For Details:
+91 9121307637

CYBER
ZIKSA

CYBER SECURITY

with AI

Introduction to Cybersecurity

- The evolution of Cybersecurity
- Cybersecurity & situational awareness
- The Cybersecurity skills gap
- Difference between Information Security & Cybersecurity Cybersecurity objectives
- Cybersecurity Roles

Understanding Devices and Infrastructure

- Infrastructure Terminology
- Designing with Security in Mind
- Network Topology
- OSI Layers & TCP/IP Model
- IPv4 & Ipv6
- Ports & protocols
- Port numbers
- Firewalls
- VPNs and VPN Concentrators
- Intrusion Detection Systems
- Router u Switch u Proxy
- Load Balancer
- Access Point
- Network Access Control (NAC)
- Mail Gateway
- Bridge

Ethical Hacking

- Introduction to CyberSecurity
- Introduction to Ethical hacking
- Computer & Networking Basics
- Lab setup for Virtual Machines
- Foot Print/Information Gathering
- Scanning
- Vulnerability Analysis
- Sniffing & Man-In-Middle
- System Hacking
- Metasploit Attacks
- Malware Threats
- Phishing Attacks
- Social Engineering Attacks
- Hacking webserver & Web Applications
- SQL Injection
- Wireless Attacks
- Firewalls u IDS/IPS
- Honeypots
- Cloud Computing
- IOT Hacking
- Cryptography
- Penetration Testing
- Identity Theft
- Security Compliances
- Steganography
- Risk Management
- Mobile Hacking
- DOS/DDOS Attacks
- Proxies & VPn's
- Computer Forensic
- OSIntframework
- Information Gathering with Maltego Tool
- DNS Spoofing
- MAC Spoofing
- Web Application with Nessus Vulnerability Scanner
- Kon Boot for password Breaking
- Countermeasures for Local Systems

Bugbounty

- Introduction to Bug Bounty
- Basic Terminology on Bug Bounty
- Information Gathering
- Lab setup for Bug Bounty
- Installation of Burp Suite Tool
- Bug Bounty Platforms
- Report Writing for Bugs
- Vulnerability Scanner Tools
- Web Application Vulnerabilities
- Cross Site Scripting
- Host Header Injection
- URL Redirection Attack
- Parameter Tampering
- File Upload Vulnerability
- SQL Injection
- Bypass Authentication
- Sensitive Information Disclosure Vulnerability
- CSRF Attack Vulnerability
- Word Press Sensitive information disclosure
- XML Vulnerability in Word Press Vulnerability
- Missing SPF Records vulnerability
- OTP Bypass Technique Vulnerability
- IDOR Vulnerability
- No rate Limit Vulnerability
- Session Hijacking Vulnerability
- Long Password Attack Vulnerability

Security Operations Center (SOC)

- SOC Overview
- SOC Team Structure
- Tier 1 Responsibilities
- Tier 2 Responsibilities
- Tier 3 Responsibilities
- SOC Workflow and Escalation Path
- Alert Lifecycle Stages
- Incident Response Phases
- Types of Alerts Handled in SOC
- Daily SOC Monitoring Activities
- KPIs and Metrics for SOC
- Log Collection Strategy
- Log Parsing and Normalization
- Key SOC Log Sources
- Firewall Logs
- IDS/IPS Logs
- DNS Logs
- Endpoint Logs (Sysmon/EDR)
- Active Directory Logs
- Cloud Logs (CloudTrail, Azure Activity)
- Use Case Design in SIEM
- Rule Writing – SPL (Splunk), AQL (Qradar)
- MITRE ATT\&CK Mapping to Alerts
- Threat Hunting Basics
- Alert Enrichment Techniques
- Alert Suppression & False Positive Handling
- Ticketing Systems (ServiceNow, JIRA) Integration
- Shift Handover Protocols

SIEM and EDR Focus

- Introduction to SIEM
- Overview of Splunk Architecture
- Splunk Ingestion and Indexing
- Writing SPL Queries
- Splunk Dashboards and Alerts
- QRadar Architecture and Flow Collection
- QRadar Rule Creation using CRE
- AQL Querying in Qradar
- Introduction to EDR
- SentinelOne Architecture
- SentinelOne Agent Capabilities
- Remote Response Actions

Malware Analysis

- Introduction to Malware Analysis
- Malware Categories a. Virus b. Worm c. Trojan d. Ransomware e. Spyware f. Rootkit g. Fileless Malware
- Malware Behavior and Infection Chain
- Static Analysis Fundamentals
- File Header and Metadata Check
- String Extraction (strings, FLOSS)
- PE Header Inspection
- Hashing (MD5, SHA256) and Use Cases
- Dynamic Analysis Overview
- Sandbox Analysis (Any.run, Cuckoo)
- Tools for Monitoring Behavior a. ProcMon b. RegShot c. Wireshark d. TCPView
- Reverse Engineering Introduction
- Disassemblers (Ghidra, IDA Free)
- Debuggers (x64dbg, OllyDbg)
- Packers and Obfuscation
- IOC Extraction Process
- Types of IOCs
- File Hashes, Registry Keys
- IPs and Domains, Filenames

Email Security

- Overview of Email-Based Threats
- Anatomy of a Phishing Email
- Spear Phishing vs Generic Phishing
- Business Email Compromise (BEC)
- Malware Delivery via Email
- Spoofing and Lookalike Domains
- Email Header Components
- SPF Record Validation
- DKIM Signature Verification
- DMARC Policy Enforcement
- Email Flow and Received Headers
- Tools for Email Security a. Microsoft Defender for O365 b. Cisco ESA c. Proofpoint d. Mimecast
- Email Sandbox Solutions
- SOC Response to Phishing
- IOC Search in Mailboxes
- Quarantining and Purging Emails
- User Awareness and Reporting Channels

Threat Intelligence

- Threat Intelligence Fundamentals
- Intelligence Lifecycle Stages
- Strategic vs Tactical vs Operational vs Technical TI
- IOC Formats (IP, Hash, URL, Domain)
- TI Sources and Feeds a. VirusTotal b. AlienVault OTX c. Recorded Future d. Shodan e. URLScan.io
- MITRE ATT&CK Overview
- IOC Enrichment in SIEM

Digital Forensics

- Introduction to Digital Forensics
- Forensics in Incident Response
- Evidence Identification
- Disk Imaging with FTK Imager
- File Recovery and Analysis
- Windows Registry Artifact Locations
- Browser History and Cache Inspection
- Event Log Collection
- Timeline Analysis Basics
- Memory Analysis using Volatility
- Chain of Custody Requirements
- Legal Considerations for Evidence
- Role of Forensics in Root Cause Analysis

Cloud Security

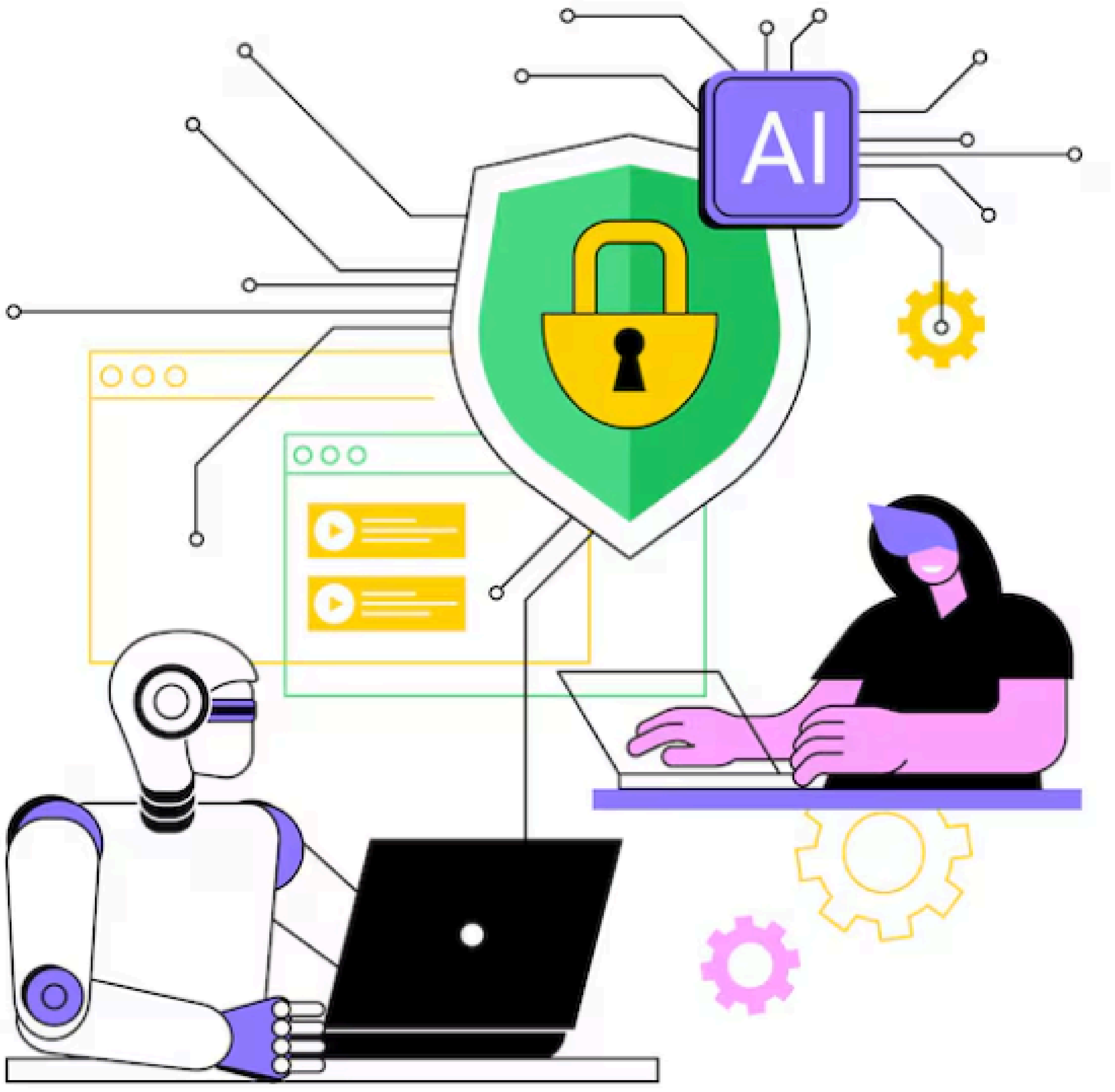
- Cloud Security Fundamentals
- Shared Responsibility Model
- Cloud Infrastructure Threats
- Misconfigured Storage Buckets (e.g., S3)
- Cloud Resource Exploitation
- Unmonitored API Calls and Access Keys
- Credential Theft from Repositories
- Cloud Identity Attacks
- Lateral Movement in Cloud Environments
- Lack of Visibility and Logging

Mobile Security(Threats)

- Cloud Security Fundamentals
- Shared Responsibility Model
- Cloud Infrastructure Threats
- Misconfigured Storage Buckets (e.g., S3)
- Cloud Resource Exploitation
- Unmonitored API Calls and Access Keys
- Credential Theft from Repositories
- Cloud Identity Attacks
- Lateral Movement in Cloud Environments
- Lack of Visibility and Logging

AI in Cybersecurity

- Introduction to AI in Cybersecurity
- What is Artificial Intelligence (AI) & Machine Learning (ML)
- Difference between AI, ML, and Deep Learning
- Why AI matters in modern cybersecurity
- Generating policy templates using LLMs
- NLP-based review for policy clarity & compliance alignment
- OneTrust AI – Policy automation & compliance tracking
- Open-source AI risk tools: RiskSense, OpenGRC



Governance & Information Security Frameworks

- Overview of Governance in Cybersecurity
- Role of governance in InfoSec
- Key governance principles and policies
- Information Security Management Systems (ISMS)
- Purpose and structure of ISMS
- PDCA (Plan–Do–Check–Act) cycle
- Major Cybersecurity Frameworks
- ISO 27001/27002 Overview
- NIST Cybersecurity Framework (CSF)
- CIS Controls
- COBIT for Information Security Governance
- Security Policies & Standards
- Policy hierarchy (Policies → Standards → Procedures → Guidelines)
- Writing effective security policies
- Roles & Responsibilities in GRC
- Board, CISO, risk managers, compliance officers
- RACI matrix in security governance