
ASD ACADEMY

# CYBER SECURITY WITH AI

## 1 YEAR DIPLOMA

**ONLINE/OFFLINE COURSE**

Introducing..

India's Most Advanced Hacking & Coding Academy

POWERED BY

REGISTERED BY

## ONLINE DIPLOMA COURSE

Super 30 Diploma
3 Month Internship
100% Placement Assitance

Super 30 Diploma Fee
50000+Gst =59000/-

Let's win Diploma
without Internship
Without Placement Assitance

Let's Win Diploma Fee
30000+Gst = 35400/-

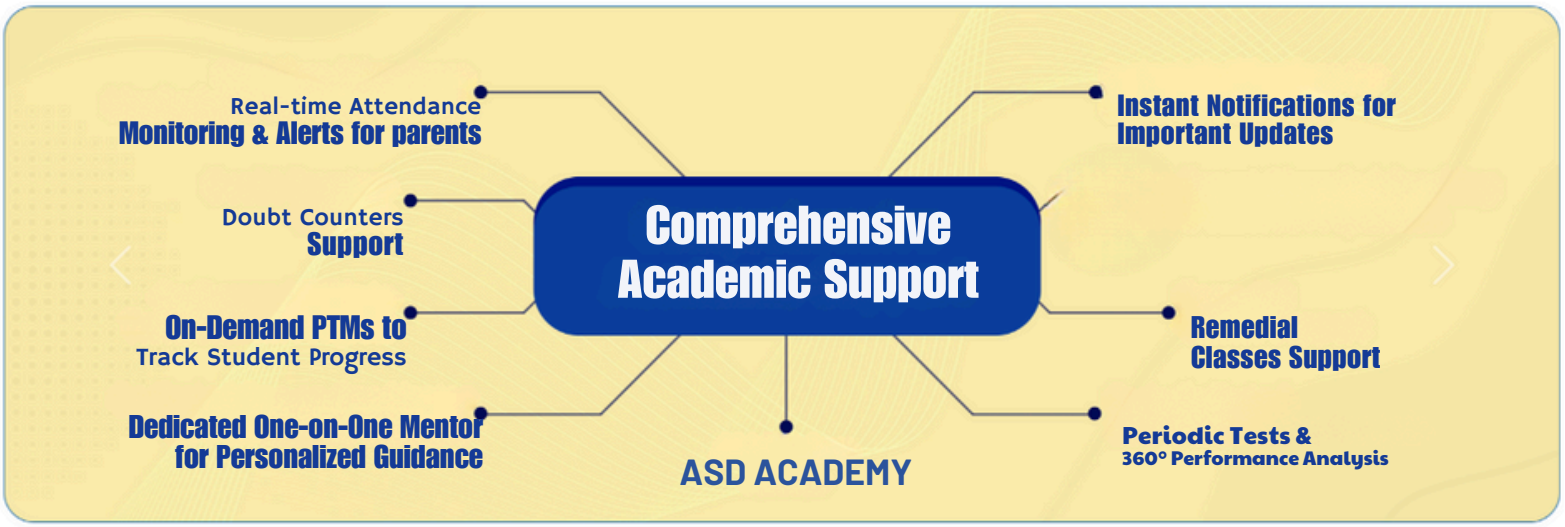
## OFFLINE DIPLOMA COURSE

Super 30 Diploma
3 Month Internship
100% Placement Assitance

Super 30 Diploma Fee
67800+Gst =80000/-

Let's win Diploma
1.5 Month Internship
Without Placement Assitance

Let's Win Diploma Fee
50000+Gst = 59000/-



# ONLINE DIPLOMA COURSE

## 🔥 "Beat Hackers at Their Own Game with SUPER 30 BATCH & AI — A Revolutionary Way to Learn Cyber Security Diploma !" 🔥

## ABOUT OUR SUPER 30 BATCH (ONLINE)

### 1. Learn

👉 1 Year Training + 3 Month Internship Program led by Experienced Trainers (7+ Years) from Metro Cities (Bangalore, Hyderabad, Mumbai, Delhi), with Assistant Trainers for doubt solving, project guidance, practical sessions, and assignments.

👉 100% Placement Assistance

👉 **Course Modules Covered: (Monday to Friday classes )**

✅ Network Fundamentals

✅ Programming Basics (HTML & CSS)

✅ Python

✅ Linux Fundamentals

✅ SOC (Splunk)

✅ Windows Server 2022

✅ SC-900 (Microsoft Security Compliance Certification)

✅ ISO-27001 (Information Security Management Systems)

👉 **Course Modules Covered: (Alternative Classes )**

✅ CEH (Certified Ethical Hacker)

✅ VAPT (Vulnerability Assessment & Penetration Testing)

✅ Mobile App Testing & API Testing

✅ Source Code Review

👉 **Program Highlights:**

- ✅ Recorded Lectures available for easy revision
- ✅ Final exams for every batch on Proctored basis to assess learning progress
- ✅ Exam Fee Rs. 2000 each
- ✅ 2 Assignments per Week for practical application
- ✅ Monthly Performance Report Card for continuous evaluation
- ✅ Interview Preparation & Personality Development Classes
- ✅ Mock Interviews for HR & Technical Rounds
- ✅ Resume Building Sessions to enhance your profile
- ✅ Diploma in Cybernetics upon course completion
- ✅ 2 certificates in course (Diploma Certificate + Proctored Certificate)
- ✅ Exclusive Alumni Upgrade Program for better job opportunities & latest course updates

# ONLINE DIPLOMA COURSE

## 🔥 "Beat Hackers at Their Own Game with LET'S WIN BATCH & AI — A Revolutionary Way to Learn Cyber Security Diploma !" 🔥

## ABOUT OUR LET'S WIN BATCH (ONLINE)

### 1. Learn

👉 1 Year Training Program led by Experienced Trainers (7+ Years) from Metro Cities (Bangalore, Hyderabad, Mumbai, Delhi), with Assistant Trainers for doubt solving, project guidance, practical sessions, and assignments.

👉 **Course Modules Covered: (Monday to Friday classes )**

- ✅ Network Fundamentals
- ✅ Programming Basics (HTML & CSS)
- ✅ Python
- ✅ Linux Fundamentals
- ✅ SOC (Splunk)
- ✅ Windows Server 2022
- ✅ SC-900 (Microsoft Security Compliance Certification)
- ✅ ISO-27001 (Information Security Management Systems)

👉 **Course Modules Covered: (Alternative Classes )**

- ✅ CEH (Certified Ethical Hacker)
- ✅ VAPT (Vulnerability Assessment & Penetration Testing)
- ✅ Mobile App Testing & API Testing
- ✅ Source Code Review

👉 **Program Highlights:**

✅ Recorded Lectures available for easy revision

✅ Final exams for every batch on Proctored basis to assess learning progress

✅ Exam Fee Rs. 2000 each

✅ 1 Assignment per Week for practical application

✅ Monthly Performance Report Card for continuous evaluation

✅ Mock Interviews for HR & Technical Rounds

✅ Resume Building Sessions to enhance your profile

✅ Diploma in Cybernetics upon course completion

✅ 2 certificates in course (Diploma Certificate + Proctored Certificate)

✅ Exclusive Alumni Upgrade Program for better job opportunities & latest course updates

# OFFLINE DIPLOMA COURSE

## 🔥 "Beat Hackers at Their Own Game with SUPER 30 BATCH & AI — A Revolutionary Way to Learn Cyber Security Diploma !" 🔥

## ABOUT OUR SUPER 30 BATCH (OFFLINE)

### 1. Learn

👉 1 Year Training + 3 Month Internship Program led by Industry Based Trainers , with Assistant Trainers for doubt solving, project guidance, practical sessions, and assignments.

👉 Personal Development Classes - Spoken classes , Interview Preparation , Expert Lectures

👉 Extraa Curricular Activities- Indoor & Outdoor Activity , Freshers Party Cultural Activity

👉 100% Placement Assistance

👉 **Course Modules Covered: (Monday to Friday classes )**

✅ Network Fundamentals
✅ Programming Basics (HTML & CSS)
✅ Python
✅ Linux Fundamentals
✅ SOC (Splunk)
✅ Windows Server 2022
✅ SC-900 (Microsoft Security Compliance Certification)
✅ ISO-27001 (Information Security Management Systems)

👉 **Course Modules Covered: (Alternative Classes )**

✅ CEH (Certified Ethical Hacker)
✅ VAPT (Vulnerability Assessment & Penetration Testing)
✅ Mobile App Testing & API Testing
✅ Source Code Review

👉 **Program Highlights:**

- ✅ Recorded Lectures available for easy revision
- ✅ Final exams for every batch on Proctored basis to assess learning progress
- ✅ Exam Fee Rs. 2000 each
- ✅ 2 Assignments per Week for practical application
- ✅ Monthly Performance Report Card for continuous evaluation
- ✅ Interview Preparation & Personality Development Classes
- ✅ Mock Interviews for HR & Technical Rounds
- ✅ Resume Building Sessions to enhance your profile
- ✅ Diploma in Cybernetics upon course completion
- ✅ 2 certificates in course (Diploma Certificate + Proctored Certificate)
- ✅ Exclusive Alumni Upgrade Program for better job opportunities & latest course updates

# OFFLINE DIPLOMA COURSE

🔥 "Beat Hackers at Their Own Game with LET'S WIN BATCH & AI — A Revolutionary Way to Learn Cyber Security Diploma !" 🔥

## ABOUT OUR LET'S WIN BATCH (OFFLINE)

### 1. Learn

👉 1 Year Training Program led by Industry Based Trainers , with Assistant Trainers for doubt solving, project guidance, practical sessions, and assignments.

👉 **Course Modules Covered: (Monday to Friday classes )**

- ✅ Network Fundamentals
- ✅ Programming Basics (HTML & CSS)
- ✅ Python
- ✅ Linux Fundamentals
- ✅ SOC (Splunk)
- ✅ Windows Server 2022
- ✅ SC-900 (Microsoft Security Compliance Certification)
- ✅ ISO-27001 (Information Security Management Systems)

👉 **Course Modules Covered: (Alternative Classes )**

- ✅ CEH (Certified Ethical Hacker)
- ✅ VAPT (Vulnerability Assessment & Penetration Testing)
- ✅ Mobile App Testing & API Testing
- ✅ Source Code Review

👉 **Program Highlights:**

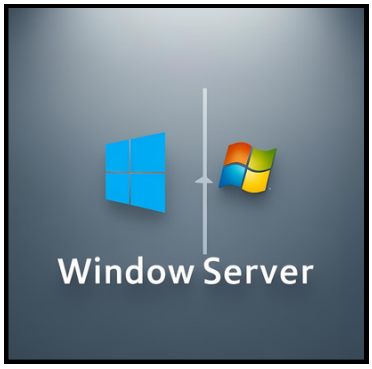
- ✅ Recorded Lectures available for easy revision
- ✅ Final exams for every batch on Proctored basis to assess learning progress
- ✅ Exam Fee Rs. 2000 each
- ✅ 1 Assignments per Week for practical application
- ✅ Monthly Performance Report Card for continuous evaluation
- ✅ Interview Preparation & Personality Development Classes
- ✅ Mock Interviews for HR & Technical Rounds
- ✅ Resume Building Sessions to enhance your profile
- ✅ Diploma in Cybernetics upon course completion
- ✅ 2 certificates in course (Diploma Certificate + Proctored Certificate)
- ✅ Exclusive Alumni Upgrade Program for better job opportunities & latest course updates

# IN THIS DIPLOMA WE HAVE THIRTEEN COURSES

NETWORK FUNDAMENTALS

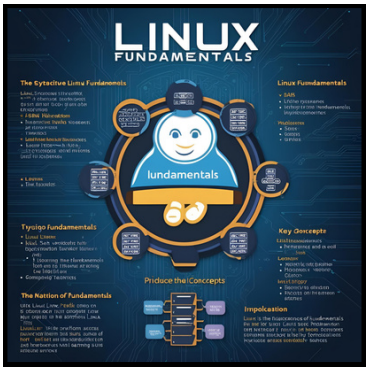

PROGRAMMING BASICS (HTML + CSS)

PYTHON




WINDOWS SERVER 2022

SOC (SPLUNK)




LINUX FUNDAMENTALS


CEH

VAPT

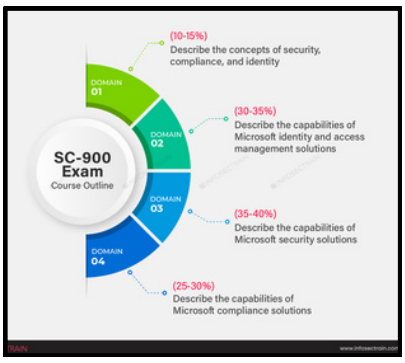
MOBILE APP TESTING

# IN THIS DIPLOMA WE HAVE THIRTEEN COURSES



**APT TESTING**

**SOURCE CODE REVIEW**





**SC-900**

**ISO 27001 LA**


## What is a Networking course?

Networking course helps students to understand the basics of computer networks and how these devices communicate with each other using wired and wireless networks. This course is important from the industry point of view as without a network nothing is possible.

## WHAT WE TEACH YOU IN NETWORKING COURSE ?

- Introduction , scope of CCNA , growth , and job
- Introduction of Network
- Basic introduction of Network devices, basic tools
- Introduction of Router, switch, firewall, and other network device
- Basic configuration of Router
- OSI MODEL & their function
- Explanation of layer
- Function of layer
- Tcp and udp
- Network layer protocol
- Introduction of IP Adddress
- Ipv4 address

- Classes of IP
- Public IP Address
- Private IP Address
- Subnetting
- Introduction of IPv6
- Routing and Their Protocols
- RIP Protocol
- Function of RIP
- Practical of RIP
- Static Routing and Their Types
- Configuration of Static Routing
- EIGRP and Their Function
- Practical of EIGRP
- Hold Time and Hello Time (Practical)
- Introduction of OSPF
- Function of OSPF
- Introduction of Switch
- VLAN
- VTP
- STP and Their Function
- Practical to Create VLAN
- Configuration of Switch
- Introduction of Wireless
- Practical of Wireless Communication
- Wireless Media
- How to Create SSID
- How to Communicate in Wireless Mode
- Introduction of Security Device
- Firewall and Their Types
- Function of Firewall

After completing the **Networking course** you'll have job opportunities like:

- System administrator
- Network Engineer
- Technical Support
- Network administrator
- IT administrator

# What is a Programming Basics (HTML + CSS) course?

HTML (HyperText Markup Language) is the standard language used to create and structure web pages.

It defines the content on a webpage, such as headings, paragraphs, links, images, and lists.

HTML uses tags and elements to organize and display content in a structured format.

CSS (Cascading Style Sheets) controls the look and feel of the HTML content.

CSS is used to style elements by changing colors, fonts, layouts, and spacing.

It helps make web pages more attractive, user-friendly, and responsive across devices.

HTML and CSS together build the front-end (visual part) of a website.

They are essential for creating basic static web pages before moving on to advanced coding.

Understanding HTML and CSS is the first step towards becoming a web developer.

They lay the foundation for learning more complex web technologies like JavaScript, React, or backend development.

# What we teach you in Programming Basics (HTML + CSS) course?

## INTRODUCTION ON HTML5

- CLient-Server Architecture
- Building Blocks
- Boiler Plate Code

## HTML BODY ELEMENTS

- Heading
- Formatting tags
- Paragraph

## HTML WITH CSS

- Types of CSS
- Syntax, property value pair
- HTML with CSS

## SEMANTICS TAGS

- <article>
- <header>
- <footer>

## CSS PROPERTIES

- Height/Width
- Max-width
- Animation

## HTML HEAD ELEMENTS

- <base> Tag
- <meta> Tag
- <title> Tag


## What is Python?

Python is one of the most popular programming languages today, and it's widely used in many different fields such as web development, data analysis, AI, and automation. It's known for its simplicity and versatility, making it an excellent choice for beginners and experts alike.

Python is a high-level programming language, meaning that it is user-friendly and allows us to write code that is easy to read and understand. It was created by Guido van Rossum and first released in 1991.

# What we teach you in **Python** course ?

**Python Powered by AI**

## Get the AI edge with 15 Power-packed Modules of the Python

**Course Outline**

**Module 01** **Introduction to Python Programming**
- Overview of Python, installing Python, and setting up the development environment.

**Module 02** **Variables and Data Types**
- Strings, Integers, Floats, Booleans, and Type Conversion.

**Module 03** **Operators in Python**
- Arithmetic, Logical, Relational, and Bitwise Operators.C

**Module 04** **Control Flow and Conditional Statements**
- If, Elif, Else statements, and Nested conditions.

**Module 05** **Loops in Python**
- For loops, While loops, Loop control with break, continue, and pass.

**Module 06** **Functions in Python**
- Defining Functions, Arguments, Return Values, Lambda Functions.

**Module 07** **File Handling**
- Reading from and Writing to files, Working with file modes and file objects.

**Module 08** **Lists, Tuples, and Sets**
- List Operations, Tuple and Set Basics.

**Module 09** **Dictionaries**
- Working with key-value pairs and Dictionary methods.

**Module 10** **Working with APIs in Python**
- RESTful APIs, JSON parsing, and making requests in Python.

**Module 11** **Python for Automation**
- Automating tasks with Python using libraries.

**Module 12** **Cryptography in Python**
- Symmetric and Asymmetric Encryption, using libraries.

**Module 13** **Testing and Debugging in Python**

- Writing Unit Tests with unittest, Debugging with pdb.

**Module 14** **Building GUI Applications in Python**

- Tkinter basics for creating simple desktop applications.

**Module 15** **Cyber Security tools creation with using Python**

- Creating cybersecurity tools with Python for security testing and automation.

## After completing the **Python** course You're eligible to do:

- Python Developer
- Data Scientist
- Software Engineer
- Automation Tester / Scripting Expert
- Web Developer (Backend)
- Machine Learning Engineer
- Data Analyst


## What is Window Server?

Windows Server is a powerful server operating system developed by Microsoft, designed to manage and support enterprise-level IT infrastructure. It enables organizations to build and control networks where multiple users and devices can access shared resources like files, printers, applications, and databases. One of its key features is Active Directory, which allows administrators to manage users, computers, and security policies centrally. It also includes DNS and DHCP services that help with network configuration and IP address management. Internet Information Services (IIS) enables web hosting on the server, while Remote Desktop Services (RDS) provides remote access to applications and desktops. Windows Server comes with Hyper-V, Microsoft's built-in virtualization platform, which allows running multiple virtual machines on a single physical server, helping businesses reduce hardware costs. It also offers advanced security features, including firewalls, encryption, and group policies, ensuring data protection and compliance. Windows Server supports clustering, backup, and disaster recovery solutions to enhance system availability and reliability. Versions like Windows Server 2012, 2016, 2019, and the latest 2022 bring continuous improvements in performance, security, cloud integration, and hybrid capabilities with Microsoft Azure.

# What we teach you in **window Server ?**

**window ServerPowered by AI**

## Get the AI edge with 12 Power-packed Modules of the Window Server

**Course Outline**

**Module 01** **Introduction to window server**
- Windows Server is Microsoft’s operating system for managing enterprise network services

**Module 02** **Print Server**
- Configuration & Management

**Module 03** **HTTP Server**
- Basics & Configuration

**Module 04** **FTP Server**
- Basics & Secure File Transfers

**Module 05** **DHCP Server**
- Dynamic IP Management

**Module 06** **Mail Server**
- Email Communication & Security

**Module 07** **Data Management & Optimization**
- Data Management & Optimization

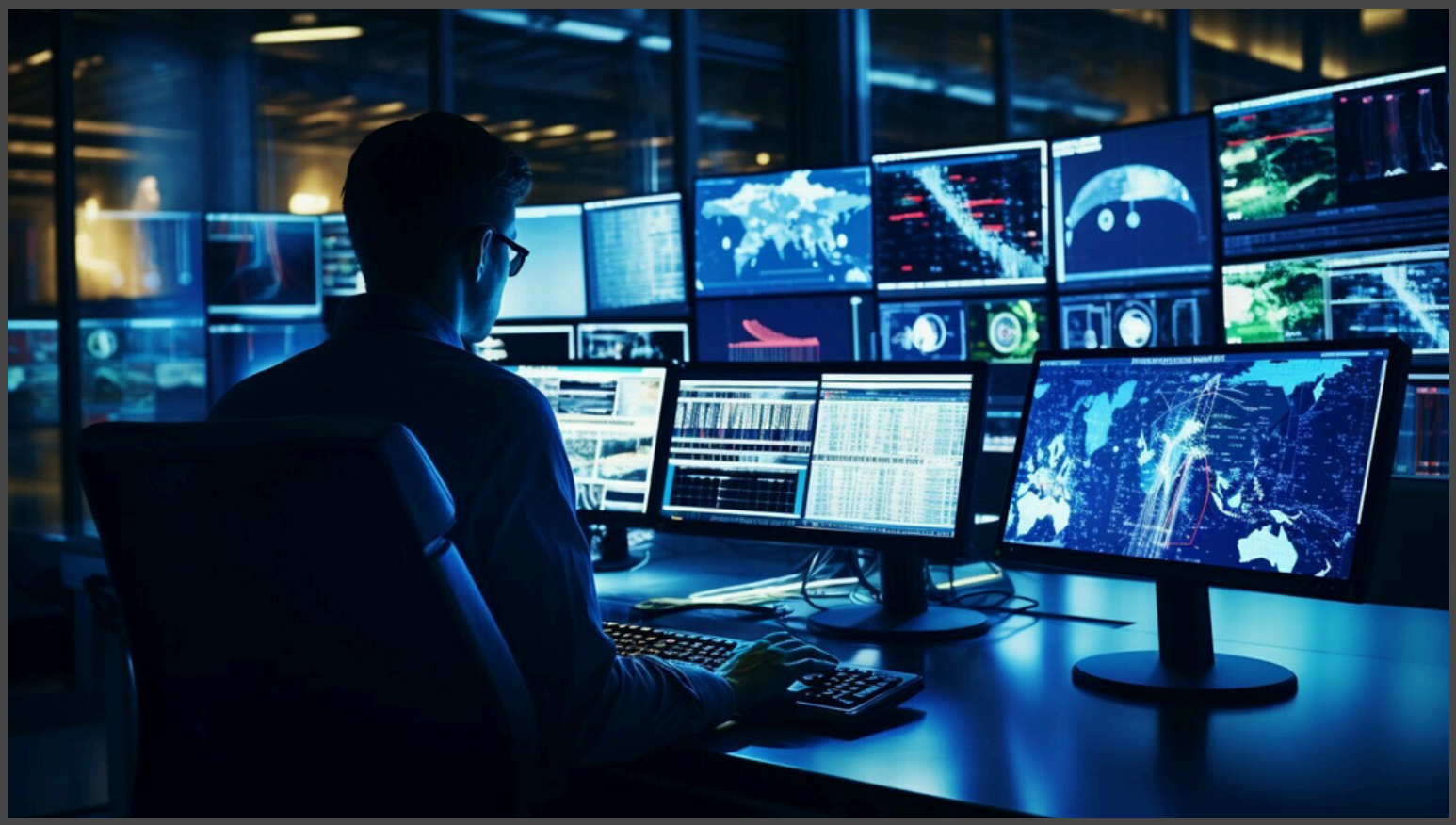
**Module 08** **SMD Server**
- List Operations, Tuple and Set Basics.

**Module 09** **Dictionaries**
- Working with key-value pairs and Dictionary methods.

**Module 10** **File Handling**
- Reading from and Writing to files, Working with file modes and file objects.

**Module 11** **Lists, Tuples, and Sets**
- List Operations, Tuple and Set Basics.

**Module 12** **Active Directory**
- Active Directory centralizes user management, authentication, and security policies in a network



After completing the **Window Server** course
You're eligible to do:

- System Administrator
- Network Administrator
- Server Support
- Engineer
- IT Support Specialist
- Cloud Support Engineer (Azure/Hybrid)
- Security Analyst (SOC)


# What is SOC (SPLUNK) ?

A Security Operations Center (SOC) is a centralized unit that monitors and manages an organization's security posture.

It detects, analyzes, and responds to cybersecurity incidents in real-time to protect IT infrastructure.

Splunk is a powerful tool used in SOCs for Security Information and Event Management (SIEM).

It collects, indexes, and analyzes large volumes of machine-generated data from servers, networks, and applications.

With Splunk, SOC teams can detect suspicious activities and potential threats more efficiently.

It helps automate alerts, generate reports, and visualize security data through dashboards.

Splunk enables correlation of events from different data sources to identify complex attack patterns.

SOC analysts use Splunk to conduct threat hunting, incident response, and forensic investigations.

It supports compliance management by generating audit reports for standards like GDPR, HIPAA, etc.

Overall, Splunk empowers SOCs to improve cyber threat detection, response times, and security visibility.

# What we teach you in **SOC (SPLUNK) course ?**

**SOC (SPLUNK) Powered by AI**

## Get the AI edge with 11 Power-packed Modules of the SOC (SPLUNK)

**Course Outline**

**Module 01 Introduction to Splunk & Installation**

- learning about Splunk as a powerful platform for searching, analyzing, and visualizing machine-generated data, along with steps to install and set it up on various operating systems.

**Module 02 Understanding Splunk Architecture & Indexing**

- covers how Splunk components (forwarders, indexers, search heads) work together to collect, index, and search machine data efficiently.

**Module 03 Performing Basic Searches in Splunk**

- involves using simple search commands to find, filter, and analyze data from indexed logs and events.

**Module 04 Advanced Searching & Data Filtering**

- Splunk involves using complex search commands, keywords, and filters to extract specific insights from large datasets efficiently.

**Module 05 Data Visualization & Dashboarding**

- Splunk involves creating interactive charts, graphs, and dashboards to monitor and analyze data insights in real time.

**Module 06 Lookup Tables & Data Enrichment**

- Splunk involve enhancing event data by adding external information through lookup files, improving search results and analysis

**Module 07 Alerts & Scheduled Searches**

- Splunk automate monitoring by running searches at defined intervals and triggering alerts based on specific conditions or thresholds

**Module 08 User & Role Management**

- Splunk involves creating, assigning, and controlling user access and permissions to ensure secure and role-based access to data and features.

**Module 09 Splunk Data Models & CIM**

provide a standardized framework for organizing and normalizing data, enabling consistent searches, reports, and accelerated data analysis across different data sources

**Module 10 Integrating External Data & APIs**

- Splunk involves connecting and importing data from third-party sources and services using REST APIs or other integration methods for enhanced data analysis and correlation

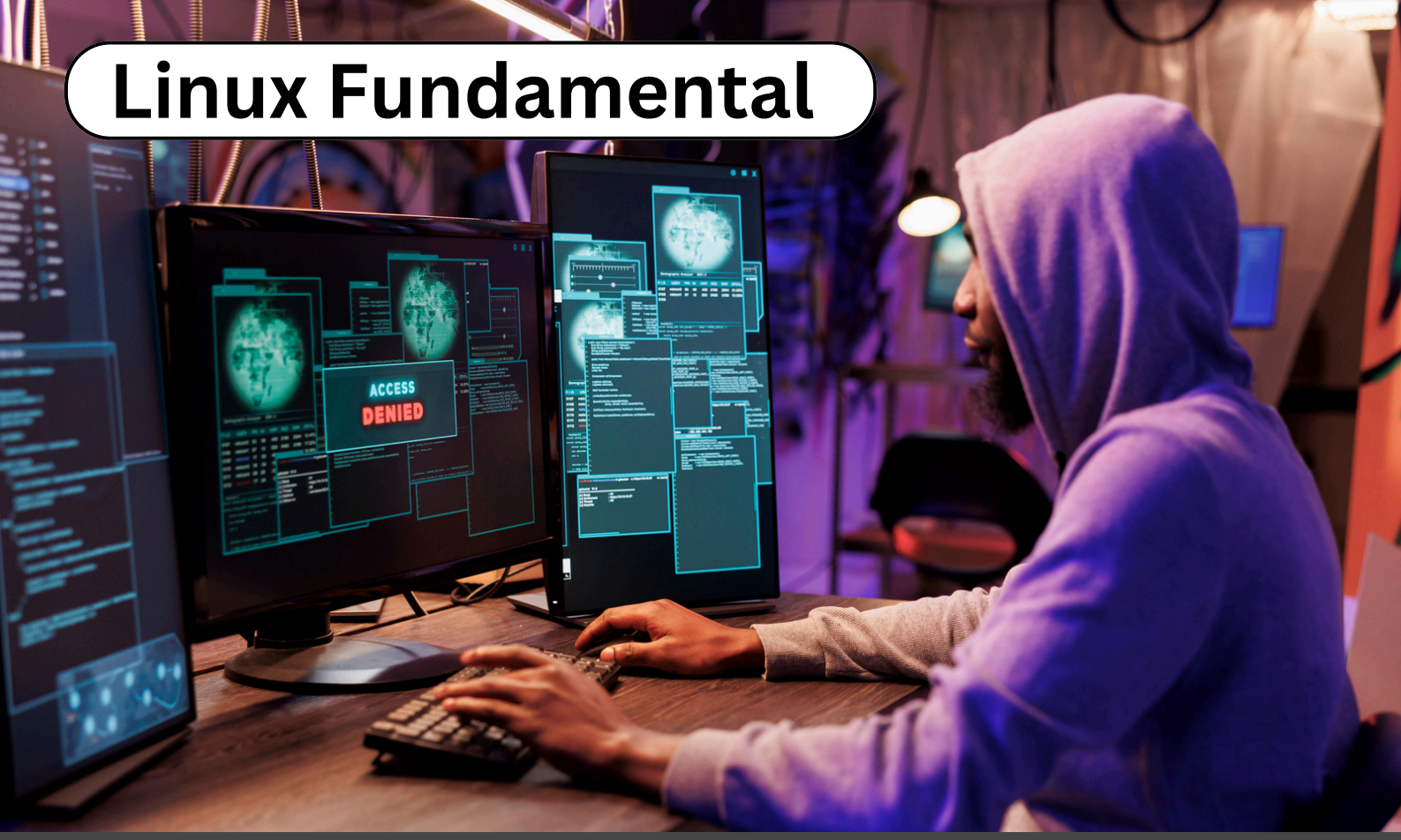
**Module 11 Performance Tuning & Optimization**

- Splunk focuses on improving search efficiency, indexing speed, and system resource utilization to ensure faster data processing and optimal platform performance

After completing the **SOC(SPLUNK)** course
You're eligible to do:

- SOC Analyst (Level 1/2/3)
- SIEM Engineer
- Security Analyst
- Threat Hunter
- Splunk Administrator
- Incident Responder
- Cybersecurity Consultant

# Linux Fundamental




## What is Linux Fundamental ?

Linux Fundamentals refer to the basic concepts and skills required to understand and work with the Linux operating system. Linux is an open-source, Unix-like system widely used for servers, desktops, and embedded devices. In Linux fundamentals, you learn about its architecture, including the kernel, shell, and file system hierarchy. It covers essential command-line operations such as navigating directories, managing files, and setting permissions. User and group management, process control, and software installation using package managers are key areas of focus. Additionally, you explore basic networking tasks like configuring IP addresses and testing network connectivity. Shell scripting is introduced to automate tasks and simplify system administration. Security concepts, including managing file permissions and configuring firewalls, are also part of Linux fundamentals. These skills lay the foundation for more advanced system administration and cybersecurity roles.

# What we teach you in **Linux Fundamental ?**

**Linux Fundamental Powered by AI**

## Get the AI edge with 9 Power-packed Modules of the Linux Fundamental

**Course Outline**

**Introduction to Linux Fundamental**

Linux Fundamentals introduce the basics of the Linux operating system, including file systems, commands, user management, and system administration

### Module 01 Introduction to Linux

- Linux is a free, open-source operating system - used on servers, desktops, and devices.
- It's known for security, stability, and flexibility- making it popular in IT and cybersecurity.
- Linux uses a command-line interface (CLI) - for powerful system control.
- **Tools**-Ubuntu, CentOS, and Kali Linux

### Module 02 Getting Started with Linux

- Choose a Linux Distribution (Distro)
- Install Linux
- Learn Basic Commands
- Explore the File System
- Practice Package Management

### Module 03 User and Group Management

- Administrators
- Permissions
- Users
- Group Management
- User Management

### Module 04 File Permissions and Ownership

- File Permissions define who can read, write, or execute
- Ownership assigns a User (Owner) and a Group
- Read (r) – View file contents
- Write (w) – Modify file contents
- Execute (x) – Run files or enter directories

### Module 05 Process and Job Management

- efficient system performance and resource allocation.
- Job Management
- Process ID (PID)
- Process Management
- Process and Job Management

**Module 06 Linux Networking Basics**

- Trace Network Routes
- View Network Connections
- Connectivity Check
- Network Interface Management
- Configure

**MODEL 07 Security Basics in Linux**

- Process Monitoring
- Password Policies
- Updates and Patching
- SSH Security
- Firewalls

**Module 08 Linux Security Essentials**

- Strong Password Policies
- Firewall Configuration
- Secure SSH Access
- System Updates & Patching

**Model 09 System Administration Basics**

- Backup and Restore
- Security Management
- Log Management
- Network Configuration
- Performance Monitoring

After completing the **Linux Fundamental**course
You're eligible to do:

- Linux System Administrator
- Technical Support Engineer (Linux)
- Technical Support Engineer (Linux)
- IT Support Specialist
- Network Administrator (Linux)
- DevOps Engineer (Entry-Level)
- System Analyst (Linux)


# What is a Certified Ethical Hacking v13 course?

By joining the AI Revolution as a Certified Ethical Hacker, you'll gain the expertise to navigate the cutting-edge world of cybersecurity.

Certified Ethical Hackers, trained in the latest version of CEH v13, are equipped with AI-powered tools and techniques to identify, exploit, and secure vulnerabilities in systems and networks. You'll learn to leverage AI for automating threat detection, predicting security breaches, and responding swiftly to cyber incidents. Moreover, you'll also gain the skills needed to secure AI-driven technologies against potential threats. This combination of ethical hacking and AI capabilities will place you at the forefront of cybersecurity, ready to defend organizations across industries from advanced threats and adapt to evolving challenges.

Amplify Your Edge as a Certified Ethical Hacker Powered by AI Capabilities:

Advanced Knowledge: As a Certified Ethical Hacker powered by AI, you'll possess in-depth knowledge of ethical hacking methodologies, enhanced with cutting-edge AI techniques.

AI Integration: You'll effectively integrate AI across every phase of ethical hacking, from reconnaissance and scanning to gaining access, maintaining access, and covering your tracks.

Automation and Efficiency: You'll leverage AI to automate tasks, boost efficiency, and detect sophisticated threats that traditional methods might overlook.

Proactive Defense: With AI at your disposal, you'll be equipped for proactive threat hunting, anomaly detection, and predictive analysis to prevent cyber-attacks before they happen.

# CEH v13: The World's First Ethical Hacking Certification with a 4-Phase AI-Powered Learning Framework

The CEH v13 is a specialized, one-of-a kind training program that helps you gain expertise in ethical hacking, AI, and machine learning. With hands-on training labs, knowledge-based and practical exams, a mock ethical hacking engagement on live networks, and a global hacking competition, this program ensures you master the most in-demand skills needed to excel and stand out in the cybersecurity industry.

This learning framework offers not only a comprehensive training program to prepare you for the certification exam but also the industry's most robust, in-depth, hands on lab and practice range experience

**Master Ethical Hacking and AI Skills That Go Beyond Certification**

## Learn

Courseware
Cyber Range
Gain Skills

1

## Certify

Knowledge-Based
Practical Exam
Gain Recognition

2

## Engage

Live Cyber Range
Gain Experience

3

## Compete

Global Ethical
Hacking Competition
Gain Respect

4

## Certified Ethical Hacker Powered by AI

### Get the AI edge with 20 Power-packed Modules of the CEH v13

| Learn | Course Outline |
|---|---|
| **Module 01** Introduction to Ethical Hacking | Learn the fundamentals and key issues in information security, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures. |
| **Module 02** Footprinting and Reconnaissance | Learn how to use the latest techniques and tools for footprinting and reconnaissance, a critical pre-attack phase of ethical hacking |
| **Module 03** Scanning Networks | Learn different network scanning techniques and countermeasures. |
| **Module 04** Enumeration | Learn various enumeration techniques, including Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits and associated countermeasures. |
| **Module 05** Vulnerability Analysis | Learn how to identify security loopholes in a target organization's network, communication infrastructure, and systems. Diferent types of vulnerability assessment and vulnerability assessment tools are also included. |
| **Module 06** System Hacking | Learn about the various system hacking methodologies used to discover system and network vulnerabilities, including steganography, steganalysis attacks, and how to cover tracks. |
| **Module 07** Malware Threats | Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures. |
| **Module 08** Sniffing | Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus countermeasures to defend against snifing attacks. |
| **Module 09** Social Engineering | Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures. |
| **Module 10** Denial-of-Service | Learn about different Denial of Service (DoS) and Distributed Dos (DDoS) attack techniques, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections. |

| Learn | Course Outline |
| --- | --- |
| **Module 11**<br>Session Hijacking | Learn the various session-hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures. |
| **Module 12**<br>Evading IDS, Firewalls, and Honeypots | Learn about firewalls, intrusion detection systems (IDS), and honeypot evasion techniques; the tools used to audita network perimeter for weaknesses; and countermeasures. |
| **Module 13**<br>Hacking Web Servers | Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures. |
| **Module 14**<br>Hacking Web Applications | Learn about web application attacks, including a comprehensive hacking methodology for auditing vulnerabilities in web applications and countermeasures. |
| **Module 15**<br>SQL Injection | Learn about SQL injection attack techniques, evasion techniques, and SQL injection countermeasures. |
| **Module 16**<br>Hacking Wireless Networks | Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools, and countermeasures for wireless networks. |
| **Module 17**<br>Hacking Mobile Platforms | Learn mobile platform attack vectors, Android and ios hacking, mobile device management, mobile security guidelines, and security tools. |
| **Module 18**<br>IoT Hacking | Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures. |
| **Module 19**<br>Cloud Computing | Learn different cloud computing concepts, such as container technologies and serverless computing. various cloud computing threats, attacks, hacking methodologies, and cloud security techniques and tools. |
| **Module 20**<br>Cryptography | Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools. |

# After completing the CEH course
# You're eligible to do:

- Ethical Hacker / Penetration Tester
- Information Security Analyst
- Security Consultant
- Vulnerability Assessor
- Network Security Engineer
- SOC (Security Operations Center) Analyst
- Cybersecurity Analyst


# What is a VAPT course?

The Vulnerability Assessment and Penetration Testing (VAPT) Course is designed to provide students with a comprehensive understanding of network security through both practical and theoretical knowledge. This course introduces the basics of network security, explaining the difference between vulnerability assessment and penetration testing. Students learn methodologies for identifying vulnerabilities in systems using various tools and techniques, and how to analyze and report their findings. The course also covers the phases of penetration testing, including planning, discovery, attack, and reporting, and teaches students to conduct ethical hacking to exploit vulnerabilities using industry-standard tools. Students gain knowledge in risk analysis and management, evaluating and prioritizing risks based on the severity of vulnerabilities and implementing mitigation strategies to protect against security threats.

**VAPT Powered by AI**

# Get the AI edge with 7 Power-packed Modules of the VAPT

## Course Outline

### Module 01 Understanding Web Application Concepts

- Introduction to web applications
- How web applications work
- Web application architecture
- Web 2.0 Applications
- Vulnerability Stack

### Module 02 Understanding Web Application Threats

- Unvalidated Input
- Parameter/Form Tampering
- Directory Traversal
- Security Misconfiguration
- Web Service Attack
- Hidden Field Manipulation Attack j.
- Cross-Site Scripting (XSS) Attack k.
- Cross-Site Request Forgery (CSRF)
- Web Application Denial-of-Service Attack
- Web Service Architecture
- Improper Error Handling
- Insecure Cryptographic Storage
- Broken Authentication and Session Management
- Unvalidated Redirects and Forwards
- Buffer Overflow
- Cookies/Session Poisoning
- Session Fixation Attack
- Insufficient Transport Layer protection
- Injection Flaws
- SQL Injection Attacks
- Command Injection Attacks
- LDAP Injection
- XML Poisoning

### Module 03 Understanding Web Application Hacking Methodology

- Footprint Web Infrastructure
- Attack Web Servers
- Analyze Web Application
- Attack Authentication Mechanism
- Attack Authorization Schemes
- Attack Session Management Mechanism
- Perform Injection Attacks
- Attack Data Connectivity
- Attack Web App Client
- Attack Web Services

### Module 04 Web Application hacking Tools

- Burp Suite Professional
- Zap Proxy

## Course Outline

### Module 05 Understanding Web Application Countermeasure

- Encoding Schemes
- How to defend against SQL Injection Attack
- How to defend against Command Injection Flaw
- How to defend against XSS Attack
- How to defend against DoS Attack
- How to defend against Web Services Attack
- Guidelines for Secure CAPTCHA Implementation
- Web Application Attack Countermeasure
- How to defend against Web Application Attacks

### Module 06 Web Application Security Tools

- Acunetix Web Vulnerability Scanner
- Netsparker
- Nikto

### Module 07 Overview of Web Application Penetration Testing

- Information Gathering
- Configuration Management Testing
- Authentication Testing
- Session Management Testing
- Authorization Testing
- Data Validation Testing
- Denial-of-Service Testing
- Web Service Testing
- AJAX Testing

## After completing the VAPT course ?
## You're eligible to do:

- Penetration Tester
- Cybersecurity Consultancy
- Security Analyst
- Perform Security Audits
- Conduct Vulnerability Assessments


## What is a Mobile App testing ?

The **Mobile App Testing with OWASP Top 10 Tools and AI Course** is a specialized training program designed to teach participants how to identify, analyze, and fix security vulnerabilities in mobile applications. The course focuses on the **OWASP Mobile Top 10 risks**, such as insecure data storage, insufficient cryptography, and insecure communication.

It combines traditional **manual testing** techniques with **AI-powered tools** to automate vulnerability scanning, improve threat detection, and enhance security assessments. Learners gain practical experience in using industry-standard testing tools alongside AI for smarter, faster, and more accurate mobile app security testing. This course is ideal for penetration testers, security analysts, and mobile app developers looking to secure their applications against modern threats.

# Mobile App Testing Powered by AI

## Get the AI edge with 10 Power-packed Modules of the Mobile App Testing

### Course Outline

**Introduction to OWASP Mobile Top 10**

- **Overview of OWASP Mobile Top 10 & why mobile security is crucial**
- **Setup tools: MobSF, Burp Suite, Frida, JADX, Objection**

**Module 01 Improper Credential Usage**

- What it is → Hardcoded credentials, weak session handling
- Attack Techniques → Extracting credentials via decompilation
- Best Practices → Secure storage (Keystore, Keychain)
- **Tools → JADX, Objection, Frida**

**Module 02 Inadequate Supply Chain Security**

- What it is → Risks from third-party SDKs & dependencies
- Attack Techniques → Code injection, scanning for vulnerabilities
- Best Practices → SCA, package integrity verification
- **Tools → MobSF, OWASP Dependency-Check, Snyk**

**Mini Project 1 Hardcoded Credentials & Supply Chain Attack**

**Vulnerable App: InsecureBankV2**

- Objectives:
- Extract hardcoded credentials from the app
- Analyze and modify third-party library vulnerabilities
- Exploit weak authentication mechanisms
- **Tools: JADX, Frida, Objection, MobSF**

**Module 03 Insecure Authentication/Authorization**

- What it is → Weak passwords, missing MFA, session hijacking
- Attack Techniques → Login bypass, session replay
- Best Practices → OAuth 2.0, JWT security
- **Tools → Burp Suite, JWT.io, Postman**

**Module 04 Insufficient Input/Output Validation**

- What it is → SQL Injection, XSS, XML Injection in mobile APIs
- Attack Techniques → Fuzzing API requests, using SQLmap
- Best Practices → Input validation, parameterized queries
- **Tools → Burp Suite, SQLmap, ZAP, MobSF**

**Mini Project :2 Authentication Bypass & Injection Attacks**

**Vulnerable App: Damn Vulnerable Bank (DVB)**

- Objectives:
- Perform authentication bypass using Burp Suite
- Exploit SQL Injection in login & API requests
- Intercept and modify JWTs
- **Tools: Burp Suite, SQLmap, JWT.io**

## Module 05 Insecure Communication

- What it is → MITM attacks, weak TLS configurations
- Attack Techniques → Capturing & modifying HTTPS traffic
- Best Practices → TLS 1.2+, certificate pinning
- **Tools → Burp Suite, mitmproxy, SSL Labs Test**

## Module 06 Inadequate Privacy Controls

- What it is → Excessive permissions, data leaks
- Attack Techniques → Checking app permissions & data leaks
- Best Practices → Least privilege, GDPR compliance
- **Tools → MobSF, Exodus Privacy, APK Analyzer**

## Mini Project :3 MITM Attack & Privacy Violations

### Vulnerable App: DIVA (Damn Insecure and Vulnerable App)

- Objectives:
- Perform a MITM attack to capture login credentials
- Identify excessive permissions in an Android app
- Extract sensitive user data leaks
- **Tools: Burp Suite, mitmproxy, MobSF**

## Module 07 Insufficient Binary Protections

- What it is → Reverse engineering, repackaging, tampering
- Attack Techniques → Decompiled APK modification, tampering
- Best Practices → Obfuscation, anti-debugging, runtime protection
- **Tools → JADX, APKTool, Frida, Objection**

## Module 08 Security Misconfiguration

- What it is → Exported activities, deep link vulnerabilities
- Attack Techniques → Exploiting exported components, weak permissions
- Best Practices → Secure manifest configurations
- **Tools → Drozer, MobSF, APKTool**

## Mini Project :4 Reverse Engineering & Security

### Vulnerable App: InsecureShop

- Objectives:
- Reverse engineer and modify an APK
- Exploit exported activities and weak permissions
- Bypass root detection and tamper security mechanisms
- **Tools: JADX, Frida, Objection, APKTool**

## Module 09/10 Insecure Data Storage & Insufficient Cryptography

- What it is → Storing credentials in plaintext, weak encryption
- Attack Techniques → Extracting stored data, decrypting weak crypto
- Best Practices → Secure storage (Keystore, AES-256)
- **Tools → Frida, MobSF, SQLCipher, CyberChef**

**Final Project: MSTG Labs (OWASP Crackmes)**

**Project: Hands-on practice with OWASP Mobile Security Testing Guide (MSTG) Labs**

**Repo: OWASP Crackmes**

- Objectives:
- Reverse engineer Android apps with weak cryptography, insecure storage, and obfuscation issues
- Perform binary analysis, tampering, and debugging with Frida, JADX, and Objection
- Solve different CrackMe challenges to strengthen Android pentesting skills

**Required Tools:**

**JADX, APKTool (Reverse Engineering)**
**Frida, Objection (Runtime Exploitation)**
**MobSF (Automated Analysis)**
**Burp Suite (API Security Testing)**

**Approach: 1**

- **Select different CrackMe challenges from MSTG Labs 2**
- **Perform static & dynamic analysis on each app 3**
- **Modify or bypass security mechanisms (anti-debugging, root detection, weak encryption)**
- **Document findings & remediations as a report**

After completing the Mobile App Testing
You're eligible to do:

- Mobile App QA Engineer / Tester
- Mobile Application Security Testing
- Performance and Load Testing of Mobile Apps
- Functional and UI Testing for Android and iOS apps
- Automated Testing


# What is a API TESTING?

The API with AI Course is a specialized training program that focuses on designing, developing, and securing APIs (Application Programming Interfaces) while integrating Artificial Intelligence (AI) technologies. This course covers the fundamentals of API creation, including RESTful APIs, authentication, and security, along with how to use AI to enhance API functionality—such as enabling smart data processing, predictive analytics, and automation.

Learners also explore how AI can be used for API testing, monitoring, and optimization, ensuring faster and more intelligent workflows. It's ideal for developers, data scientists, and security professionals who want to build intelligent and secure API-driven applications.

**API Powered by AI**

**Course Outline**

## Module 01 Introduction

- Purpose and Objectives .....
- Scope and Audience.....
- Methodology and Research Approach .....
- Document Organization ....

## Module 02 Background and Context

- Overview of API Security .....
- Evolution of API Threats .....
- Importance of API Security in Modern Applications .....
- Key Terminologies and Concepts .....

## Module 03 OWASP API Security Top 10 – 2023

- Introduction to the OWASP API Security Project .....
- Comparison with Previous OWASP Top 10 Editions.....
- Criteria for Risk Ranking and Assessment .....

## Module 04 Detailed Analysis of OWASP API Security Top 10 – 2023 Risks

### 4.1 API1:2023 – Broken Object Level Authorization .....

- Description and Background .....
- Common Attack Vectors and Examples .....
- Impact Analysis.....

### 4.2 API2:2023 – Broken Authentication .....

- Description and Background .....
- Real-World Examples and Attack Scenarios .....
- Impact and Consequences .....
- Mitigation Best Practices .....

### 4.3 API3:2023 – Broken Object Property Level Authorization .....

- Description and Overview .....
- Data Exposure Risks and Case Studies .....
- Impact Analysis.....
- Strategies for Data Minimization and Protection.....

**Course Outline**

## 4.4 API4:2023 – Unrestricted Resource Consumption .....

- Description and Context .....
- Scenarios and Impact on Availability .....
- Mitigation Techniques and Best Practices .....

## 4.5 API5:2023 – Broken Function Level Authorization .....

- Description and Examples .....
- Analysis of Authorization Flaws .....
- Impact Assessment .....
- Recommended Security Controls .....

## 4.6 API6:2023 – Unrestricted Access to Sensitive Business Flows .....

- Description and Background .....
- Vulnerability Exploitation Techniques .....
- Impact and Case Examples .....
- Mitigation and Prevention Strategies .....

## 4.7 API7:2023 – Server-Side Request Forgery .....

- Description and Common Scenarios .....
- Analysis of Misconfiguration Risks .....
- Impact on API Security .....
- Best Practices for Secure Configuration .....

## 4.8 API8:2023 – Security Misconfiguration .....

- Description and Types of Injection Attacks .....
- Examples and Real-World Incidents .....
- Impact Analysis.....
- Mitigation Techniques .....

## 4.9 API9:2023 – Improper Inventory Management.....

- Description and Scope .....
- Identifying and Managing API Endpoints.....
- Impact and Risk Analysis .....
- Strategies for Effective Asset Management .....

## 4.10 API10:2023 – Unsafe Consumption of APIs .....

- Description and Background .....
- Analysis of Logging and Monitoring Gaps .....
- Impact on Incident Detection and Response .....
- Best Practices for Logging, Monitoring, and Alerting .....

## Course Outline

### Module 05 API Security Testing and Assessment .....

- Vulnerability Assessment Techniques .....
- Penetration Testing Methodologies .....
- Tools and Frameworks for API Security Testing .....
- Continuous Monitoring and Automated Testing Approaches.....

### Module 06 Best Practices and Mitigation Strategies .....

- Secure API Design Principles .....
- Authentication and Authorization Controls .....
- Input Validation and Data Sanitization .....
- Error Handling and Response Management .....
- Deployment and Configuration Best Practices .....
- Monitoring, Logging, and Incident Response .....

### Module 07 Case Studies and Real-World Examples.....

- Analysis of Notable API Breaches .....
- Lessons Learned from Past Incidents .....
- Application of OWASP Recommendations in Practice .....

### Module 08 Emerging Trends and Future Directions .....

- Evolving Threat Landscape for APIs .....
- Innovations in API Security Technologies .....
- Predictions and Future Challenges .....

### Module 09 Conclusion .....

- Summary of Key Findings .....
- Recommendations for Stakeholders .....
- Final Thoughts .....

### Module 10 References .....

- Bibliography of Sources .....
- Further Reading and Resources .....

### Module 11 Appendices .....

- Glossary of Terms .....
- Additional Tools and Checklists .....
- Contact Information and Support Channels .....


**After completing the API Testing**
**You're eligible to do:**

- Conduct Performance and Load Testing on APIs
- Validate API Security, Authentication, and Authorization (OAuth, JWT)
- Automate API Testing
- Perform Functional and Non-Functional Testing of APIs
- API Tester / QA Engineer


# What is a Source Code Review 🔐 course?

Source Code Review is a detailed analysis of an application's source code to identify security vulnerabilities, coding errors, and potential flaws. It ensures that the code follows secure coding practices and is free from common security issues like SQL Injection, Cross-Site Scripting (XSS), insecure authentication, and more. The process can be manual, where security experts or developers review the code line by line, or automated, using specialized tools like SonarQube, Fortify, or Checkmarx. Source Code Review helps detect vulnerabilities early in the development cycle, reducing the risk of exploitation in production. It also improves the overall quality, maintainability, and security of the application, making it a crucial part of the Secure Software Development Lifecycle (SSDLC).

Source Code Review Powered by AI

# Get the AI edge with 10 Power-packed Modules of the Source Code Review

## Course Outline

### Introduction to Source CODE Reviw

- Identifies Security Flaws – Detects vulnerabilities, bugs, and coding errors before deployment.
- Enhances Code Quality – Improves security, performance, and compliance with industry standards

### Module 01 Understanding Security, Threats and Attacks

- What is secure application
- Need for secure application
- Most common application attacks:-
  a) SQL injection attack
  b) Cross site scripting attacks
  c) Parameter tampering
  d) Directory traversal
  e) Cross-site Request Forgery(CSRF)
- Session Attack
- Why application become vulnerable to attacks
- Common reasons for existence of application vulnerabilities
- Improper input validation
- Insufficient Transport Layer Protection
- 3W's in application security
- Functional vs Security Activities in DSLC
- Software Security Standards, Models and Frameworks

### Module 02 Security Requirements Gathering

- Importance of Gathering Security Requirements
- Security Requirement Engineering
- Abuse Case and Security Use Case Modeling
- Abuser and Security Stories
- Security Quality Requirements Engineering
- Operationally Critical Threat, Assest and Vulnerability Evaluation

### Module 03 Secure Application Design and Architecture

- Relative Cost of Fixing Vulnerabilities at Different Phases of SDLC
- Secure Application Design and Architecture
- Goal of Secure Design Process
- Secure Design Actions
- Secure Design Principles
- Threat Modelling
- Decompose Application

a) Prepare and Document Threat Model Information
b) Identify the external dependencies
c) Identify the Trust Levels
d) Perform application Modelling using Data Flow Diagrams
e) Determine the Threats: Create a Security Profile

- Secure Application Architecture

## Module 04 Secure Coding Practices for input Validation

- Input Validation Pattern
- Validation and Security Issues
- Impact of invalid Data input
- Data validation techniques
- Input validation using Frameworks and APIs
- Servlet Filters
- Validation filter for Servlet
- Data validation using OWASP ESAPI
- Data Validation : Struts Framework
- Data Validation : Spring Framework
- Input Validation Errors
- Common Secure Coding Practices

## Module 05 Secure Coding Practices for Authentication and Authorization

- Introduction to Authentication
- Types of Authentication
- Authentication Weaknesses and Prevention
- Introduction to Authorization
- Access Control Model
- EJB Authorization
- Java Authentication and Authorization
- Java EE Security
- Authorization Common Mistakes and Countermeasures
- Authentication and Authorization in Spring Security Framework
- Defensive Coding Practises against Broken Authentication and Authorization
- Secure Development Checklists: Broken Authentication and Session Management

## Module 06 Secure Coding Practices for Cryptography

- Java Cryptography
- Encryption and Secret Keys
- Ciper Class
- Digital Signature
- Secure Socket Layer
- Key Management
- Digital Certificates
- Signed Code Sources
- Hashing
- Java Card Cryptography
- Spring Security: Crypto Module
- DO’s and Don’ts in Java Cryptography
- Best Practices for Java Cryptography

## Module 07 Secure Coding Practices for Session Management

- Session Management
- Session tracking
- Session management in Spring Security
  a) Spring Session Management
  b) Session Management using Spring Security
  c) Controlling Session Timeout
  d) Prevent using URL parameter for session tracking
  e) Prevent session fixation with Spring Security
  f) Use SSL for Secure Connection
- Session Vulnerabilities and their Mitigation Techniques
- Session Vulnerabilities
- Types of Session Hijacking Attacks
- Best Practices and Guidelines for Secured Session Management

## Module 08 Secure Coding Practices for Error Handling

- Introduction to Exceptions
- Erroneous Exceptional Behaviours
  a) Disclosing Sensitive Information
  b) Logging Sensitive Data
- Do's and Don'ts in Error Handling
- Spring MVC Error Handling
- Exception Handling in Struts 2
- Best Practices for Error Handling
- Introduction to logging
- Logging using Log4j
- Secure coding in Logging
- Secured Practices in Logging

## Module 09 Static and Dynamic Application Security Testing

- Static Application Security Testing
- Why SAST
- Skills required for SAST
- Types of SAST
- SAST Steps
- SAST Activities: flow chart
- SAST Deliverable
- Manual Secure Code Review for most Common Vulnerabilities
- Code Review for PCI DSS Compliance
- Code Review for Client-side validation approach
- Code Review for Weak Password Authentication
- Code Review for Hard-Coded Passwords
- Code Review for Empty Password in Connection String
- Code Review for Insecure LDAP Authentication
- Code Review for Insecure Authorization
- Code Review for insecure file upload
- Code review for Sensitive Information Exposure
- Code Review for Sensitive Information Leakage
- Code Review : Check List Approach
- Proxy-based Security Testing Tools: burp suite, owasp zap proxy

## Module 10 Secure Deployment and Maintenance

- Secure Deployment
- Prior Deployment Activity
- Deployment Activities: Ensuring Security at various levels
- Ensuring Security at Host Level
- Ensuring Security at Network Level
- Ensuring Security at Application Level
- Ensuring Security at Web Container Level
- Role based Security
- Securing Tomcat at Network Level
- Tomcat Security Setting
- Verify maxPostSize Setting
- Tomcat Security Checklist
- Ensuring Security in Oracle
- Security Maintenance and Monitoring

**After completing the Source Code Review**
**You're eligible to do:**

- Source Code Reviewer
- Application Security Analyst
- Secure Code Auditor
- Penetration Tester with Code Review Expertise
- Cybersecurity Consultant
- Security Software Developer
- VAPT (Vulnerability Assessment and Penetration Testing) Specialist
- DevSecOps Engineer


# What is a SC-900 Course ?

The SC-900 course, also known as Microsoft Security, Compliance, and Identity Fundamentals**,** is an entry-level certification focused on the basics of Microsoft's security solutions. It covers core concepts like identity and access management, compliance, and threat protection. The course introduces Microsoft Entra (Azure Active Directory), Microsoft Defender, Microsoft Purview, and Microsoft Sentinel.

SC-900 explains key principles such as Zero Trust security, defense in depth, and shared responsibility models in cloud environments. It is designed for beginners, IT professionals, and business stakeholders who want to understand Microsoft's security ecosystem. No prior technical knowledge is required.

Completing SC-900 helps you prepare for roles in security administration, compliance, and identity management, and serves as a foundation for advanced Microsoft security certifications.

# SC - 900 Powered by AI

## Get the AI edge with 05 Power-packed Modules of the SC-900

**Course Outline**

### Introduction to SC - 900

- **SC-900 Overview – Microsoft's fundamental certification on security, compliance, and identity concepts.**
- **Importance – Helps beginners understand Microsoft security solutions and compliance frameworks.**

### Module 01 Introduction to SC-900

- Overview of the certification
- Who should take this exam?
- Exam details (format, duration, passing score)
- Describe the Concepts of Security, Compliance, and Identity

### Module 02 Security Requirements Gathering

- Basic security principles
- Zero Trust model
- Shared responsibility model
- Authentication vs. Authorization
- Identity providers and directory services
- Describe the Capabilities of Microsoft Entra ID

### Module 03 Microsoft Entra ID

- Overview of Microsoft Entra ID (formerly Azure AD)
- Authentication methods (MFA, SSO, Conditional Access)
- Identity protection and access management
- Governance features (Privileged Identity Management - PIM)
- Describe the Capabilities of Microsoft Security Solutions

### Module 03 SMicrosoft Defender

- Microsoft Defender suite (Defender for Endpoint, Defender for Cloud, etc.)
- Microsoft Sentinel (SIEM & SOAR)
- Microsoft Purview Compliance solutions
- Threat protection and security monitoring
- Describe the Capabilities of Microsoft Compliance Solutions

### Module 04 Microsoft Purview Information Protection

- Microsoft Purview Information Protection (DLP, sensitivity labels)
- Insider risk management and audit capabilities
- Compliance Manager and regulatory compliance features
- Data governance and eDiscovery
- Exam Preparation and Resources

### Module 05 Microsoft Learning

- Study materials and learning paths
- Practice tests and exam tips

**Useful Microsoft documentation**

**After completing the SC-900**
**You're eligible to do:**

- Security Software Developer
- Cybersecurity Consultant
- Penetration Tester with Code Review Expertise
- Secure Code Auditor
- Application Security Analyst
- Source Code Reviewer


# What is a ISO -27001 Course ?

The ISO 27001 course provides comprehensive training on the international standard for Information Security Management Systems (ISMS). ISO 27001 outlines best practices for managing sensitive company data, ensuring confidentiality, integrity, and availability. The course teaches you how to implement, manage, and continually improve an ISMS within an organization. You'll learn about risk assessment, risk treatment plans, security policies, and controls based on the standard's framework. It covers compliance requirements, audits, and how to maintain certification. The training is ideal for IT managers, security professionals, auditors, and anyone responsible for safeguarding information assets. By completing this course, you'll be equipped to help organizations minimize security risks, protect data, and ensure regulatory compliance.

ISO -27001 Powered by AI

# Get the AI edge with 09 Power-packed Modules of the ISO -27001

**Course Outline** | **Organizational Controls**

## Module 01 Governance & Risk Management Controls

- Information Security Governance – Establishing a governance framework for security policies.
- Risk Management – Identifying, assessing, and mitigating risks.
- Compliance Management – Ensuring adherence to regulations like GDPR, HIPAA, etc.
- Security Policies and Procedures – Defining and enforcing security policies.
- Roles and Responsibilities – Assigning security responsibilities within the organization.
- Third-Party Risk Management – Assessing risks from vendors and suppliers.
- Business Continuity and Disaster Recovery (BCDR) – Ensuring resilience against disruptions.
- Asset Management – Inventory and classification of organizational assets.
- Change Management – Managing changes to systems and processes securely.

## Module 02 Part-1 Human Resources Security Controls

- Background Checks – Conducting pre-employment screening.
- Security Awareness Training – Training employees on security best practices.
- Onboarding and Offboarding Processes – Ensuring secure employee transitions.
- Code of Conduct and Ethics – Establishing ethical behavior expectations.
- Incident Reporting and Whistleblower Protection – Encouraging responsible disclosure.

## Part- 2 Access Control & Identity Management

- Access Control Policy – Defining access privileges and principles (e.g., least privilege).
- Multi-Factor Authentication (MFA) – Strengthening authentication processes.
- Role-Based Access Control (RBAC) – Assigning access based on job roles.
- Privileged Access Management (PAM) – Controlling admin-level access.
- User Account Management – Creating, maintaining, and disabling accounts securely.

## Module 03 Part -1 Incident Response & Security Monitoring

- Incident Response Plan (IRP) – Defining steps for handling security incidents.
- Security Operations Center (SOC) – Monitoring and responding to threats.
- Threat Intelligence and Monitoring – Gathering and analyzing threat data.
- Forensic Investigation Procedures – Conducting post-incident investigations.
- Security Logging and Auditing – Maintaining logs for security events.

## Part- 2 Legal & Compliance Controls

- Data Protection and Privacy Compliance – Adhering to laws like GDPR, CCPA, HIPAA.
- Intellectual Property Protection – Safeguarding proprietary information.
- Contract and Vendor Security Requirements – Enforcing security clauses in agreements.
- Audit and Compliance Reviews – Conducting periodic security audits.
- Regulatory Reporting – Reporting incidents and compliance status to authorities.

## Module 04 Insufficient Input/Output Validation

- Secure Software Development Lifecycle (SDLC) – Integrating security in development.
- Vulnerability Management – Identifying and remediating security weaknesses.
- Penetration Testing and Red Teaming – Proactively testing security defenses.
- Network Security and Segmentation – Isolating critical network assets.
- Secure Configuration Management – Enforcing secure settings on systems.
- Data Encryption and Key Management – Protecting sensitive data in transit and at rest.
- Cloud Security Management – Applying security measures to cloud environments.
- Backup and Recovery Management – Ensuring data integrity through backups.

## People Controls

**Module 05**

- Security Awareness and Training
- Background Checks and Screening
- Role-Based Security Responsibilities
- Onboarding and Offboarding Processes.
- Insider Threat Management
- Code of Conduct and Ethical Behavior
- Incident Reporting and Whistleblower Protection
- Continuous Monitoring and Performance Reviews

**EXAM , ASSIGNMENT**

## Part - 3 Physical control

**Module 06 Human Resources Security Controls**

- Perimeter Security
- Security Guards and Patrols
- Surveillance Systems (CCTV)
- Access Control Systems.
- Visitor Management System
- Alarm Systems
- Security Lighting
- Secure Doors and Locks
- Environmental Controls
- Secure Equipment and Device Storage
- Physical Security Policies and Procedures
- Asset Tagging and Inventory Management
- Backup Power and Redundancy Systems
- Data Center and Server Room Security

## Technological Controls

**Module 07 Part -1 Access Control & Identity Management**

- Multi-Factor Authentication (MFA) – Requiring multiple forms of authentication for secure access.
- Single Sign-On (SSO) – Allowing users to authenticate once for multiple systems.
- Role-Based Access Control (RBAC) – Granting permissions based on job roles.
- Privileged Access Management (PAM) – Managing and restricting high-level access.
- Identity and Access Management (IAM) – Centralized control of user identities.
- Account Lockout and Session Management – Preventing brute-force attacks.
- Biometric Authentication – Using fingerprints, facial recognition, or other biometric factors

**Part -2 Network Security Controls**

- Firewalls (Next-Gen & Traditional) – Filtering network traffic for threats.
- Intrusion Detection & Prevention Systems (IDS/IPS) – Monitoring and blocking malicious activity.
- Virtual Private Network (VPN) – Securing remote connections.
- Network Segmentation – Isolating systems to limit the spread of threats.
- Zero Trust Network Access (ZTNA) – Enforcing least-privilege access on networks.
- Network Access Control (NAC) – Ensuring only authorized devices connect to networks

## Part -3 Endpoint & Device Security

- Endpoint Detection and Response (EDR) – Detecting and responding to endpoint threats.
- Mobile Device Management (MDM) – Securing mobile devices used in business environments.
- Antivirus and Anti-Malware Software – Detecting and removing malicious software.
- USB and Removable Media Controls – Restricting unauthorized devices.
- Application Whitelisting and Blacklisting – Controlling allowed software execution

## Part - 4 Data Security Controls

- Data Encryption (At Rest & In Transit) – Protecting sensitive information using cryptographic techniques.
- Data Loss Prevention (DLP) – Preventing unauthorized data transfers.
- Secure File Transfer Protocols (SFTP, HTTPS, TLS/SSL) – Ensuring encrypted data transmissions.
- Data Masking & Tokenization – Hiding sensitive information for security purposes.
- Database Security Measures – Implementing access controls and encryption for databases.

## Part -5 Application Security Controls

- Secure Software Development Lifecycle (SDLC) – Integrating security into the development process.
- Web Application Firewalls (WAF) – Protecting applications from web-based attacks.
- Static and Dynamic Application Security Testing (SAST/DAST) – Identifying vulnerabilities in applications.
- .API Security Management – Protecting APIs against unauthorized access and misuse.
- Patch and Vulnerability Management – Ensuring timely updates and remediation of security flaws.

## Module 08 Application Security Controls

- Secure Software Development Lifecycle (SDLC) – Integrating security into the development process.
- Web Application Firewalls (WAF) – Protecting applications from web-based attacks.
- Static and Dynamic Application Security Testing (SAST/DAST) – Identifying vulnerabilities in applications.
- API Security Management – Protecting APIs against unauthorized access and misuse.
- Patch and Vulnerability Management – Ensuring timely updates and remediation of security flaws.

## Module 09 Logging, Monitoring & Threat Detection

- Security Information and Event Management (SIEM) – Aggregating and analyzing security logs.
- Threat Intelligence Platforms (TIP) – Gathering and analyzing threat data.
- User and Entity Behavior Analytics (UEBA) – Detecting anomalies in user behavior.
- Automated Incident Response & Orchestration (SOAR) – Automating security workflows.
- Cloud Security Posture Management (CSPM) – Ensuring security compliance in cloud environments.
- Automated Backups and Recovery Solutions – Ensuring data integrity and availability in case of incidents.

**FINAL EXAM**
**ASSIGNMENT**
**Write & Publish 1 Research Paper in every Subject**

# After completing the **ISO -27001** course ?
# You’re eligible to do:

- Information Security Analyst
- ISO 27001 Lead Auditor
- Information Security Manager
- Compliance Officer
- Risk Analyst/Manager
- IT Security Consultant
- Data Protection Officer (DPO)

# Note for Academy students :

✅ Trainer Availability: Trainers may be changed based on availability.

✅ Training Timings: Class timings may fluctuate between 7 PM to 10 PM due to technical issues or trainer availability.

✅ Special Sessions: Tapan Sir and Riddhi Ma'am will not take regular classes, but a special session will be arranged with them once a month.

✅ Course Updates: Courses will be updated regularly to align with real-world requirements.

✅ Student Responsibilities:

➡ Ensure regular attendance in classes.

➡ Attend Parent-Teacher Meetings (PTM).

➡ Submit feedback forms, tests, and assignments on time.

✅ CLASS RECORDING WILL UPLOAD BETWEEN 12 TO 2 PM

---

## 📌 Class Timings & Schedule Policy

🕐 Regular Class Timings:

Classes will be held between 7:00 PM to 10:00 PM.

🔁 Backup / Revision Classes:

These will be conducted by an alternate trainer when needed.

🔄 Timing Flexibility:

Class timings may fluctuate based on trainer availability.

🚫 No Time Customization:

The academy will not be liable to change class timings based on individual preferences.

📅 Trainer-Dependent Scheduling:

Any changes in schedule will occur only if the assigned trainer is unavailable

# ACADEMY CERTIFICATES

## DIPLOMA CERTIFICATES

# ACADEMY CERTIFICATES

## PROCTORED CERTIFICATES

# OUR CERTIFICATES

ISO 9001

ISO 9001 sets out the criteria for a quality management system and is the only standard in the family that can be certified to (although this is not a requirement).

ISO 27001

ISO 27001 is widely known, providing requirements for an information security management system.

iStart Rajasthan is a flagship initiative by the Government of Rajasthan, intended to foster innovation, create jobs, and facilitate investment.

Startup India: A flagship initiative by the Government of India to empower startups, drive innovation, and build a robust entrepreneurial ecosystem.

DPIIT: Promoting industrial growth, entrepreneurship, and policies for India's economic development.

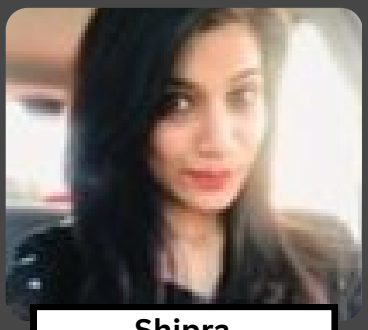
MSME: Micro, Small, and Medium Enterprises drive innovation, create jobs, and play a vital role in India's economic growth and self-reliance.

# OUR PLACEMENTS

Abhishek
3.5 Lakhs P.A

Lukman Nadaf
3.2 Lakhs P.A

Abhinav
18.5 Lakhs P.A



Shipra
7 Lakhs P.A

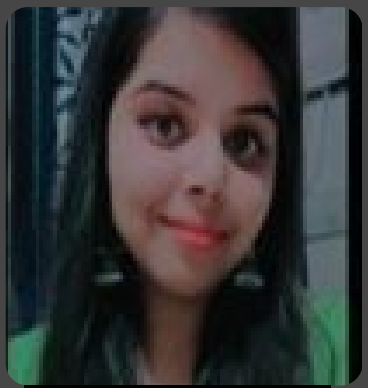
Neeraj
5 Lakhs P.A

Japneet
7.5 Lakhs P.A

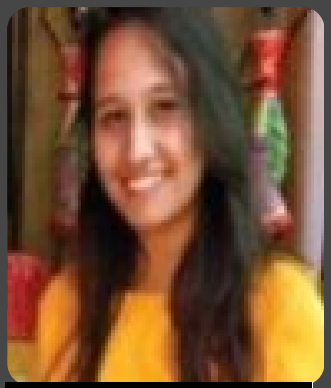
Sorabh Mishra
2 Lakhs P.A

Nistha
5 Lakhs P.A

Mohit Pandey
8 Lakhs P.A



Samraddhi
7 Lakhs P.A



Sheetal
4.5 Lakhs P.A

# COMPANIES WE WORK WITH

BIBA, India

Himalaya, India

**Reel Cinema Dubai**

**Emmar, UAE**

**Realme**

**OPPO**

**LEGO**

**OLA**

# COMPANIES REGISTERED WITH

ISO 9001

ISO 9001 sets out the criteria for a quality management system and is the only standard in the family that can be certified to (although this is not a requirement).

ISO 27001

ISO 27001 is widely known, providing requirements for an information security management system.

iStart Rajasthan is a flagship initiative by the Government of Rajasthan, intended to foster innovation, create jobs, and facilitate investment.

Startup India: A flagship initiative by the Government of India to empower startups, drive innovation, and build a robust entrepreneurial ecosystem.

DPIIT: Promoting industrial growth, entrepreneurship, and policies for India's economic development.

MSME: Micro, Small, and Medium Enterprises drive innovation, create jobs, and play a vital role in India's economic growth and self-reliance.

# NEWS CUTTINGS

## साइबर क्राईम को अब एएसडी एकेडमी सुलझाएगी

साइबर

इनका कहना है







## 12 साल के छात्र ने बनाया इंडिया की सोशल नेटवर्किंग साइट

कोटा। दादाबाड़ी की एसडी अकादमी में पढ़ने वाले पहले सेमस्टर के छात्र राहुल चौधरी (प्रोहित नगर एक्सटेंशन कोटा) और ईशान उपाध्याय ने फ्रेंड्स नेटवर्क नामक सोशल नेटवर्किंग साइट बनाई है।

इस वेबसाइट के जरिए लोग अपने फ्रेंड्स से जुड़ सकते है। जिससे फ्रेंड्स रिकवेस्ट भेज सकते है, मैसेज कर सकते है, इमेज अपलोड कर सकते है। इसका मैनेजमेंट मंसूर अली, मोहम्मद अमन, हिमांशु मुगोत संभाल रहे है। मीडीया और प्रमोशन डिपार्टमेंट शकि सिंह ओर फरहान एहमद, संस्कार अग्रवाल संभाल रहे है।

नया फेसबक से करने वाले सारे वेबसाइट की सिक्योरिटी International Cyber Security Experts स्वयं अपनी एसडी साइबर सिक्योरिटी टीम के साथ देख रहे है। एसडी अकादमी के स्टडेंटस ने सोशल मीडिया पर बढते अकाउंट बनाके कोई धोखाधडी ना कर सके।

**क्या है फ्रेंड्स नेटवर्क?**

यह एक सोशल मीडिया प्लेटफॉर्म है जिससे फेसबुक जैसा सारा कार्य किया जा सकता है। इस में ...

## भास्कर एक्सपर्ट व्यू

कोटा के साइबर एक्सपर्ट तपन झा का कहना है कि हाल में हुए साइबर अटैक का अभी कोई हल नहीं है। जागरूकता ही बचाव है।

**डाटा बैकअप लें :** बिना देर किए सभी फाइलों का एक अलग सिस्टम में बैकअप ले लें। ध्यान रहे कि यह बैकअप एक्सटर्नल हार्ड डिस्क में ही लें व कम्प्यूटर से दूर रखें।

**एंटीवायरस का इस्तेमाल :** विश्वसनीय एंटीवायरस का इस्तेमाल करें। एंटी वायरस कभी भी वेबसाइट से डाउनलोड न करें क्योंकि वे खुद ही वायरस होते हैं।

**ईमेल पर निगरानी :** फर्जी ईमेल्स, प्रलोभन वाले विज्ञापन और अनवेरिफाइड एप्स का इस्तेमाल व क्लिक करने से बचें।

**अपडेट्स इंस्टॉल करें :** सॉफ्टवेयर को अपडेट रखें।

झालावाड़, पिड़ावा, भवानीमंडी, डग, रामगंजमंडी, मोडक की खबरें

कोटा में आरी 'प्राइवेट कंप्यूटर फॉरेंसिक लैब'

## 3 घंटे में सॉल्व किया अंतर्राष्ट्रीय साइबर अपराध

(विशेष संवाददाता)

कोटा। ऐ.एस.डी साइबर सिक्योरिटी कंसल्टेंट इग्रा, कोटा ने शुरू हुई कंप्यूटर सम्बन्धित फोरेंसिक लेब। इस लेब मे कंप्यूटर सम्बन्धित होने वाले सभी क्राइम को जल्द से जल्द रोका जा सकता है। ये लेब इंटरनेट क्राइम, ऑनलाइन ट्रैकिंग, कम्प्यूटर फॉरेंसिक, डाटा रिकवरी, डिजिटल एविडेंस कलेक्शन जैसे सभी कार्य करने में निपुण है। अभी इस फोरेंसिक लेब में 5 फोरेंसिक इन्वेस्टिगेटर ,3 लॉयर है। खास बात यह है की इसमें कार्य कर रहे सभी इन्वेस्टिगेटर यू. ए. से. अमेरिका की ई.सी- कौंसिल आर्गेनाइजेशन से सर्टिफाइड है। कंप्यूटर फोरेंसिक और एथिकल हैकिंग में यह लेब पूरे राजस्थान राज्य में सर्विस देने के लिए बनाई गयी है। किसी भी जिले की पुलिस को ऐ.एस.डी फोरेंसिक लेब की सहायता चाहये केस को सलिव करने लिए है तो केस को सलिव करने के लिए लिखित में उस जिले के ऐ.एस .पी से आज्ञा लिखनी होती है। फोरेंसिक लेब उसके बाद कंप्यूटर सम्बन्धित सभी जानकारी इकट्ठी करके उन्हें जल्द से जल्द प्रदान करती है। एक दिन पहले विक्रान नगर पुलिस स्टेशन में दर्ज हुए ईमेल फ्रॉड को लेकर विक्रान नगर पुलिस स्टेशन ने फोरेंसिक लेब की सहायता ली और 3 घंटे में ईमेल फ्रॉड केस को सॉल्व कर दिखाया।

इस केस को इंटरनेशनल साइबर क्राइम इन्वेस्टिगेटर तपन कुमार झा और साइबर क्राइम कंसल्टेंट रिद्धि सोरल अपनी टीम मंसूर अली, अमन चेतनीय के साथ देख रहे थे। इन्वेस्टिगेटर तपन कुमार झा का कहना है की ऐसा पहली बार हुआ है की कोटा के जानेमाने हस्ती पर साइबर अटैक किया गया है वो भी इंडिया के बाहर से हैकर का नकाबद्द था उसके ईमेल में रखी जानकारी चुराना, और उसके ईमेल में बैकडोर बनाकर छेड़ देना ताकि पासवर्ड चेंज करने के बाद भी ईमेल पर हैकर का कन्ट्रोल रहे पर इस केस को बड़ी गंभीरता से लेते हुए हमारी टीम ने 3 घंटे में उस बैकडोर को ढूंढ कर हटा दिया और ईमेल को रिकवर कर दिया। इसमें जरूरी है की हम हमारी सिक्योरिटी पहले से रखे, ताकि हैक होने खतरा बिलकुल नहीं हो इसके लिए हमने एक सेवा शुरू की है जिसके द्वारा आप कॉल करके अपने आपको कैसे सुरक्षित रखना है उसकी जानकारी ले सकते है। इस लिए आपको +91 - 9680100687 पर कॉल करना होगा। उसके बाद हमारी फोरेंसिक लेब आपको पूरी जानकारी देगी। पुलिस या किसी और सर्विस एजेंसी को फोरेंसिक लेब सहायता चाहये। तो ऐ.एस.डी.एन साइबरसेक्योरिटी प्राइवेट लिमिटेड 1-ए, 16, प्रथम फ्लोर अर्बेजिंद कृष्णानी दादाबाड़ी कोटा (91 -9680100687) पर संपर्क कर सकते है।

धुळे मैदान

## राष्ट्रीय सायबर कॉन्फरन्समध्ये अॅड.भंडारी यांची निवड

धुळे । येत्या ४ फेब्रुवारी रोजी नाशिक येथे होणाऱ्या भारतातील राष्ट्रीय कॉन्फरन्सच्या प्रमुख वक्ते म्हणून धूळे येथील सायबर तज्ञ अॅड.चैतन्य भंडारी यांची निवड झाली आहे.

यात भारतभरातून विविध शाळा, महाविद्यालयातील विद्यार्थी गण उपस्थित राहणार असून त्यांना भारतातून विविध सायबर तज्ञांचे मार्गदर्शन लाभणार आहे. यात अॅड. भंडारी हे प्रमुख वक्ते म्हणून भूमिका मांडणार आहे. सदरील राष्ट्रीय सायबर सेक्युरिटी कॉन्फरन्स, नाशिक चॅप्टरचे आयोजक स्वरदा करवनूरकर (व्हाईट बॅण्ड असोसिएट्स) यांनी आयोजित केली आहे. सदरील राष्ट्रीय कॉन्फरन्स येथे श्री. तपनकुमार झा, रिध्दी सोरल व दीपक राज राव, दिल्ली हे या सायबर तज्ञांचा देखील समावेश असणार आहे. सदरील एकदिवसीय राष्ट्रीय कॉन्फरन्स मध्ये संपूर्ण भारतातून आलेल्या विदयार्थी, डॉक्टर, इंजिनिअर्स, शिक्षक तसेच सर्वसामान्य नागरीकांना अॅड. भंडारी हे मार्गदर्शन करणार आहे. नागरीकांनी मोठया संख्येने या राष्ट्रीय कॉन्फरन्स मध्ये उपस्थित राहन सायबर सुरक्षिततेसंबंधी जागरुक रहावे.

## 12-yr-old rolls out Indian version of 'Facebook'

Rajiv Saxena @jaipur.tnn

Kota: A 12-year-old school student conceptualised the idea of the Indian version of social networking site Facebook and with assistance from three seniors, he came up the Friends Networking site that allows registration of only Indians.

The four also ensured complete security of user data. In the first two days of launch, over a one hundred people have joined the networking site with around 30 users turning out to be 'fake'.

Rahul Chowdhary, a class 9 student, proposed around a year ago, the idea of developing Indian version of Facebook. He had a team comprising Riddhi Soral, an engineering graduate of Rajasthan Technical University and security developer, Ishan Upadhyay, a class 10 student who carried out research on developing an Indian version of Facebook and Tapan Kumar Jha, who is an engineering graduate and a cyber security expert who heads the four-member team.

The application is similar to Facebook and other chatting sites but it is safer and secure on users account with zero possibility of fake ID users. The user account on the site is activated not instantly but after eight hours through manual verification decreasing the possibility of a fake ID account, Jha said adding that users here cannot create multiple accounts with the same ID or mobile number.

Friends Networking site also has a mobile app of only 2.5 MB, which can be used with any small version of a cellphone. One is not required to have an expensive mobile phone to use the application but it can be used in an ordinary mobile phone also, he said. The site provides features like finding local friends, sending friend request, messaging, chatting, photo sharing, likes and comments, profile picture and cover image.

ALSO MOBILE APP

- Friends Networking site also has a mobile app of only 2.5 MB, which can be used with any small version of a cellphone. One is not required to have an expensive mobile phone to use the application but it can be used in an ordinary mobile phone also.

## कोटा के साइबर दंपती राजस्थान पुलिस व मुंबई क्राइम ब्रांच के भी मददगार, इन्हीं ने खोला था मॉडल मानसी मर्डर केस

एजुकेशन रिपोर्टर | कोटा

टा के तपन झा और पत्नी रिद्धि रल साइबर सिक्योरिटी एक्सपर्ट कई मुश्किल केस हल करने मंबई क्राइम ब्रांच, अन्य पुलिस एजेंसियों की इन्होंने मदद की। देशों में भी कंपनियों के लिए डाटा वेसी रोकने के लिए सॉफ्टवेयर ल्प किए हैं। राजस्थान सरकार र पुलिस को निःशुल्क सेवा हैं। करीब 5 साल पहले मुंबई कोटा की मॉडल मानसी दीक्षित चर्चित मर्डर केस के खुलासे में का हाथ था। साायबर पुलिस को ग देते हैं।

तपन और रिद्धि

### इन केस में पुलिस की मदद

केस-1: झालावाड़ में पुलिस ने सवा 2 करोड़ का सट्टा पकड़ा था। सारा हिसाब-किताब ऑनलाइन था। पुलिस ने इनकी मदद ली।

केस-2: कोटा पुलिस ने सोशल मीडिया पर हथियार समेत पोस्ट डालने, हिस्ट्रीशीटर फॉलो करने वाले युवकों को इनकी मदद से ट्रेस किया।

### 17 लोगों की टीम, 50 लाख से अधिक का टर्नओवर

तपन झा ने राज्य सरकार से स्टार्ट अप फंड के लिए अपलाई किया है। सरकार यदि इस स्टार्टअप को उपयोगी मानेगी तो 25 लाख का फंड देगी। सूचना प्रौद्योगिकी विभाग के मनोज मीना का कहना है कि आई स्टार्ट अप में एक माह पहले ही एसडी साइबर सिक्योरिटी कंपनी बनाकर रजिस्टर्ड हो चुके हैं। कंपनी में 17 लोग हैं। पिछले साल 50 लाख से अधिक टर्नओवर था। अब स्कूल में जाकर स्टूडेंट्स को साइबर जागरूक करते हैं।

**भास्कर नॉलेज : बिना अनुमति डाटा इस्तेमाल नहीं कर सकते**

नागरिकों के अपने डेटा सुरक्षित रखने के लिए तीन साल पहले डेटा प्रोटेक्शन बिल केंद्र सरकार लेकर आई थी। हालांकि, उस समय लागू नहीं हो पाया था। इस बिल में प्रावधान है कि किसी भी व्यक्ति या संस्था का डाटा बिना अनुमति से इस्तेमाल नहीं कर सकते। व्यक्ति को डेटा संरक्षण का अधिकार दिया गया था। इस्तेमाल करने पर दंडित करने व कार्रवाई करने का प्रावधान है।

जलपला महाराष्ट्र बुधवार ३१ जानेवारी २०२४

## राष्ट्रीय सायबर कॉन्फरन्समध्ये प्रमुख वक्ते म्हणून अॅड.भंडारी यांची निवड

धुळे, दि.३०- येत्या चार फेब्रुवारी रोजी नाशिक येथे होणाऱ्या भारतातील राष्ट्रीय कॉन्फरन्सच्या प्रमुख वक्ते म्हणून धूळे येथील सायबर तज्ञ अॅड.चैतन्य भंडारी यांची निवड झाली आहे.

यात भारतभरातून विविध शाळा, महाविद्यालयातील विद्यार्थी गण उपस्थित राहणार असून त्यांना भारतातून विविध सायबर तज्ञांचे मार्गदर्शन लाभणार आहे. यात अॅड.भंडारी हे प्रमुख वक्ते म्हणून भूमिका मांडणार आहे. सदरील राष्ट्रीय सायबर सेक्युरिटी कॉन्फरन्स, नाशिक चॅप्टरचे आयोजक असोसिएट्स) यांनी आयोजित केली आहे. सदरील राष्ट्रीय कॉन्फरन्स येथे तपनकुमार झा, रिध्दी सोरल व दीपक राज राव, दिल्ली हे या सायबर तज्ञांचा देखील समावेश असणार आहे. सदरील एकदिवसीय राष्ट्रीय कॉन्फरन्समध्ये संपूर्ण भारतातून आलेल्या विदयार्थी, डॉक्टर, इंजिनिअर्स, शिक्षक तसेच सर्वसामान्य नागरीकांना अॅड.भंडारी हे मार्गदर्शन करणार आहे.तसेच त्यांना सायबर सेक्युरिटी विषयी ज्ञान देणार आहे, म्हणून नागरीकांनी मोठया संख्येने या राष्ट्रीय कॉन्फरन्समध्ये उपस्थित राहन सायबर सुरक्षिततेसंबं ...ना करवनूरकर (व्हाईट बॅण्ड जागरुक रहावे.

# FOUNDER VISION

Earth to Sky - The role of ASD is evident in every minute of man's evolution for better living. ASD should be instrumental in shaping careers should be an intelligence incubator for potential research and should be a source of effective manpower for the nation's progress is synonymous with disciplined learning, dedication to working, and a destination for success. ASD offers three assurances for our students' Confidence, Character, and Career.


**Er. Tapan Kumar Jha**
**Founder & Director**

**Hacking is a talent. You won't learn it at school. It's like being Messi and Ronaldo if you are born to become a hacker, it's your destiny. Otherwise, you will hacked.**

# FOUNDER VISION

ASD Academy has a pyramidal model of development. This aims at the convergence of excellence in academic performance and Strengthening the core value system at the summit of Institutional success. This serves the dual purpose of building a solid foundation of ethical and technical background besides enriching the components of confidence, creativity, and innovation among the students. "True leaders do not just extend their authority. They share their ideas, and skills and create many more strong leaders to guide the Way". The campus imbibes this ideology in the work culture and Encourages proactive leadership at every level of our system. It is heart-warming to share that there are 25+ Companies visited us Last academic year and every student secured a job through our campus recruitment program. Our Milestones are unique, our references are our founder chancellor's vision, and our performance is to sustain the smiles of the students. We have a rich legacy to continue, we have a path to take further and we have the will to further.

**Er. Riddhi Soral**
**Founder & Director**

**Most Good Programmers Do Programming Not Because They Expect to Get Paid Or Get Adulation By the Public , But Because it is Fun to Code .**

Certified Cyber security Powered by AI

## Contact Us:


Website: www.asdacademy.in

Email: training@asdacademy.in

Phone: 8003534436 / 8233150687 / 7597214473

Hacker Vlog

Hacker Vlog Podcast

@hackervlogofficial / @hackervlog / @cyberexpert.riddhisoral


## Address:


Akansha Deep Heights, 18th Floor, No. 1841-1842, Kunadi, Kota, Rajasthan, Pin Code - 324008


www.asdacademy.in

SCAN ME

**ASD ACADEMY**
**India's Most Advanced Hacking & Coding Academy**

*Thank You*