SIEM XPERT
Learn. Secure. Succeed.

CTIA 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.

Mid-level to high-level cybersecurity professionals with a minimum of three years of experience.

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.

Individuals with EC-Council's C|EH and C|ND certifications can enroll in this course.

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.

CTIA CERTIFICATION (SYLLABUS)

Domain 1: Introduction to Threat Intelligence

1.1 Understanding Intelligence

- Definition of Intelligence and Its Essential Terminology
- Intelligence vs. Information vs. Data
- Intelligence-Led Security Testing (Background and Reasons)

1.2 Understanding Cyber Threat Intelligence

- Definition of Cyber Threat Intelligence
- Stages of Cyber Threat Intelligence
- Characteristics of Threat Intelligence
- Benefits of Cyber Threat Intelligence
- Enterprise Objectives for Threat Intelligence Programs
- How Can Threat Intelligence Help Organizations?
- Types of Threat Intelligence
  - Strategic Threat Intelligence
  - Tactical Threat Intelligence
  - Operational Threat Intelligence
  - Technical Threat Intelligence
- Threat Intelligence Generation
- Threat Intelligence Informed Risk Management
- Integration of Threat Intelligence into SIEM

SIEM XPERT
Learn. Secure. Succeed.

CTIA CERTIFICATION (SYLLABUS)

- Leverage Threat Intelligence for Enhanced Incident Response
  - Enhancing Incident Response by Establishing SOPs for Threat Intelligence
- Organizational Scenarios Using Threat Intelligence
- What Do Organizations and Analysts Expect?
- Common Information Security Organization Structure
- Responsibilities of Cyber Threat Analyst
- Threat Intelligence Use Cases

1.3 Overview of Threat Intelligence Lifecycle and Frameworks

- Threat Intelligence Lifecycle
- Role of Threat Analyst in Threat Intelligence Lifecycle
- Threat Intelligence Strategy
- Threat Intelligence Capabilities
- Capabilities to Look for in Threat Intelligence Solution
- Threat Intelligence Maturity Model
- Threat Intelligence Frameworks
  - Collective Intelligence Framework (CIF)
  - CrowdStrike Cyber Threat Intelligence Solution
  - NormShield Threat and Vulnerability Orchestration
  - MISP - Open-Source Threat Intelligence Platform
  - TC Complete™
  - Yeti
  - ThreatStream

SIEM XPERT
Learn. Secure. Succeed.

CTIA CERTIFICATION (SYLLABUS)

- Additional Threat Intelligence Frameworks

Domain 2: Cyber Threats and Kill Chain Methodology

2.1 Understanding Cyber Threats

- Overview of Cyber Threats
- Cyber Security Threat Categories
- Threat Actors/Profiling the Attacker
- Threat: Intent, Capability, Opportunity Triad
- Motives, Goals, and Objectives of Cyber Security Attacks
- Hacking Forums

2.2 Understanding Advanced Persistent Threats

- Definition of Advanced Persistent Threats
- Characteristics of Advanced Persistent Threats
- Advanced Persistent Threat Lifecycle

2.3 Understanding Cyber Kill Chain

- Cyber Kill Chain Methodology
- Tactics, Techniques, and Procedures
- Adversary Behavioral Identification
- Kill Chain Deep Dive Scenario - Spear Phishing

2.4 Understanding Indicators of Compromise

SIEM XPERT
Learn. Secure. Succeed.

CTIA CERTIFICATION (SYLLABUS)

- Indicators of Compromise
- Why Indicators of Compromise Important?
- Categories of Indicators of Compromise
- Key Indicators of Compromise
- Pyramid of Pain

Domain 3: Requirements, Planning, Direction, and Review

3.1 Understanding Organization's Current Threat Landscape

- Identify Critical Threats to the Organization
- Assess Organization's Current Security Pressure Posture
  - Assess Current Security Team's Structure and Competencies
  - Understand Organization's Current Security Infrastructure and Operations
- Assess Risks for Identified Threats

3.2 Understanding Requirements Analysis

- Map Out Organization's Ideal Target State
- Identify Intelligence Needs and Requirements
- Define Threat Intelligence Requirements
  - Threat Intelligence Requirement Categories
- Business Needs and Requirements
  - Business Units, Internal Stakeholders, and Third Parties
  - Other Teams

SIEM XPERT
Learn. Secure. Succeed.

CTIA CERTIFICATION (SYLLABUS)

- Intelligence Consumers Needs and Requirements
- Priority Intelligence Requirements
- Factors for Prioritizing Requirements
- MoSCoW Method for Prioritizing Requirements
- Prioritize Organizational Assets
- Scope of the Threat Intelligence Program
- 11. Rules of Engagement
- Non-disclosure Agreements
- Avoid Common Threat Intelligence Pitfalls

3.3 Planning a Threat Intelligence Program

- Prepare People, Processes, and Technology
- Develop a Collection Plan
- Schedule a Threat Intelligence Program
- Plan a Budget
- Develop a Communication Plan to Update Progress to Stakeholders
- Aggregate Threat Intelligence
- Select a Threat Intelligence Platform
- Consuming Intelligence for Different Goals
- Track Metrics to Keep Stakeholders Informed

3.4 Establishing Management Support

- Prepare Project Charter and Policy to Formalize the Initiative

SIEM XPERT
Learn. Secure. Succeed.

CTIA CERTIFICATION (SYLLABUS)

- Establish Your Case to Management for a Threat Intelligence Program
- Apply a Strategic Lens to the Threat Intelligence Program

3.5 Building a Threat Intelligence Team

- Satisfy Organizational Gaps with the Appropriate Threat Intelligence Team
  - Understand different Threat Intelligence Roles and Responsibilities
  - Identify Core Competencies and Skills
  - Define Talent Acquisition Strategy
  - Building and Positioning an Intelligence Team
  - How to Prepare an Effective Threat Intelligence Team

3.6 Overview of Threat Intelligence Sharing

- Establishing Threat Intelligence Sharing Capabilities
- Considerations for Sharing Threat Intelligence
- Sharing Intelligence with Variety of Organizations
- Types of Sharing Partners
- Important Selection Criteria for Partners
- Sharing Intelligence Securely

3.7 Reviewing Threat Intelligence Program

- Threat Intelligence-Led Engagement Review
- Considerations for Reviewing Threat Intelligence Program

SIEM XPERT
Learn. Secure. Succeed.

CTIA CERTIFICATION (SYLLABUS)

- Assessing the Success and Failure of the Threat Intelligence Program

Domain 4: Data Collection and Processing

4.1 Overview of Threat Intelligence Data Collection

- Introduction to Threat Intelligence Data Collection
- Data Collection Methods
- Types of Data
- Types of Threat Intelligence Data Collection

4.2 Overview of Threat Intelligence Collection Management

- Understanding Operational Security for Data Collection
- Understanding Data Reliability
- Ensuring Intelligence Collection Methods Produce Actionable Data
- Validate the Quality and Reliability of Third-Party Intelligence Sources
- Establish Collection Criteria for Prioritization of Intelligence Needs and Requirements
- Building a Threat Intelligence Collection Plan

4.3 Overview of Threat Intelligence Feeds and Sources

- Threat Intelligence Feeds
- Threat Intelligence Sources

SIEM XPERT
Learn. Secure. Succeed.

CTIA CERTIFICATION (SYLLABUS)

4.4 Understanding Threat Intelligence Data Collection and Acquisition

- Threat Intelligence Data Collection and Acquisition
- Data Collection through OpenSource Intelligence (OSINT)
  - Data Collection through Search Engines
  - Data Collection through Web Services
  - Data Collection through Website Footprinting
  - Data Collection through Emails
  - Data Collection through Whois Lookup
  - Data Collection through DNS Interrogation
  - Automating OSINT Effort Using Tools/Frameworks/ Scripts
- Data Collection through Human Intelligence (HUMINT)
  - Data Collection through Humanbased Social Engineering Techniques
  - Data Collection through Interviewing and Interrogation
  - Social Engineering Tools
- Data Collection through Cyber Counterintelligence (CCI)
  - Data Collection through Honeypots
  - Data Collection through Passive DNS Monitoring
  - Data Collection through Pivoting Off Adversary's Infrastructure
- Data Collection through Malware Sinkholes
- Data Collection through YARA Rules
- Data Collection through Indicators of Compromise (IoCs)
  - IoC Data Collection through External Sources

SIEM XPERT
Learn. Secure. Succeed.

CTIA CERTIFICATION (SYLLABUS)

- IoC Data Collection through Internal Sources
- Tools for IoC Data Collection through Internal Sources
- Data Collection through Building Custom IoCs
- Tools for Building Custom IoCs
- Steps for Effective Usage of Indicators of Compromise
- (IoCs) for Threat Intelligence

- Data Collection through Malware Analysis
  - Preparing Testbed for Malware Analysis
  - Data Collection through Static Malware Analysis
  - Data Collection through Dynamic Malware Analysis
  - Malware Analysis Tools
  - Tools for Malware Data Collection

4.5 Understanding Bulk Data Collection

- Introduction to Bulk Data Collection
- Forms of Bulk Data Collection
- Benefits and Challenges of Bulk Data Collection
- Bulk Data Management and Integration Tools

4.6 Understanding Data Processing and Exploitation

- Threat Intelligence Data Collection and Acquisition
- Introduction to Data Processing and Exploitation
- Structuring/Normalization of Collected Data
- Data Sampling
  - Types of Data Sampling
- Storing and Data Visualization
- Sharing the Threat Information

SIEM XPERT
Learn. Secure. Succeed.

CTIA CERTIFICATION (SYLLABUS)

Domain 5: Data Analysis

5.1 Overview of Data Analysis

- Introduction to Data Analysis
- Contextualization of Data
- Types of Data Analysis

5.2 Understanding Data Analysis Techniques

- Statistical Data Analysis
  - Data Preparation
  - Data Classification
  - Data Validation
  - Data Correlation
  - Data Scoring
  - Statistical Data Analysis Tools
- Analysis of Competing Hypotheses
  - Hypothesis
  - Evidence
  - Diagnostics
  - Refinement
  - Inconsistency
  - Sensitivity
  - Conclusions and Evaluation
- ACH Tool
  - PARC ACH

SIEM XPERT
Learn. Secure. Succeed.

CTIA CERTIFICATION (SYLLABUS)

- Structured Analysis of Competing Hypotheses
- Other Data Analysis Methodologies

5.3 Overview of Threat Analysis

- Introduction to Threat Analysis
- Types of Threat Intelligence Analysis

5.4 Understanding the Threat Analysis Process

- Threat Analysis Process and Responsibilities
- Threat Analysis Based on Cyber Kill Chain Methodology
- Aligning the Defensive Strategies with the Phases of the Cyber Kill Chain Methodology
- Perform Threat Modeling
  - Asset Identification
  - System Characterization
  - System Modeling
  - Threat Determination and Identification
  - Threat Profiling and Attribution
  - Threat Ranking
  - Threat Information Documentation
- Threat Modeling Methodologies
  - STRIDE
  - PASTA
  - TRIKE
  - VAST
  - DREAD
  - OCTAVE

SIEM XPERT
Learn. Secure. Succeed.

CTIA CERTIFICATION (SYLLABUS)

- Threat Modeling Tools
  - Microsoft Threat Modelling Tool
  - ThreatModeler
  - securiCAD Professional
  - IriusRisk
- Enhance Threat Analysis Process with the Diamond Model Framework
- Enrich the Indicators with Context
- Validating and Prioritizing Threat Indicators

5.5 Overview of Fine-Tuning Threat Analysis

- Fine-Tuning Threat Analysis
- Identifying and Removing Noise
- Identifying and Removing Logical Fallacies
- Identifying and Removing Cognitive Biases
- Automate Threat Analysis Processes
- Develop Criteria for Threat Analysis Software
- Employ Advanced Threat Analysis Techniques
  - Machine Learning-Based Threat Analysis
  - Cognitive-Based Threat Analysis

5.6 Understanding Threat Intelligence Evaluation

- Threat Intelligence Evaluation
- Threat Attribution

SIEM XPERT
Learn. Secure. Succeed.

CTIA CERTIFICATION (SYLLABUS)

5.7 Creating Runbooks and Knowledge Base

- Developing Runbooks
- Create an Accessible Threat Knowledge Base
- Organize and Store Cyber Threat Information in Knowledge Base

5.8 Overview of Threat Intelligence Tools

- Threat Intelligence Tools
  - AlienVault® USM® Anywhere
  - IBM X-Force Exchange
  - ThreatConnect
  - SurfWatch Threat Analyst
  - AutoFocus
  - Additional Threat Intelligence Tools

Domain 6: Intelligence Reporting and Dissemination

6.1 Overview of Threat Intelligence Reports

- Threat Intelligence Reports
- Types of Cyber Threat Intelligence Reports
  - Threat Analysis Reports
  - Threat Landscape Reports
- Generating Concise Reports
- Threat Intelligence Report Template

SIEM XPERT
Learn. Secure. Succeed.

CTIA CERTIFICATION (SYLLABUS)

- How to Maximize the Return from Threat Intelligence Report
- Continuous Improvement via Feedback Loop
- Report Writing Tools
  - MagicTree
  - KeepNote

6.2 Introduction to Dissemination

- Overview of Dissemination
- Preferences for Dissemination
- Benefits of Sharing Intelligence
- Challenges to Intelligence Sharing
- Disseminate Threat Intelligence Internally
- Building Blocks for Threat Intelligence Sharing
- Begin Intelligence Collaboration
- Establish Information Sharing Rules
- Information Sharing Model
- Information Exchange Types
- TI Exchange Architectures
- TI Sharing Quality
- Access Control on Intelligence Sharing
- Intelligence Sharing Best Practices

6.3 Participating in Sharing Relationships

- Why Sharing Communities are Formed?
- Join a Sharing Community

SIEM XPERT
Learn. Secure. Succeed.

CTIA CERTIFICATION (SYLLABUS)

- Factors to be Considered When Joining a Community
- Engage in Ongoing Communication
- Consume and Respond to Security Alerts
- Consume and Use Indicators
- Produce and Publish Indicators
- External Intelligence Sharing
- Establishing Trust
- Organizational Trust Models

6.4 Overview of Sharing Threat Intelligence

- Sharing Strategic Threat Intelligence
- Sharing Tactical Threat Intelligence
- Sharing Operational Threat Intelligence
- Sharing Technical Threat Intelligence
- Sharing Intelligence Using YARA Rules
- IT-ISAC (Information Technology - Information Security and Analysis Center)

6.5 Overview of Delivery Mechanisms

- Forms of Delivery
- Machine-Readable Threat Intelligence
- Standards and Formats for Sharing Threat Intelligence
  - Traffic Light Protocol (TLP)
  - MITRE Standards
  - Managed Incident Lightweight Exchange (MILE)
  - VERIS and IDMEF

SIEM XPERT
Learn. Secure. Succeed.

CTIA CERTIFICATION (SYLLABUS)

6.6 Understanding Threat Intelligence Sharing Platforms

- Information Sharing and Collaboration Platforms
  - Blueliv Threat Exchange Network
  - Anomali STAXX
  - MISP (Malware Information Sharing Platform)
  - Cyware Threat Intelligence eXchange (CTIX)
  - Soltra Edge
  - Information Sharing and Collaboration Platforms

6.7 Overview of Intelligence Sharing Acts and Regulations

- Cyber Intelligence Sharing and Protection Act (CISPA)
- Cybersecurity Information Sharing Act (CISA)

6.8 Overview of Threat Intelligence Integration

- Integrating Threat Intelligence
- How to Integrate CTI into the Environment
- Acting on the Gathered Intelligence
- Tactical Intelligence Supports IT Operations: Blocking, Patching, and Triage
- Operational Intelligence Supports Incident Response: Fast Reaction and Remediation
- Strategic Intelligence Supports Management: Strategic Investment and Communications

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

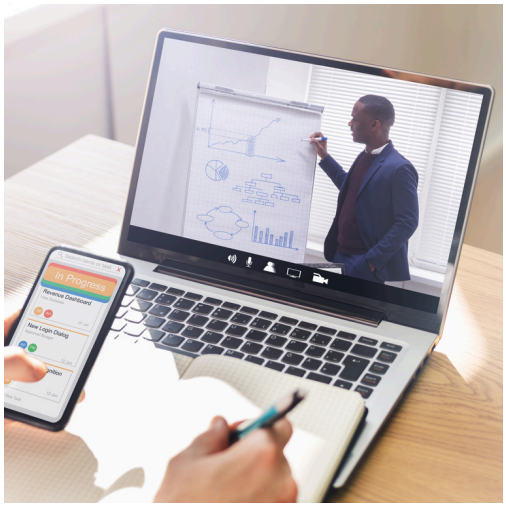
Sulabh Mishra has around 12+ years of experience in Cyber Security. He worked as Security tool administrator, Technical Consultant, Solutions Architect in the companies like Altisource, Accenture, Ericsson etc. Sulabh is Certified expert for Arcsight, Splunk, McAfee, Qradar and other SIEM tools as well 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

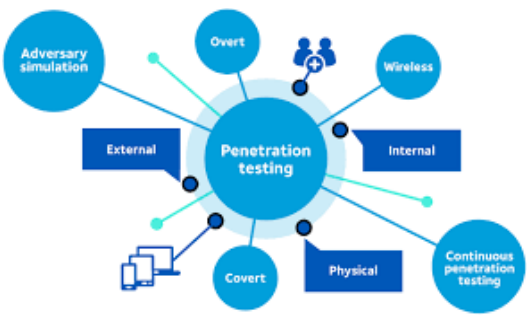
CISSP Certified Information Systems Security Professional

CISA Certified Information Systems Auditor. An ISACA Certification

SIEM XPERT
Learn. Secure. Succeed.

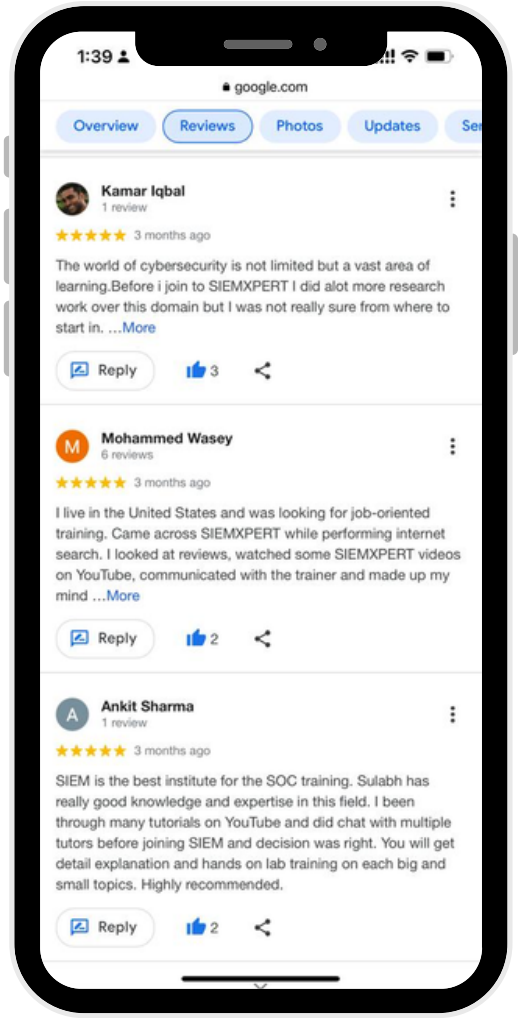
CYBER SECURITY SERVICES

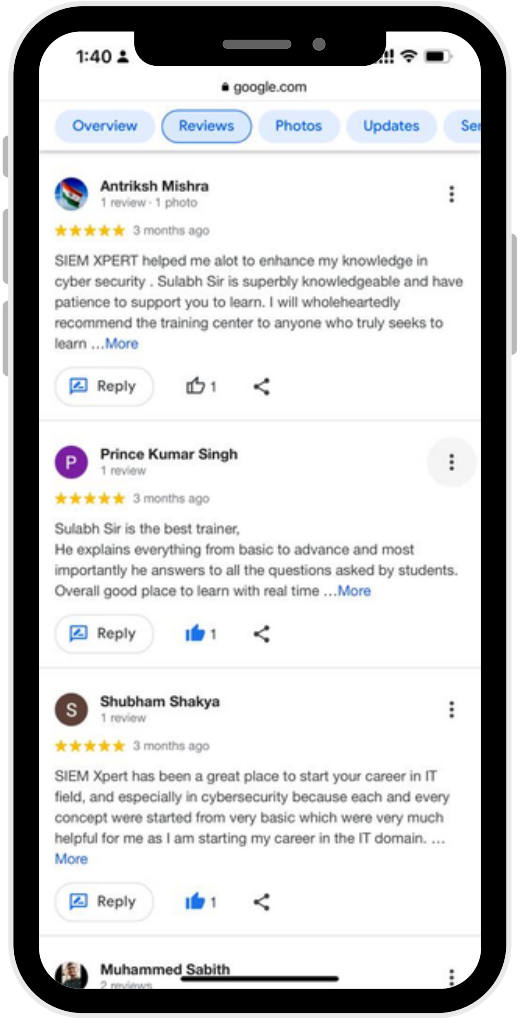
- Managed SOC Services
- Penetration services
- Security compliance and governance services
- and many more



WHAT OUR **TRAINEES** ARE SAYING

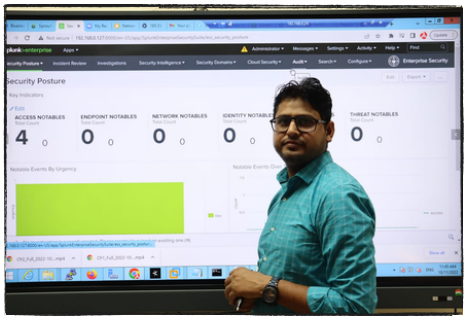
4.8 ★★★★★ **2031 Google reviews**





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