CYBERYAAN
TRAINING & CONSULTANCY

# CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL CISSP

Basic to Advanced DevOps concepts, covering Linux fundamentals, CI/CD pipelines, Docker, Kubernetes, cloud infrastructure, automation tools, deployment strategies, monitoring, and modern DevOps technologies used in the industry.

For More Information
+91-7428748576
training@cyberyaan.com

# 1. Security & Risk Management

## 1.1 Security Governance & Compliance

- Security governance frameworks — COBIT, ISO 27001/27002, NIST CSF, ITIL
- Organizational security roles and responsibilities — CISO, DPO, data owner, data custodian, data processor
- Security policies, standards, procedures, guidelines, and baselines — hierarchy and relationship
- Regulatory and legal compliance — GDPR, HIPAA, SOX, PCI-DSS, GLBA, FISMA, FERPA
- Security governance alignment with business strategy and enterprise risk management
- Due care vs. due diligence — Legal concepts and organizational liability
- Security posture assessment — Maturity models (CMM, CMMI)

## 1.2 Risk Management

- Risk management concepts — Threat, vulnerability, likelihood, impact, risk
- Risk management frameworks — NIST RMF (SP 800-37), ISO 31000, FAIR model
- Qualitative vs. quantitative risk analysis — ALE, SLE, ARO, EF calculations
- Risk response strategies — Avoid, transfer, mitigate, accept
- Risk register creation, maintenance, and reporting
- Residual risk, risk appetite, and risk tolerance definitions
- Supply chain risk management — Third-party and vendor risk assessments

## 1.3 Threat Modeling

- Threat modeling methodologies — STRIDE, PASTA, VAST, Trike
- STRIDE — Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
- Threat modeling in system and application design phases
- Attack trees and attack surface analysis
- Trust boundaries, data flow diagrams (DFDs), and security zones

## 1.4 Business Continuity Planning (BCP)

- BCP vs. DRP — Scope, purpose, and relationship
- Business Impact Analysis (BIA) — Critical function identification, MTD, RTO, RPO, MTTR
- BCP lifecycle — Initiation, analysis, solution design, implementation, maintenance
- Continuity plan testing — Tabletop, walkthrough, simulation, parallel, full interruption
- Crisis communication planning and executive escalation procedures
- Succession planning and staff redundancy for critical security roles

## 1.5 Legal & Ethics

- Computer crime categories — Cybercrime, fraud, espionage, IP theft, unauthorized access
- Intellectual property law — Copyright, patents, trademarks, trade secrets
- Privacy laws and frameworks — GDPR data subject rights, CCPA, PIPEDA, APEC Privacy Framework
- Import/export controls — EAR, ITAR, cryptography export regulations
- Evidence handling — Chain of custody, legal holds, admissibility requirements
- (ISC)² Code of Ethics — Four canons and professional conduct expectations
- Ethics of security research and responsible disclosure

## 1.6 Personnel Security

- Security awareness, training, and education programs — Design and effectiveness measurement
- Pre-employment screening — Background checks, reference verification
- Onboarding, role-based training, and security acknowledgment agreements
- Separation of duties, least privilege, need-to-know principles
- Employee termination procedures — Account revocation, asset recovery, exit interviews
- Insider threat program design and behavioral indicators
- Social engineering defenses and phishing simulation programs

# 2. Asset Security

## 2.1 Data Classification & Handling

- Government classification — Top Secret, Secret, Confidential, Unclassified
- Commercial classification — Confidential/Restricted, Private, Sensitive, Public
- Data classification criteria — Sensitivity, criticality, regulatory requirement, business value
- Classification labeling, marking, and handling procedures
- Declassification and reclassification processes and approvals
- Data ownership model — Owner, custodian, processor, user roles and responsibilities
- Data handling policies — Transmission, storage, printing, faxing, and verbal discussion

## 2.2 Data Lifecycle Management

- Data lifecycle phases — Create, store, use, share, archive, destroy
- Data retention policies and legal hold requirements
- Data remanence and secure data destruction methods — Clearing, purging, destruction
- Media sanitization standards — NIST SP 800-88 (Clear, Purge, Destroy levels)
- Physical destruction methods — Shredding, degaussing, incineration, disintegration
- Cloud data lifecycle considerations — Multi-tenancy, shared responsibility, data sovereignty

## 2.3 Privacy Protection

- Personally Identifiable Information (PII) — Definition, types, and protection requirements
- Privacy by Design (PbD) — Seven foundational principles
- Data minimization, purpose limitation, and storage limitation principles
- Data anonymization, pseudonymization, and tokenization techniques
- Privacy impact assessments (PIA) and data protection impact assessments (DPIA)
- Cross-border data transfer mechanisms — Standard contractual clauses, adequacy decisions, binding corporate rules

## 2.4 Asset Inventory & Management

- Asset inventory management — Hardware, software, data, and intellectual assets
- Configuration management and configuration baselines
- Software licensing management and compliance
- Asset valuation — Tangible and intangible asset assessment methods
- Physical asset security controls — Tagging, tracking, and access restriction

# 3. Security Architecture & Engineering

## 3.1 Security Architecture Frameworks

- Enterprise security architecture frameworks — SABSA, Zachman, TOGAF
- Security engineering principles — Least privilege, fail-safe defaults, economy of mechanism, open design, complete mediation, separation of privilege, least common mechanism, psychological acceptability
- Defense in depth and defense in breadth strategies
- Zero Trust Architecture (ZTA) — NIST SP 800-207 principles and implementation
- Security models — Bell-LaPadula (confidentiality), Biba (integrity), Clark-Wilson, Brewer-Nash (Chinese Wall)
- Trusted Computing Base (TCB) — Reference monitor, security kernel, security perimeter

## 3.2 Cryptography

- Cryptography fundamentals — Plaintext, ciphertext, key, algorithm, cipher
- Symmetric encryption — AES, DES, 3DES, Blowfish, Twofish; key management challenges
- Asymmetric encryption — RSA, Diffie-Hellman, ECC, ElGamal; public/private key pairs
- Hybrid cryptography — How SSL/TLS combines symmetric and asymmetric methods
- Hashing algorithms — MD5, SHA-1, SHA-2, SHA-3; collision attacks; HMAC
- Digital signatures — Non-repudiation, signing process, verification, certificate binding
- Public Key Infrastructure (PKI) — CA, RA, CRL, OCSP, certificate lifecycle
- Key management — Generation, distribution, storage, rotation, escrow, destruction
- Cryptographic attacks — Brute force, birthday attack, meet-in-the-middle, side-channel, rainbow tables
- Quantum computing impact on cryptography — Post-quantum algorithms (CRYSTALS-Kyber, CRYSTALS-Dilithium)
- Steganography and digital watermarking

## 3.3 Hardware & Firmware Security

- Trusted Platform Module (TPM) — Functions, attestation, key storage
- Hardware Security Modules (HSM) — Use cases, FIPS 140-2/3 levels
- Secure boot and measured boot processes
- BIOS/UEFI security — Firmware attacks and protection mechanisms
- Embedded systems and IoT security considerations — Constrained devices, firmware updates
- Industrial Control Systems (ICS) and SCADA security — OT/IT convergence challenges
- Side-channel attacks — Timing attacks, power analysis, electromagnetic attacks

## 3.4 Virtualization & Cloud Security Architecture

- Virtualization security — Hypervisor types (Type 1, Type 2), VM isolation, VM escape attacks
- Container security — Docker, Kubernetes security principles, image integrity
- Cloud service models — IaaS, PaaS, SaaS security responsibilities (shared responsibility model)
- Cloud deployment models — Public, private, hybrid, community cloud security implications
- Cloud security architecture — CASB, CSPM, CWPP, SASE frameworks
- Serverless and microservices security considerations

# 3.5 Physical & Environmental Security

- Site and facility security planning — Crime Prevention Through Environmental Design (CPTED)
- Physical access controls — Mantraps, turnstiles, biometrics, guards, locks, key management
- Data center physical security — Perimeter security, server room access, visitor management
- Environmental controls — HVAC, fire suppression (wet pipe, dry pipe, Halon alternatives), UPS, power conditioning
- Electromagnetic emanation security — TEMPEST, Faraday cages, shielded rooms
- Physical intrusion detection — CCTV design, motion sensors, door contacts, glass break sensors

# 4. Communication & Network Security

## 4.1 Network Architecture & Protocols

- OSI model — All 7 layers, protocols at each layer, security implications per layer
- TCP/IP model — Network access, internet, transport, application layer comparison
- IPv4 and IPv6 — Addressing, subnetting, CIDR, IPv6 transition security considerations
- Core protocols — TCP, UDP, ICMP, ARP, DNS, DHCP, HTTP/S, SMTP, FTP/SFTP, SNMP, NTP
- Routing protocols — BGP, OSPF, RIP security vulnerabilities and hardening
- Network topologies — Bus, ring, star, mesh, hybrid; security trade-offs

## 4.2 Network Security Controls

- Firewalls — Packet filtering, stateful inspection, application-layer (NGFW), Web Application Firewall (WAF)
- Intrusion Detection & Prevention Systems — NIDS, HIDS, NIPS, HIPS; signature vs. anomaly detection
- Network segmentation — DMZ design, VLANs, microsegmentation, network zones
- Proxy servers — Forward proxy, reverse proxy, transparent proxy use cases
- Network Access Control (NAC) — 802.1X, posture assessment, quarantine networks
- DDoS protection — Volumetric, protocol, and application-layer attack mitigation
- Software-Defined Networking (SDN) — Control plane / data plane separation, security implications
- Content Delivery Networks (CDN) and cloud-based DDoS mitigation services

## 4.3 Secure Communications

- VPN technologies — IPSec (AH, ESP, IKE), SSL/TLS VPN, split tunneling risks
- Wireless security — WEP weaknesses, WPA2/WPA3, EAP variants (PEAP, EAP-TLS), rogue AP detection
- TLS/SSL — Handshake process, certificate validation, cipher suites, TLS 1.3 improvements
- Email security — SPF, DKIM, DMARC, S/MIME, PGP, email gateway filtering
- VoIP security — SIP vulnerabilities, call hijacking, toll fraud, encryption requirements
- Bluetooth and NFC security — Pairing vulnerabilities, bluejacking, bluesnarfing, eavesdropping
- Secure DNS — DNSSEC, DNS over HTTPS (DoH), DNS over TLS (DoT), DNS filtering
-

## 4.4 Network Attacks & Defenses

- Reconnaissance attacks — Port scanning (Nmap), OS fingerprinting, banner grabbing
- Man-in-the-Middle (MitM) attacks — ARP poisoning, DNS spoofing, SSL stripping
- Denial of Service — SYN flood, Smurf attack, amplification attacks (DNS, NTP)
- Sniffing and eavesdropping — Passive sniffing, promiscuous mode, SPAN ports
- Network-based malware propagation — Worms, botnets, C2 infrastructure
- Network forensics — Flow analysis, pcap analysis, NetFlow for incident investigation

# 4. Identity & Access Management (IAM)

## 5.1 Identity Management

- Identity concepts — Digital identity, identity proofing, identity lifecycle management
- Directory services — LDAP, Microsoft Active Directory, Azure AD structure and security
- Provisioning and deprovisioning — Automated identity lifecycle, joiner-mover-leaver processes
- Identity federation — SAML 2.0, WS-Federation, trust relationships between organizations
- Single Sign-On (SSO) — Kerberos, SAML, OAuth 2.0, OpenID Connect (OIDC)
- Identity Governance and Administration (IGA) — Role mining, access certification campaigns

## 5.2 Authentication Methods

- Authentication factors — Knowledge (passwords), possession (tokens), inherence (biometrics), location, behavior
- Multi-Factor Authentication (MFA) — TOTP, HOTP, push notifications, hardware tokens (FIDO2)
- Password policies — Complexity, length, history, aging, lockout; password manager guidance
- Biometric authentication — Accuracy metrics (FAR, FRR, CER/EER), types, attack vectors
- Passwordless authentication — FIDO2/WebAuthn, passkeys, certificate-based authentication
- Continuous authentication and risk-based adaptive authentication

## 5.3 Authorization & Access Control Models

- Access control models — MAC, DAC, RBAC, ABAC, Rule-Based AC
- Mandatory Access Control (MAC) — Labels, clearances, compartments; government/military use
- Discretionary Access Control (DAC) — Owner-controlled permissions; risks and limitations
- Role-Based Access Control (RBAC) — Role assignment, role hierarchy, NIST RBAC standard
- Attribute-Based Access Control (ABAC) — Policy-based, context-aware, fine-grained control
- Principle of least privilege — Minimum necessary access enforcement
- Separation of duties — Fraud prevention through role splitting and dual control
- Access control lists (ACLs), capability tables, and access control matrices

## 5.4 Privileged Access Management

- Privileged accounts — Types: local admin, domain admin, service accounts, root, emergency accounts
- PAM solutions — CyberArk, BeyondTrust, Delinea — vault, session recording, credential rotation
- Just-In-Time (JIT) privilege elevation — Removing standing privileged access
- Privileged Identity Management (PIM) in cloud environments — Azure PIM, AWS IAM roles
- Service account management — Password rotation, Managed Service Accounts (MSA)
- Insider threat detection through privileged access monitoring and behavioral analytics

## 5.5 Identity in Cloud & Federation

- Cloud IAM — AWS IAM, Azure RBAC, Google Cloud IAM policies and roles
- OAuth 2.0 authorization framework — Grant types, scopes, tokens, refresh tokens
- OpenID Connect (OIDC) — Identity layer on OAuth 2.0, ID tokens, claims
- SAML-based federation — SP-initiated vs. IdP-initiated SSO flows
- Cross-domain trust — B2B federation, guest access, external identity providers
- Zero Trust identity principles — Verify explicitly, least privilege, assume breach

# 6. Security Assessment & Testing

## 6.1 Assessment Strategy & Planning

- Assessment types — Vulnerability assessment, penetration testing, red team exercise, security audit, compliance assessment
- Testing methodologies — Black box, white box, gray box testing approaches
- Rules of engagement — Scope definition, authorization requirements, emergency stop procedures
- Assessment planning — Objectives, scope, methodology, resources, timeline, deliverables
- Risk of testing — Potential service disruption, false sense of security from incomplete testing

## 6.2 Vulnerability Management

- Vulnerability scanning tools — Nessus, Qualys, Rapid7 InsightVM, OpenVAS
- Vulnerability lifecycle — Discover, prioritize, remediate, verify, report
- CVE, CVSS scoring — Base, temporal, environmental metric groups; CVSS v3.1 vs v4.0
- Vulnerability databases — NVD, vendor advisories, exploit-db, CISA KEV catalog
- Patch management — Patch Tuesday, emergency patching, patch testing, rollback procedures
- Configuration scanning — CIS Benchmarks, STIG compliance scanning

## 6.3 Penetration Testing

- Penetration testing phases — Reconnaissance, scanning, exploitation, post-exploitation, reporting
- Penetration testing standards — PTES, OWASP Testing Guide, NIST SP 800-115
- Network penetration testing — External, internal, wireless testing methodologies
- Web application testing — OWASP Top 10, injection flaws, authentication bypass, IDOR, XSS, CSRF
- Social engineering testing — Phishing simulations, vishing, physical intrusion testing
- Report writing — Executive summary, findings, evidence, risk ratings, remediation recommendations
- Re-testing and attestation after remediation

## 6.4 Security Audits & Reviews

- Audit types — Internal audit, external audit, third-party audit, regulatory audit
- Audit standards — ISO 27001 audit process, SOC 2 Type I/II, FedRAMP, PCI DSS QSA
- Log review and analysis — Audit trails, SIEM queries, anomaly identification
- Code review — Static analysis (SAST), dynamic analysis (DAST), IAST, manual review
- Architecture review — Security design review, threat model validation
- Account management reviews — Access certification, orphaned account detection

## 6.5 Software Testing for Security

- Test coverage analysis — Code coverage, branch coverage, path coverage
- Fuzz testing — Generational vs. mutation-based fuzzing, AFL, LibFuzzer
- Interface testing — API testing, microservice interface security verification
- Regression testing — Ensuring patches don't reintroduce vulnerabilities
- Security test automation — Integrating SAST/DAST into CI/CD pipelines

# 7. Security Operations

## 7.1 Security Operations Center (SOC)

- SOC models — In-house, outsourced (MSSP), hybrid; Tier 1/2/3 analyst roles
- SIEM platforms — Splunk, IBM QRadar, Microsoft Sentinel — architecture and use
- Alert triage — Prioritization, escalation, false positive reduction techniques
- Threat intelligence integration with SOC operations
- SOC metrics and KPIs — MTTD, MTTR, MTTA, false positive rate, detection coverage

## 7.2 Incident Management

- Incident response lifecycle — NIST SP 800-61: Preparation, Detection, Containment, Eradication, Recovery, Lessons Learned
- Incident classification — Security events, incidents, breaches; severity tiers
- Incident response team (CSIRT/CERT) — Roles, responsibilities, communication protocols
- Containment strategies — Short-term containment, evidence preservation, long-term containment
- Eradication techniques — Malware removal, vulnerability remediation, credential resets
- Post-incident review — Root cause analysis, process improvement, lessons learned documentation
- Legal considerations — Breach notification obligations under GDPR, state laws, HIPAA, PCI DSS

## 7.3 Digital Forensics

- Forensics principles — Locard's Exchange Principle, chain of custody, forensic integrity
- Evidence collection order — Volatility hierarchy: CPU registers → RAM → swap → disk → backup
- Memory forensics — RAM acquisition, process analysis, malware artifacts in memory
- Disk forensics — Forensic imaging, write blockers, file system analysis, deleted file recovery
- Network forensics — Packet capture analysis, NetFlow, DNS log analysis, proxy logs
- Mobile forensics — iOS and Android evidence acquisition, cloud backup analysis
- Forensic tools — Autopsy, FTK, Volatility, Wireshark, Cellebrite, EnCase
- Anti-forensics techniques — Data wiping, timestamp manipulation, steganography, encryption

## 7.4 Identity & Access Monitoring

- Account monitoring — Privileged account activity logging, impossible travel detection
- User and Entity Behavior Analytics (UEBA) — Baseline building, anomaly scoring
- Session management — Concurrent session limits, session timeout policies
- Access review and recertification — Quarterly access reviews, automated provisioning audits

## 7.5 Disaster Recovery (DR)

- DR objectives — RTO (Recovery Time Objective), RPO (Recovery Point Objective), MTD, WRT definitions
- Backup strategies — Full, incremental, differential; backup rotation schemes (GFS)
- Recovery site types — Hot site, warm site, cold site, mobile site, cloud-based DR
- Replication technologies — Synchronous vs. asynchronous replication, journaling
- DR plan components — Contact lists, system inventories, recovery procedures, vendor agreements
- DR testing types — Tabletop, walkthrough, simulation, parallel processing, full cutover
- Cloud DR — AWS Elastic Disaster Recovery, Azure Site Recovery, DR-as-a-Service

## 7.6 Change & Configuration Management

- Change management process — RFC, CAB review, testing, rollback planning, post-implementation review
- Configuration management — CMDB, baselines, drift detection, automated remediation
- Patch management program — Scan, prioritize, test, deploy, verify cycle
- Release and deployment management — Blue/green deployment, canary releases, security gates
- Emergency change procedures — Fast-track process, retrospective documentation

## 7.7 Physical Security Operations

- Physical security program components — Policy, personnel, procedures, physical controls
- Access badge systems — Smart cards, proximity cards, PIN + card combinations
- Visitor management — Escort requirements, visitor logs, temporary access badges
- Data center operations security — Clean desk policy, no-photography zones, secure printing
- Secure media handling — Transport security, courier controls, chain of custody

# 8. Software Development Security

## 8.1 Secure Software Development Lifecycle (SDLC)

- SDLC models — Waterfall, Agile/Scrum, Spiral, DevOps — security integration in each
- Microsoft Security Development Lifecycle (SDL) phases and activities
- Security requirements gathering — Abuse cases, misuse cases, security user stories
- Secure design principles — Least privilege, fail secure, input validation, output encoding
- Security gates and checkpoints in SDLC — Security requirements, design review, code review, testing, release approval
- DevSecOps — Shifting security left, pipeline integration, security as code

## 8.2 Software Vulnerabilities & Secure Coding

- OWASP Top 10 (2021) — Injection, broken auth, IDOR, security misconfiguration, cryptographic failures, vulnerable components, SSRF, XSS, insecure design, software & data integrity failures
- Injection attacks — SQL injection, command injection, LDAP injection, XML injection; prepared statements
- Cross-Site Scripting (XSS) — Reflected, stored, DOM-based; Content Security Policy (CSP) defenses
- Cross-Site Request Forgery (CSRF) — Anti-CSRF tokens, SameSite cookies
- Insecure deserialization — Object injection, gadget chains, defense strategies
- Buffer overflow — Stack-based, heap-based; DEP, ASLR, stack canaries as mitigations
- Race conditions and time-of-check to time-of-use (TOCTOU) vulnerabilities
- Secure coding standards — CERT C/C++, OWASP ESAPI, CWE/SANS Top 25

## 8.3 Application Security Testing

- Static Application Security Testing (SAST) — Source code analysis, taint analysis, tools: Checkmarx, Fortify, SonarQube
- Dynamic Application Security Testing (DAST) — Runtime testing, tools: OWASP ZAP, Burp Suite
- Interactive Application Security Testing (IAST) — Agent-based, runtime instrumentation
- Software Composition Analysis (SCA) — Third-party and open-source library vulnerability detection
- Manual code review — Techniques, reviewer independence, structured review checklist
- API security testing — Authentication testing, authorization bypass, rate limiting, input validation

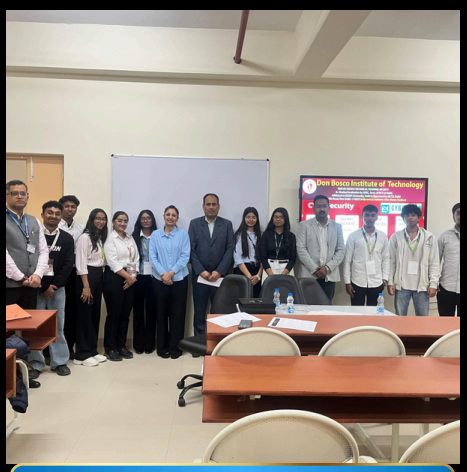
## 8.4 Secure Software Architecture

- Secure microservices architecture — API gateways, service mesh, mutual TLS (mTLS)
- Database security — Parameterized queries, stored procedures, encryption at rest, database activity monitoring
- Cryptography in applications — Proper key storage (HSM, vault), correct algorithm selection, IV/nonce management
- Input validation and output encoding — Server-side validation, whitelist vs. blacklist, encoding contexts
- Error handling and logging — Avoiding sensitive data exposure in error messages, structured security logging
- Session management — Secure session token generation, HttpOnly/Secure flags, session fixation prevention

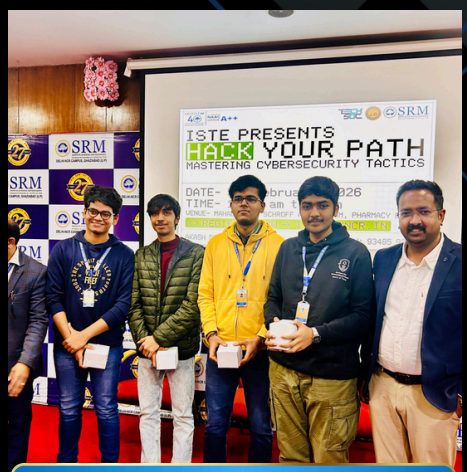
## 8.5 Third-Party & Supply Chain Software Security

- Software supply chain risks — SolarWinds attack, Log4Shell, XZ Utils as case studies
- Software Bill of Materials (SBOM) — SPDX, CycloneDX formats; NTIA minimum requirements
- Open-source software risk management — License compliance, vulnerability tracking, maintainer vetting
- Third-party code review — Vendor security assessments, contractual security requirements
- CI/CD pipeline security — Pipeline integrity, signed artifacts, secrets management (HashiCorp Vault)
- Container image security — Base image selection, image scanning, registry security

# GALLERY




Don Bosco Institute of Technology

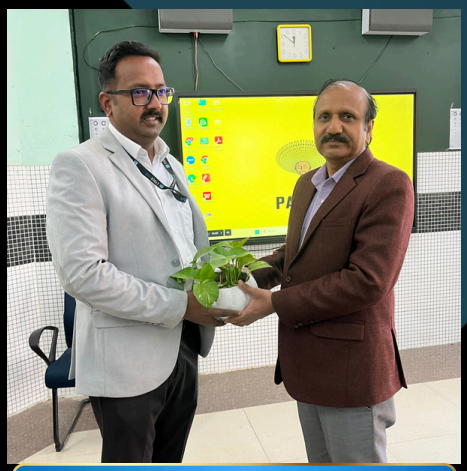



SRM Institute of Science and Technology

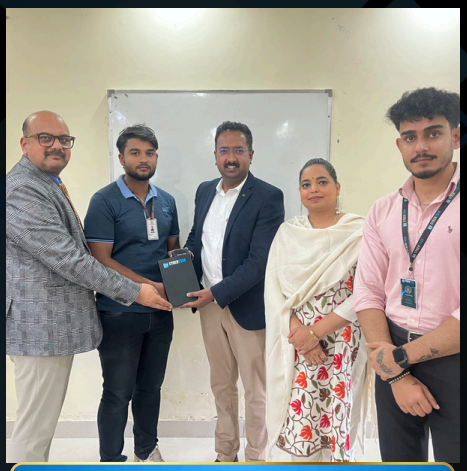
Indraprastha Institute of Information Technology Delhi

Shri Guru Tegh Bahadur Institute of Management & Information Technology (SGTBIMIT)

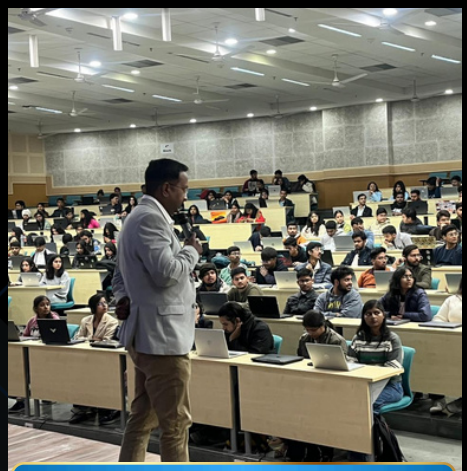
ARI Simulation



CM SHRI SEC-19 DWARKA



IIMT Group Of Colleges Greater Noida



Indraprastha Institute of Information Technology Delhi

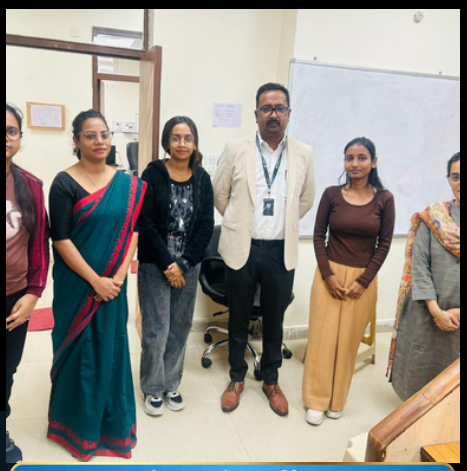
Shri Guru Tegh Bahadur Institute of management & Information technology (SGTBIMIT)

# GALLERY

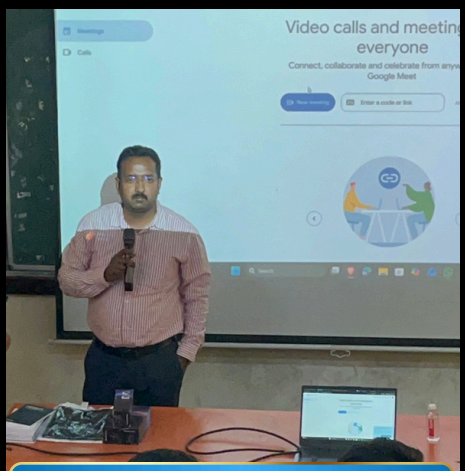
Shri Aurobindo College, of commerce and management


G.C.R.G. Group of Institutions, Lucknow

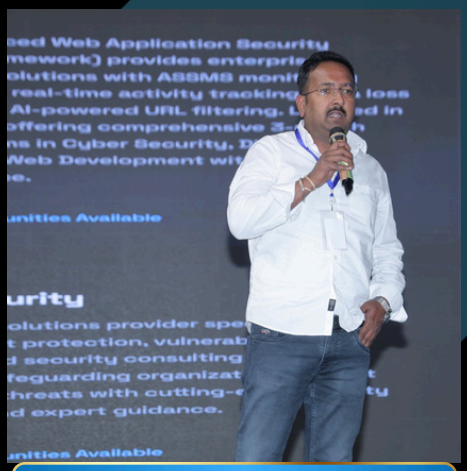
Maitreyi College, University of Delhi



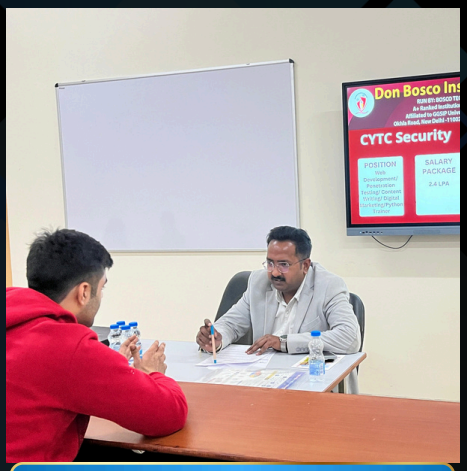
Maitreyi College, University of Delhi



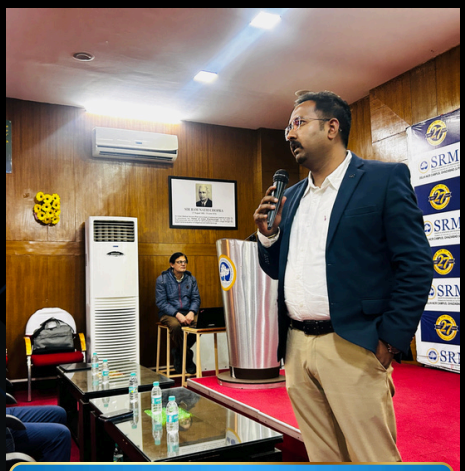

Daulat Ram College, DU



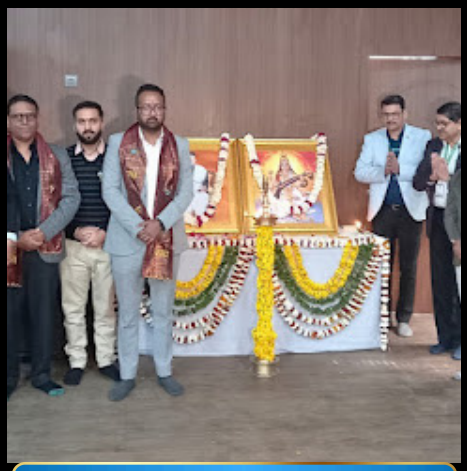
Hack Defence Summit 2026




Don Bosco Institute of Technology



SRM Institute of Science and Technology



Hackathon

# PLACEMENTS

**Vansh Gupta**
Placed in Infocus- IT
As a Cyber Security Analyst

**Yash Garg**
Placed in Innspark
As a Soc Analyst

**Shivam Yadav**
Placed in Innspark
As a Soc Analyst

**Ekas Nayyar**
Placed In CyberAlpha Consulting LLP
As a Information Security Intern

**Ishwinder**
Placed inInfocus- IT
As a Cyber Security Analyst

**Jahanvi Khurana**
Placed in Cynox Security LLP
As a Cyber Security Analyst

**Yash Garg**
Placed in Cynox Security LLP
As a Cyber Security Analyst

**Ravinshu Chauhan**
Placed in Innspark
As a Soc Analyst

**Chandan Jha**
Placed in HCL Tech
As a Cyber Security Consultant

**Ajay**
Placed in Codec Networks
As a Cyber Security Analyst

**Ritik**
Placed in SBI
As a Cyber Security Analyst

**Prince Bhardwaj**
Placed in Accenture
As a Cyber Security Analyst

# PLACEMENTS

**Aksh Yadav**
Placed in Skillmine
As a Soc Analyst

**Gyan Ranjan**
Placed in Cynox Security LLP
As a Cyber Security Analyst

**Dinesh kumar**
Placed in Infosys
As a Cyber Security Analyst

**Debjit Mohapatra**
Placed in GL Bajaj
As a Cyber Security Trainer

**Pranav**
Placed in Cynox Security LLP
As a Security Analyst Trainee

**Suraj Ashok Rathor**
Placed in Cynox Security LLP
As a Security Analyst-Trainee

**Mohit Yadav**
Placed in National informatics Center, Meity
As a SOC Analyst

**Aditi Goyal**
Placed in Capgemini
As a Cisco Tac engineer (network analyst)

**Divyanshu Shekhar**
Placed in Transbank
As a Information Security Officer

**Ravi**
Placed in hays
As a Soc Analyst

# PLACEMENTS

**Isha**
Placed in Cywarden Inc.
As a Security Analyst

**Harsh Vardhan Verma**
Placed in CISAI
As a Soc Analyst

**Tushal Kumar**
Placed in Cyberion Labs
As a Security Analyst

**Hansika Rawat**
Placed in Cynox Security LLP
As a Cyber Security Analyst

**Harsh Verma**
Placed in Hoolocom
As a Technical Support Implementation Engineer

**Pratik**
Placed in Indian Army
As a Cyber Security Analyst

**Gaurav Pathak**
Placed in Ministry of Defence
As a Information Technology Security Engineer

**G.Rohit**
Placed in KPMG
As a SOC Analyst

**kirti**
Placed in Cynox Security LLP
As a Cyber Security Analyst

**Arpit Hawa**
Placed in Capgemini
As a Cisco Tac engineer (network analyst)

# CLIENTS AND PARTNERS

PELORUS
Enabling Technology in the Right Direction

CompTIA

eSec Forte

4ACHIEVERS
WE BUILD PROFESSIONALS

GURUGRAM UNIVERSITY
विद्या जीवनाय न तु जीविकाय

KLTIF

GNIOT
GROUP OF INSTITUTIONS
Approved by AICTE, New Delhi and Affiliated to AKTU-Lucknow

SAVJC
SHREE ATAM VALLABH JAIN COLLEGE
LUDHIANA, PUNJAB
AFFILIATED TO PANJAB UNIVERSITY, CHANDIGARH
Managed by Shri Atam Nand Jain School Committee

इन्दिरा गाँधी विश्वविद्यालय
INDIRA GANDHI UNIVERSITY
MEERPUR, REWARI
मीरपुर, रेवाड़ी
सा विद्या या विमुक्तये

MAHARAJA AGRASEN INSTITUTE OF TECHNOLOGY
MAIT

IITM
Nurturing Excellence

NSG
सर्वत्र सर्वोत्तम सुरक्षा

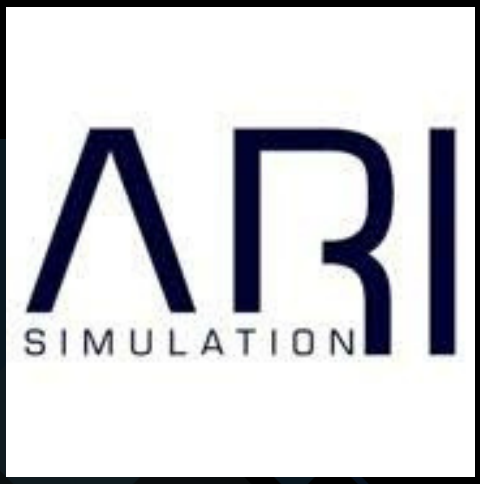
GIET UNIVERSITY
GUNUPUR, ODISHA
EXCELLENCE - OUR ESSENCE

aws

# CLIENTS AND PARTNERS










# FRANCHISE

Build the Future of Cybersecurity Education
Cybersecurity is no longer optional—it's a necessity. With rising cyber threats and increasing demand for skilled professionals, CyberYaan Training & Consultancy is on a mission to empower the next generation with industry-ready skills.

Now, you can be a part of this fast-growing revolution.

1. Join our franchise network and grow your business with our proven success.

2. Explore franchise opportunities—connect with us to embark on a thriving partnership.

**Email:** Pankaj@cyberyaan.com

# CONTACT US

+91 7428748576

training@cyberyaan.com

25/28, Tilak Nagar, Upper Ground Floor,
Opposite Raj Mandir Hypermarket,
New Delhi - 110018

SCAN ME

Youtube

Linkdin

Instagram

www.cyberyaan.com