SIEM XPERT
Learn. Secure. Succeed.

CISSP TRAINING & CERTIFICATION SYLLABUS

SIEM XPERT

Best Cyber Security Institution in India

Committed to QUALITY, Committed to YOU.

trainings@siemxpert.com • www.siemxpert.com • +91 9108318017

SIEM XPERT
Learn. Secure. Succeed.

OUR **STATISTICS**

50000+

Trainees across the globe

24*7

Real-Time Lab Setup, Accessible From Anywhere

65%

Average Salary Hike

65 LPA

Highest Package

3.5M

Job openings in 2025

SIEM XPERT
Learn. Secure. Succeed.

WHO CAN **JOIN THE COURSE?**

SIEM XPERT was founded with an intention to offer a complete course that is specifically designed as per the current industry trends. Years of experience has helped us identify and understand the graduate-employee skills gap in the industry.

Candidates must have a minimum of five years cumulative paid work experience in two or more of the eight domains of the CISSP CBK.

Candidates with a four-year college degree or an approved credential may be eligible for a one-year experience waiver.

Training gives best chance for them to reform their career and they will be able to perform the jobs like as an experience after this training.

People who are working in Cyber Security and want to get a promotion or switch jobs to get a higher payout.

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION (SYLLABUS)

Domain 1: Security and Risk Management

1.1 Understand, adhere to, and promote professional ethics

- ISC2 Code of Professional Ethics
- Organizational code of ethics

1.2 Understand and apply security concepts

- Confidentiality, integrity, availability, authenticity and nonrepudiation

1.3 Evaluate and apply security governance principles

- Alignment of the security function to business strategy, goals, mission, and objectives
- Organizational processes (e.g., acquisitions, divestitures, governance committees)
- Organizational roles and responsibilities
- Security control frameworks
- Due care/due diligence

1.4 Determine compliance and other requirements

- Contractual, legal, industry standards, and regulatory requirements
- Privacy requirements

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

1.5 Understand legal and regulatory issues that pertain to information security in a holistic context

- Cybercrimes and data breaches
- Licensing and Intellectual Property (IP) requirements
- Import/export controls
- Transborder data flow
- Privacy

1.6 Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, and industry standards)

1.7 Develop, document, and implement security policy, standards, procedures, and guidelines

1.8 Identify, analyze, and prioritize Business Continuity (BC) requirements

- Business Impact Analysis (BIA)
- Develop and document the scope and the plan

1.9 Contribute to and enforce personnel security policies and procedures

- Candidate screening and hiring
- Employment agreements and policies

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

- Onboarding, transfers, and termination processes
- Vendor, consultant, and contractor agreements and controls
- Compliance policy requirements
- Privacy policy requirements

1.10 Understand and apply risk management concepts

- Identify threats and vulnerabilities
- Risk assessment/analysis
- Risk response
- Countermeasure selection and implementation
- Applicable types of controls (e.g., preventive,
- detective, corrective)
- Control assessments (security and privacy)
- Monitoring and measurement
- Reporting
- Continuous improvement (e.g., Risk maturity modeling)
- Risk frameworks

1.11 Understand and apply threat modeling concepts and methodologies

1.12 Apply Supply Chain Risk Management (SCRM) concepts

- Risks associated with hardware, software, and services
- Third-party assessment and monitoring

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

- Minimum security requirements
- Service level requirements

1.13 Establish and maintain a security awareness, education, and training program

- Methods and techniques to present awareness and training (e.g., social engineering, phishing, security champions, gamification)
- Periodic content reviews
- Program effectiveness evaluation

Domain 2: Asset Security

2.1 Identify and classify information and assets

- Data classification
- Asset Classification

2.2 Establish information and asset handling requirements

2.3 Provision resources securely

- Information and asset ownership
- Asset inventory (e.g., tangible, intangible)
- Asset management

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

2.4 Manage data lifecycle

- Data roles (i.e., owners, controllers, custodians, processors, users/subjects)
- Data collection
- Data location
- Data maintenance
- Data retention
- Data remanence
- Data destruction

2.5 Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))

2.6 Determine data security controls and compliance requirements

- Data states (e.g., in use, in transit, at rest)
- Scoping and tailoring
- Standards selection
- Data protection methods (e.g., Digital Rights Management (DRM), Data Loss Prevention (DLP),
- Cloud Access Security Broker (CASB))

Domain 3: Security Architecture and Engineering

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

3.1 Research, implement and manage engineering processes using secure design principles

- Threat modeling
- Least privilege
- Defense in depth
- Secure defaults
- Fail securely
- Separation of Duties (SoD)
- Keep it simple
- Zero Trust
- Privacy by design
- Trust but verify
- Shared responsibility

3.2 Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)

3.3 Select controls based upon systems security requirements

3.4 Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

- Client-based systems
- Server-based systems
- Database systems
- Cryptographic systems
- Industrial Control Systems (ICS)
- Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- Distributed systems
- Internet of Things (IoT)
- Microservices
- Containerization
- Serverless
- Embedded systems
- High-Performance Computing (HPC) systems
- Edge computing systems
- Virtualized systems

3.6 Select and determine cryptographic solutions

- Cryptographic life cycle (e.g., keys, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)
- Public Key Infrastructure (PKI)

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

- Key management practices
- Digital signatures and digital certificates
- Non-repudiation
- Integrity (e.g., hashing)

3.7 Understand methods of cryptanalytic attacks

- Brute force
- Ciphertext only
- Known plaintext
- Frequency analysis
- Chosen ciphertext
- Implementation attacks
- Side-channel

3.8 Apply security principles to site and facility design

3.9 Design site and facility security controls

- Wiring closets/intermediate distribution facilities
- Server rooms/data centers
- Media storage facilities
- Evidence storage
- Restricted and work area security
- Utilities and Heating, Ventilation, and Air
- Conditioning (HVAC)
- Environmental issues

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

- Fire prevention, detection, and suppression
- Power (e.g., redundant, backup)

Domain 4: Communication and Network Security

4.1 Assess and implement secure design principles in network architectures

- Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
- Internet Protocol (IP) networking (e.g., Internet Protocol Security (IPSec), Internet Protocol (IP) v4/6)
- Secure protocols
- Implications of multilayer protocols
- Converged protocols (e.g., Fiber Channel Over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP))
- Micro-segmentation (e.g., Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD-WAN))
- Wireless networks (e.g., Li-Fi, Wi-Fi, Zigbee, satellite)
- Cellular networks (e.g., 4G, 5G)
- Content Distribution Networks (CDN)

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

4.2 Secure network components

- Operation of hardware (e.g., redundant power, warranty, support)
- Transmission media
- Network Access Control (NAC) devices
- Endpoint security

4.3 Implement secure communication channels according to design

- Voice
- Multimedia collaboration
- Remote access
- Data communications
- Virtualized networks
- Third-party connectivity

Domain 5: Identity and Access Management (IAM)

5.1 Control physical and logical access to assets

- Information
- Systems
- Devices
- Facilities
- Applications

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

5.2 Manage identification and authentication of people, devices, and services

- Identity Management (IdM) implementation
- Single/Multi-Factor Authentication (MFA)
- Accountability
- Session management
- Registration, proofing, and establishment of identity
- Federated Identity Management (FIM)
- Credential management systems
- Single Sign On (SSO)
- Just-In-Time (JIT)

5.3 Federated identity with a third-party service

- On-premise
- Cloud
- Hybrid

5.4 Implement and manage authorization mechanisms

- Role Based Access Control (RBAC)
- Rule based access control
- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Attribute Based Access Control (ABAC)
- Risk based access control

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

5.5 Manage the identity and access provisioning lifecycle

- Account access review (e.g., user, system, service)
- Provisioning and deprovisioning (e.g., on /off boarding and transfers)
- Role definition (e.g., people assigned to new roles)
- Privilege escalation (e.g., managed service accounts, use of sudo, minimizing its use)

5.6 Implement authentication systems

- OpenID Connect (OIDC)/Open Authorization (Oauth)
- Security Assertion Markup Language (SAML)
- Kerberos
- Remote Authentication Dial-In User Service (RADIUS) /Terminal Access Controller Access
- Control System Plus (TACACS+)

Domain 6: Security Assessment and Testing

6.1 Design and validate assessment, test, and audit strategies

- Internal
- External
- Third-party

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

6.2 Conduct security control testing

- Vulnerability assessment
- Penetration testing
- Log reviews
- Synthetic transactions
- Code review and testing
- Misuse case testing
- Test coverage analysis
- Interface testing
- Breach attack simulations
- Compliance checks

6.3 Collect security process data (e.g., technical and administrative)

- Account management
- Management review and approval
- Key performance and risk indicators
- Backup verification data
- Training and awareness
- Disaster Recovery (DR) and Business Continuity (BC)

6.4 Analyze test output and generate report

- Remediation
- Exception handling
- Ethical disclosure

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

6.5 Conduct or facilitate security audits

- Internal
- External
- Third-party

Domain 7: Security Operations

7.1 Understand and comply with investigations

- Evidence collection and handling
- Reporting and documentation
- Investigative techniques
- Digital forensics tools, tactics, and procedures
- Artifacts (e.g., computer, network, mobile device)

7.2 Conduct logging and monitoring activities

- Intrusion detection and prevention
- Security Information and Event Management (SIEM)
- Continuous monitoring
- Egress monitoring
- Log management
- Threat intelligence (e.g., threat feeds, threat hunting)
- User and Entity Behavior Analytics (UEBA)

7.3 Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

7.4 Apply foundational security operations concepts Need-to-know/least privilege

- Separation of Duties (SoD) and responsibilities
- Privileged account management
- Job rotation
- Service Level Agreements (SLAs)

7.5 Apply resource protection

- Media management
- Media protection techniques

7.6 Conduct incident management

- Detection
- Response
- Mitigation
- Reporting
- Recovery
- Remediation
- Lessons learned

7.7 Operate and maintain detective and preventative measures

- Firewalls (e.g., next generation, web application, network)
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

- Whitelisting/blacklisting
- Third-party provided security services
- Sandboxing
- Honeypots/honeynets
- Anti-malware
- Machine learning and Artificial Intelligence (AI) based tools

7.8 Implement and support patch and vulnerability management

7.9 Understand and participate in change management processes

7.10 Implement recovery strategies

- Backup storage strategies
- Recovery site strategies
- Multiple processing sites
- System resilience, High Availability (HA), Quality of Service (QoS), and fault tolerance

7.11 Implement Disaster Recovery (DR) processes

- Response
- Personnel
- Communications

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

7.12 Test Disaster Recovery Plans (DRP)

- Read-through/tabletop
- Walkthrough
- Simulation
- Parallel
- Full interruption

7.13 Participate in Business Continuity (BC) planning and exercises

7.14 Implement and manage physical security

- Perimeter security controls
- Internal security controls

7.15 Address personnel safety and security concerns

- Travel
- Security training and awareness
- Emergency management
- Duress

Domain 8: Software Development Security

8.1 Understand and integrate security in the Software Development Life Cycle (SDLC)

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

- Development methodologies (e.g., Agile, Waterfall, DevOps, DevSecOps)
- Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))
- Operation and maintenance
- Change management
- Integrated Product Team (IPT)

8.2 Identify and apply security controls in software development ecosystems

- Programming languages
- Libraries
- Tool sets
- Integrated Development Environment (IDE)
- Runtime
- Continuous Integration and Continuous Delivery (CI/CD)
- Security Orchestration, Automation, and Response (SOAR)
- Software Configuration Management (SCM)
- Code repositories
- Application security testing (e.g., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))

8.3 Assess the effectiveness of software security

SIEM XPERT
Learn. Secure. Succeed.

CISSP CERTIFICATION SYLLABUS)

- Auditing and logging of changes
- Risk analysis and mitigation

8.4 Assess security impact of acquired software

- Commercial-off-the-shelf (COTS)
- Open source
- Third-party
- Managed services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

8.5 Define and apply secure coding guidelines and standards

- Security weaknesses and vulnerabilities at the source-code level
- Security of Application Programming Interfaces (APIs)
- Secure coding practices
- Software-defined security

SIEM XPERT
Learn. Secure. Succeed.

ABOUT **SIEM XPERT**

Company Profile

SIEM XPERT is the Global leader in Cyber Security Trainings and Services, having headquarter in Bangalore (Karnataka) and in operations since 2015.

We have helped more than 10000 people globally to start their career in a high demanding, high paying field of cyber security and helped them to change their lives.

Our partnership with numerous businesses that hire cyber security professionals allows us to recommend our trained students to them.

We have a world-class real-time company-type lab setup on several cyber security tools that allows students real-time hands-on practise so they can become ready to deploy and can deliver quality from day one. As a result, they are favoured by employers since they don't have to train them.

By providing corporate trainings we assist companies to enhance cyber security skills of their employees.

MISSION

Company Mission

As global market is having Cyber Security resources crunch hence our mission is to fulfill those open position by generating ready to deploy cyber security resources and give them real-time practical hands-on experience with the help of world class Cyber Security Lab.

We also aim to offer the best managed cyber security services to businesses so they can monitor their networks for cyber threats.

SIEM XP
Learn. Secure. Succeed.

SULABH MISHRA

CEO, Cyber Security Trainer & Solution Architect

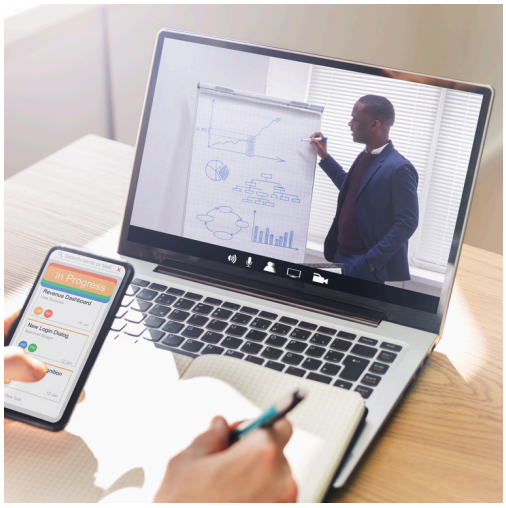
Sulabh Mishra has around 12+ years of experience in Cyber Security. He worked as Security tool administrator, Technical Consultant, Solutions Architect in the companies like Altisource, Accenture, Ericsson etc. Sulabh is Certified expert for Arcsight, Splunk, McAfee, Qradar and other SIEM tools as well as CEH, CISA and CISSP. He strongly believes that there is a huge demand in the market for Cyber Security now and near future and people should be well trained to take these new challenges to fulfil their job responsibilities.

SIEM XPERT
Learn. Secure. Succeed.

OUR STUDENTS WORK IN COMPANIES LIKE

The Best Companies

SIEM XPERT
Learn. Secure. Succeed.



CYBER SECURITY TRAININGS

- SOC Analyst
- Splunk SIEM
- Vulnerability Assessment
- Arcsight SIEM
- Microsoft Azure Sentinel
- IBM Qradar
- Certified Ethical Hacking (CEH)
- Threat Hunting
- CISSP, CISA and many more

splunk> ArcSight Azure Sentinel IBM QRadar

C|EH Certified Ethical Hacker

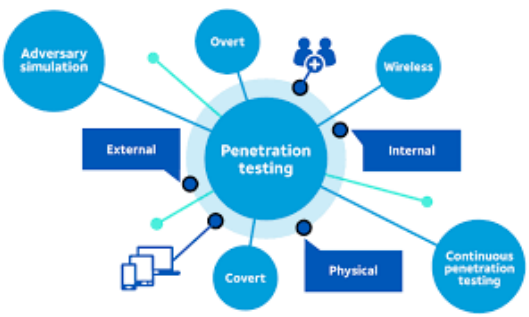
CISSP Certified Information Systems Security Professional

CISA Certified Information Systems Auditor. An ISACA Certification

SIEM XPERT
Learn. Secure. Succeed.

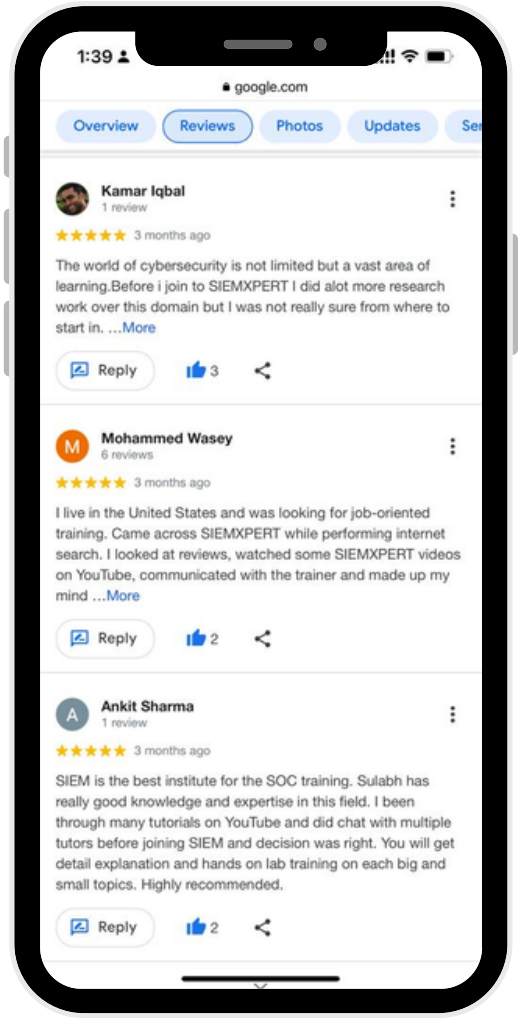
CYBER SECURITY SERVICES

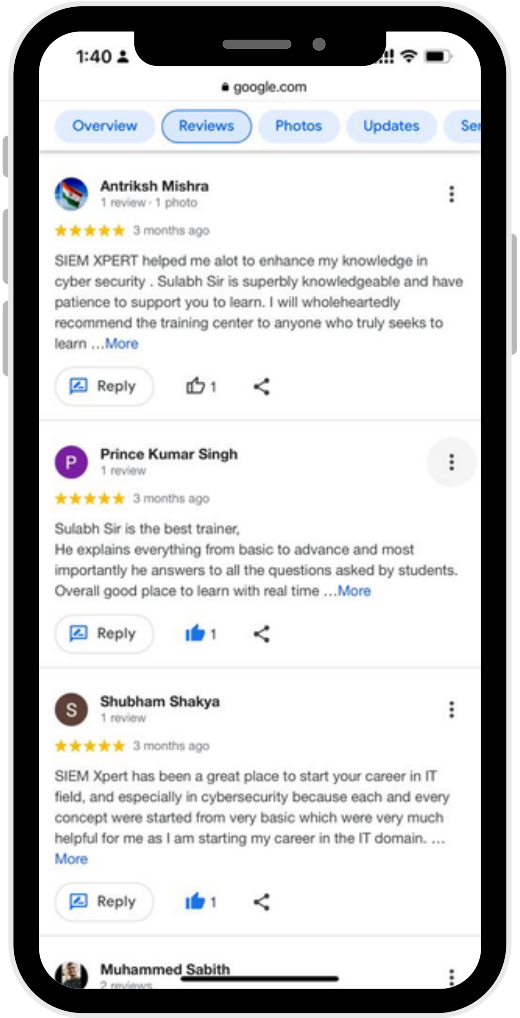
- Managed SOC Services
- Penetration services
- Security compliance and governance services
- and many more



WHAT OUR **TRAINEES** ARE SAYING

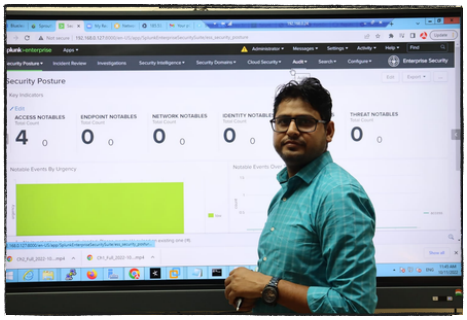
4.8 ★★★★★ **2031 Google reviews**





SIEM XPERT
Learn. Secure. Succeed.

SESSION-TIME AT **SIEM XPERT**



SIEM XPERT
Learn. Secure. Succeed.

SOME OF THE RECENTLY **PLACED TRAINEES**

Mahfooz Alam
Tata Communcations
(11.5 LPA)

Anand Dongre
Trojan Hunt
(11.5 LPA)

Ujjaval Srivas
Tata Advance
(7.5 LPA)

Ranjit Dhakad
SMBC
(8.7 LPA)

Mobbasar Khan
Tata Communcations
(9.5 LPA)

Ashish Pandey
Karvy Infotech
(7.5 LPA)

Kishor Nikam
Capgemini
(8.7 LPA)

Khushboo Tiwari
NSE 3
(11.5 LPA)

Shashidhar k
DriveIT
(6.6 LPA)

Abhishek Tiwari
Inspira
(8.8 LPA)

Sambit Padhy
Adani Group
(12.5 LPA)

Meenu Lal
HCL Technologies
(60 LPA)

SIEM XPERT
Learn. Secure. Succeed.

SOME OF THE RECENTLY **PLACED TRAINEES**

Hari Kumar
ATOS
(11.5 LPA)

Vidhi Jain
Aujas Cybersecurity
(13.5 LPA)

Vikram Rawat
KPMG
(32 LPA)

Arti Dekate
Mapple Cloud Technologies
(8.5 LPA)

Meenu Bhatt
TCS
(22.4 LPA)

Dheeraj Kumar
CMS IT
(7.5 LPA)

Sanjay Kumar
QOS Technologies
(12.5 LPA)

Amit Tiwari
Microland
(9.5 LPA)

Sangeetha R
IBM
(16 LPA)

Bharthi R
Ericsson
(13 LPA)

Swati Deshmukh
Deloitte
(17 LPA)

Ramkrishan Dubey
Sattrix
(12.5 LPA)

SIEM XPERT

Learn. Secure. Succeed.

No.1 Cyber security Training & Consulting services in India, US, UK & 30+ countries with 8+ years old Excellence.

For real-time Cyber Security trainings, contact us-

+91 9108318017

trainings@siemxpert.com

https://www.siemxpert.com

@siemxpert