically to identify security defects by providing inputs or other failure conditions to find defects in real time. Conversely, Static Application Security Testing (SAST) is the analysis of an

application's source code or object code to identify vulnerabilities without running the program.

We utilize Qualys and Rapid7 to perform vulnerability assessments and provide detailed reports, patch Tuesdays, creating advisories etc.

PENETRATION TESTING

Penetration Testing

- What is Penetration Testing
- Types of Penetration Testing
- What is to be tested
- Testing the network devices for misconfiguration
- Testing the servers and hosting applications for misconfiguration
- Testing the servers and hosting applications for vulnerabilities
- Testing wireless networks
- Testing for Denial-of-Service attack

Foot Printing/reconnaissance/Information Gathering

- What is Foot Printing
- Objectives of Foot Printing
- Finding a company's details
- Finding a company's domain name
- Finding a company's Internal URLs
- Finding a company's Public and Restricted URLs
- Finding a company's Server details
- Finding the details of domain registration
- Finding the range of IP Address
- Finding the DNS information
- Finding the services running on the server

- Finding the location of servers
- Traceroute analysis
- Tracking e-mail communications

Scanning

- What is network scanning
- Objectives of network scanning
- Finding the live hosts in a network
- Finding open ports on a server
- Finding the services on a server
- OS fingerprinting
- What is a Vulnerability Scanning
- Vulnerability Scanner tools
- Finding more details about a vulnerability
- What is a proxy server
- How does proxy server work
- Types of proxy servers
- How to find proxy servers
- Why do hackers use proxy servers
- What is a TOR network
- Why hackers prefer to use TOR network

Sniffing and Sniffers

- What is a sniffer
- How sniffer works
- Types of sniffing
- Active sniffing
- Passive Sniffing
- How MAC spoofing works

- MAC Flooding
- How to defend against MAC Spoofing attacks
- How to defend against Sniffers in network

System Hacking

- What is system Hacking
- Goals of System Hacking
- Password Cracking
- Password complexity
- Finding the default passwords of network devices and software's
- Password cracking methods
- Password guessing
- Offline password cracking
- USB password stealers
- Metasploit to hack Systems
- What is a Keylogger
- How to deploy a Keylogger to a remote pc
- How to defend against a Keylogger.

Session Hijacking

- What is session hijacking.
- Dangers of session hijacking attacks
- Session hijacking techniques
- Cross-Site scripting attack
- Session hijacking tools
- How to defend against session hijacking.

Hacking Web Servers & Web Applications

- What is a web server
- Different webserver applications in use

- Why are webservers hacked & its consequences
- Website defacement
- Website password brute forcing
- How to defend against web server hacking

SQL Injection

- What is SQL Injection
- Effects of SQL Injection attacks
- Types of SQL Injection attacks
- SQL Injection detection tools

Wireless Network Hacking

- Types of wireless networks
- Wi-Fi usage statistics
- Finding a Wi-Fi network
- Types of Wi-Fi authentications
- Using a centralized authentication server
- Using local authentication
- Types of Wi-Fi encryption methods
- WEP
- WPA
- How does WEP work
- Weakness of WEP encryption
- How does WPA work
- Hardware and software required to crack Wi-Fi
- networks
- How to crack WEP encryption
- How to crack WPA encryption
- How to defend against Wi-Fi cracking attacks

Kelly Technologies

CYBER SECURITY

Kali Linux

- What is Kali Linux
- How Kali Linux is different from other Linux distributions
- What are the uses of Kali Linux
- Tools for Footprinting, Scanning
- What is Metasploit framework
- Using Metasploit framework to attack Windows machines
- Using Metasploit framework to attack Android mobile devices

Evading Firewalls, IDS & Honeypots

- What is a Firewall
- What are the functions of a Firewall What is an IDS
- How does an IDS work
- IDS tools
- What is a honeypot
- Types of honeypots
- Honeypot tools
- Honeypot detection tools