SIEM XPERT
Get trained today !

CORTEX XSOAR WITH PYTHON SYLLABUS

SIEM XPERT

Best CyberSecurityInstitution in India

Committed to QUALITY, Committed to YOU.

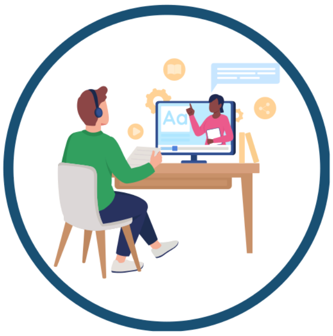
trainings@siemxpert.com • www.siemxpert.com • +91 9108318017

SIEM XPERT
Get trained today !

OUR **STATISTICS**

50,000+

Trainees
across the globe



24*7

Real-Time Lab
Setup, Accessible
From Anywhere

60%

Average Salary
Hike

65 LPA

Highest
Package

3.5M

Job openings
in 2025

SIEM XPERT
Get trained today !

WHO CAN **JOIN THE COURSE?**

SIEMXPERTwas founded with an intentionto 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.

This course is for individuals who seek an overall understanding of the SOAR (security orchestration, automation, and response).

This course also helps you prepare for the Palo Alto Cortex XSOAR exam.

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.

You will learn about SOAR concepts, architecture, pricing, and support to build your Palo Alto Cortex SOAR Cloud knowledge.

CORTEX SOAR (SYLLABUS)

- What is SOAR
- What does SOAR consist of
- What can be integrated with SOAR
- Benefits of SOAR in Today’s SOC
- SOAR Architecture
  - System Hardware Requirements
  -Remote Repositories (dev-prod)
  - Engines
  - Multi Tenancy
  - Elasticsearch/HA
  - Docker
- Describe the Incident Lifecycle within XSOAR

Module 2: Basic Python coding

- Python Introduction and Setting up the Environment .Introduction to Programming
- Python Basic Syntax and Data Types Input/output, Comments, Variables, Data types
- Operators in PythonArithmetic, Assignment, Comparison, Logical, Identity, Membership

CORTEX SOAR (SYLLABUS)

- Strings inPython--Creating,Formatting, Indexing, Slicing, String methods
- Lists in Python-- Creating, Properties, Indexing, Slicing, Methods, Modifying lists
- Tuples in Python-- Syntax, Properties, Indexing
- Sets in Python --Syntax, Updating
- Dictionaries in Python -- Syntax, Keys/values, Accessing, Methods
- Python Conditional Statements -- if, if-else, if-elif-else
- Loops in Python -- while, for, break, continue, pass, range
- List and Dictionary Comprehensions -- Syntax, Uses

Module 3: Playbook Development

- Reference and manipulate context data to manage automation workflow
- Summarize inputs, outputs, and results for playbook tasks
- Configure Inputs and Outputs for Sub-playbooks Tasks
- Enable and Configure Looping on a Sub-playbook
- Differentiate among Playbook Task Types
  - Manual
  - Automated
  - Conditional
  - Data Collection
  - Sub-Playbook

CORTEX SOAR (SYLLABUS)

- Apply filtersandtransformers to manipulate data
- Apply the Playbook Debugger to Aid in Development Playbooks

Module 4: Incident Objects

- Configure Incident Types
- Identify the Role of an Incident Type within the Incident Lifecycle
- Configure an Incident Layout
  - Fields and Buttons
  - Tabs
  - New/Edit and Close Forms
- Summarize the Function, Capabilities, and Purpose of Incident Fields
- Configure Classifier and Mappers

Module 5: Automations, Integrations & Related Concepts

- Define the Capabilities of Automation across XSOAR Functions
  - Playbook Tasks
  - War Room

CORTEX SOAR (SYLLABUS)

- Layouts(DynamicSections,Buttons)
- Jobs
- Field Trigger Scripts
- Pre/Post-Processing

- Differentiate between Automations, Commands, and Scripts
- Interpret and Modify Automation Scripts
  - Script Helper
  - Script Settings
  - Language Types
- Identify the Properties and Capabilities of the XSOAR Framework for Integration
- Configure and Manage Integration Instances

Module 6: Content Management & Solution Architecture

- Apply Marketplace Concepts for the Management of Content
  - Searching in Marketplace
  - Installation and Updates
  - Dependencies
  - Version History
  - Partner-supported Versus XSOAR-supported
  - Submitting Content to the Marketplace

SIEM XPERT
Get trained today !

CORTEX SOAR (SYLLABUS)

- Apply General Content Customization and Management Concepts
  - Custom versus System Content
  - Duplicating Content
  - Importing/Exporting Custom Content
  - Version Control
- Manage Local Changes in a Remote Repository (dev-prod) Configuration
- Describe the Components of the XSOAR System Architecture
- Define the Capabilities of RBAC
  - Page Access
  - Integration Permissions
  - Incident Tabs (Layout Specification)
  - Automation Permissions,
  - Incident Viewing Permission by Role
- Identify the Troubleshooting Tools Available to Obtain More Diagnostic Information
  - Log Bundles
  - Integration Testing
- Identify Options Available for Performance Tuning
  - Ignore Output
  - Quiet Mode
- Monitor System Health using the System Diagnostic Page

CORTEX SOAR (SYLLABUS)

Module 7: UI Workflow, Dashboards, and Reports

- Identify Methods for Querying Data
  - Indicators
  - Incidents
  - Dashboards
  - Global Search
- Summarize the Workflow Elements used during an Investigation
  - Layouts
  - War Room
  - Work Plan
  - Evidence Board
  - Actions Menu
- Interact with Layouts for Incident Management
  - Sections
  - Fields
  - Buttons
- Summarize Tools used for Managing Incidents
  - Bulk Incident Actions
  - Table View versus Summary View
  - Table Settings
- Identify the Capabilities of Existing Dashboards and Reports

SIEM XPERT

Get trained today !

CORTEX SOAR (SYLLABUS)

- Summarize whatInformation can be Created, Edited, or Shared within Dashboards and Reports
- Summarize the Capabilities of the Widget Builder

Module 8: Threat Intel Management

- Identify the Parameters Available for Configuring Indicator Objects
  - Layouts and Types
  - Fields
  - Reputation Scripts and Command
  - Expiration
- Generate Threat Intel Reports
- Describe the Features of the Threat Intel Page
  - Unit 42 Intel Feature
  - XSOAR Indicators
  - Export/Import Capabilities
- Configure Threat Intel Feed Integrations
- Identify the Options Available to Auto Extract
  - Exclusion List
  - Playbook Auto Extract
  - Regex for Auto Extract

SIEM XPERT
Get trained today !

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 XPERT
Get trained today !

SULABH MISHRA

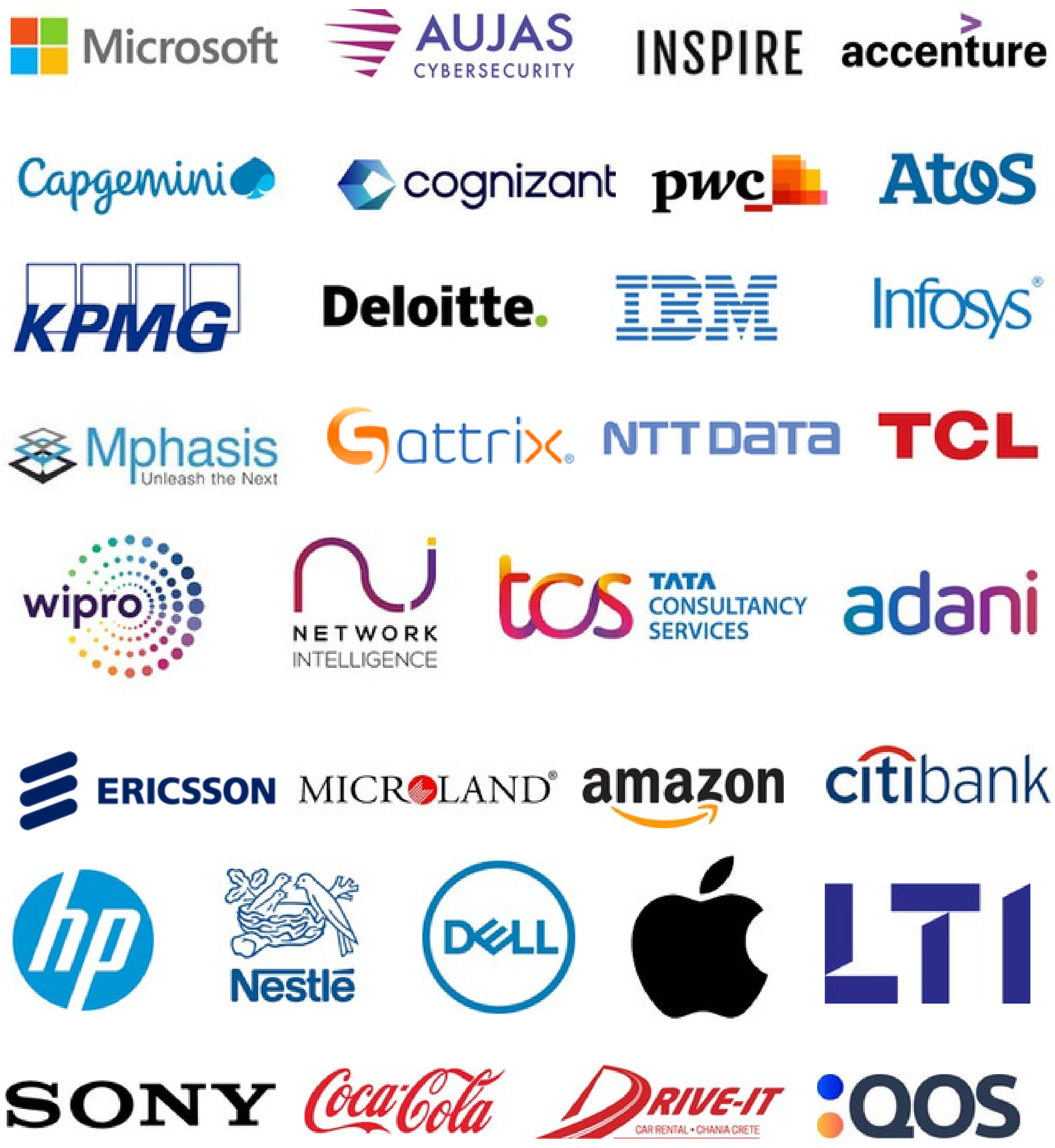
CEO,Cyber Security Trainer & Solution Architect

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
Get trained today !

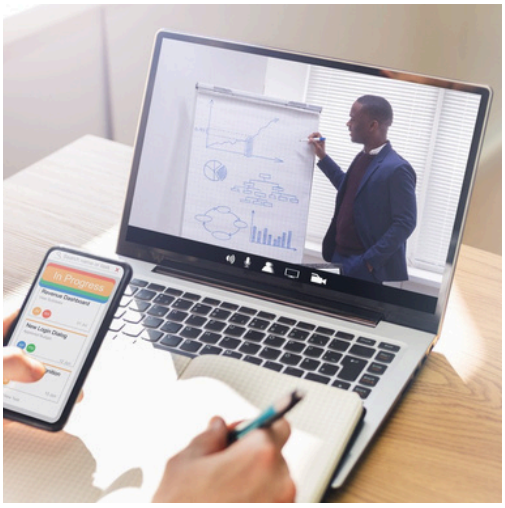
OUR STUDENTS WORK IN COMPANIES LIKE

The Best Companies



SIEM XPERT

Get trained today !



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

CEH Certified Ethical Hacker

CISSP Certified Information Systems Security Professional

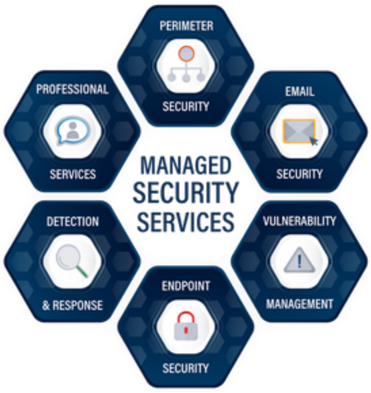
CISA Certified Information Systems Auditor. An ISACA Certification

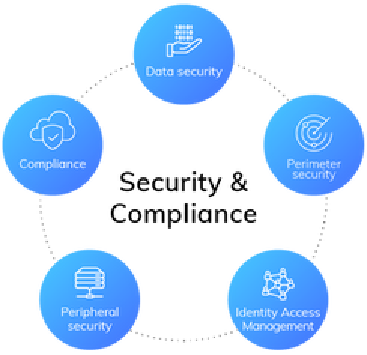
SIEM XPERT

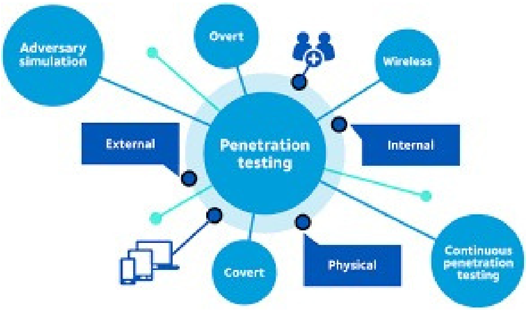
Get trained today !

CYBER SECURITY SERVICES

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





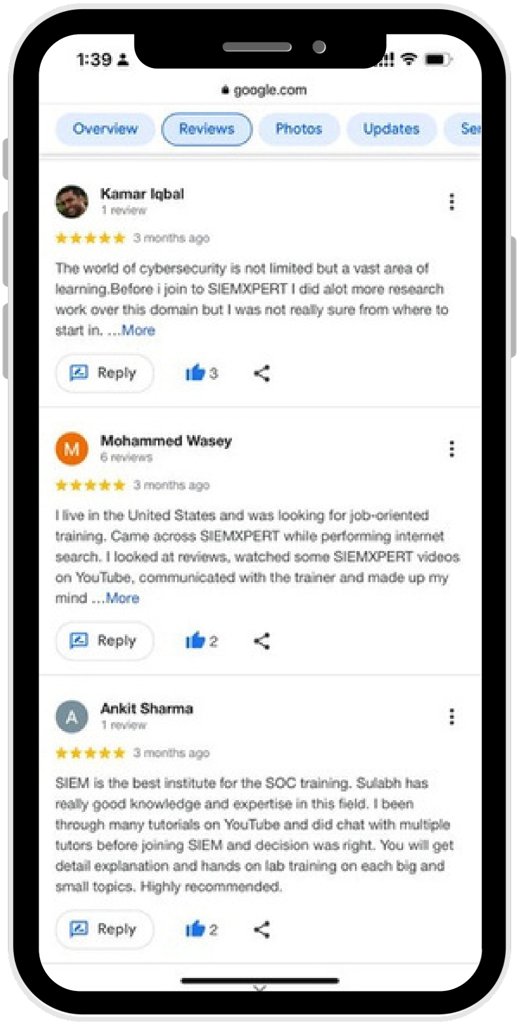


SIEM XPERT
Get trained today !

Google
Customer Reviews ★★★★★

WHAT OUR **TRAINEES** ARE SAYING

4.9 ★★★★★ **2022 Google reviews**



Kamar Iqbal
1 review
★★★★★ 3 months ago

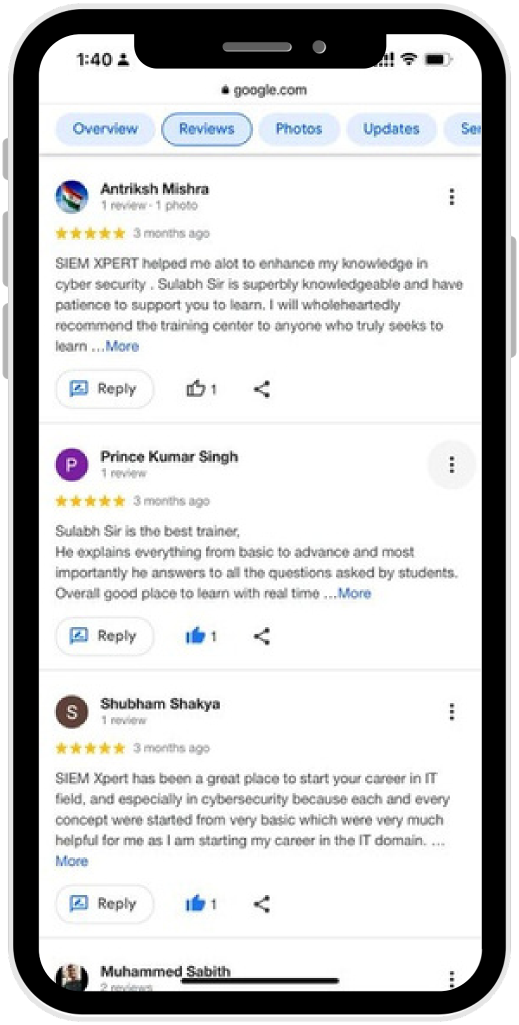
The world of cybersecurity is not limited but a vast area of learning.Before i join to SIEMXPERT I did alot more research work over this domain but I was not really sure from where to start in. ...More

Mohammed Wasey
6 reviews
★★★★★ 3 months ago

I live in the United States and was looking for job-oriented training. Came across SIEMXPERT while performing internet search. I looked at reviews, watched some SIEMXPERT videos on YouTube, communicated with the trainer and made up my mind ...More

Ankit Sharma
1 review
★★★★★ 3 months ago

SIEM is the best institute for the SOC training. Sulabh has really good knowledge and expertise in this field. I been through many tutorials on YouTube and did chat with multiple tutors before joining SIEM and decision was right. You will get detail explanation and hands on lab training on each big and small topics. Highly recommended.



Antriksh Mishra
1 review · 1 photo
★★★★★ 3 months ago

SIEM XPERT helped me alot to enhance my knowledge in cyber security . Sulabh Sir is superbly knowledgeable and have patience to support you to learn. I will wholeheartedly recommend the training center to anyone who truly seeks to learn ...More

Prince Kumar Singh
1 review
★★★★★ 3 months ago

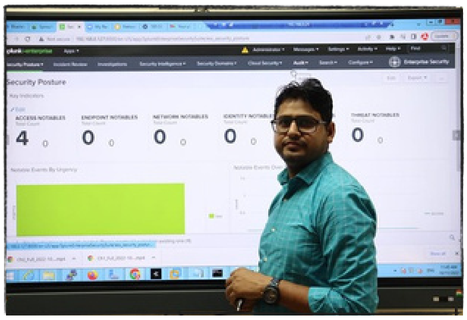
Sulabh Sir is the best trainer,
He explains everything from basic to advance and most importantly he answers to all the questions asked by students. Overall good place to learn with real time ...More

Shubham Shakya
1 review
★★★★★ 3 months ago

SIEM Xpert has been a great place to start your career in IT field, and especially in cybersecurity because each and every concept were started from very basic which were very much helpful for me as I am starting my career in the IT domain. ... More

Muhammed Sabith
2 reviews

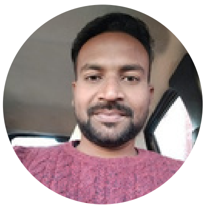
SESSION-TIME AT **SIEM XPERT**



SIEM XPERT
Get trained today !

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)

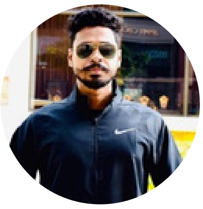
Ashish Pandey
Karvy Infotech
(7.5 LPA)

Kishor Nikam
Capgemini
(8.7 LPA)

Khushboo Tiwari
NSE3
(11.5 LPA)

Shashidhar k
DriveIT
(6.6 LPA)

Abhishek Tiwari
Inspira
(8.8 LPA)

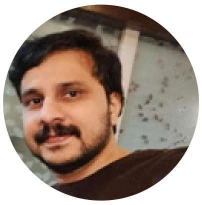


Sambit Padhy
Adani Group
(12.5 LPA)

Meenu Lal
HCL Technologies
(60 LPA)

SIEM XPERT
Get trained today !

SOME OF THE RECENTLY **PLACED TRAINEES**

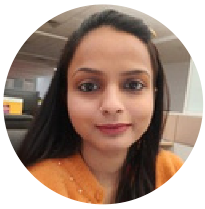


Hari Kumar
ATOS
(11.5 LPA)

Vidhi Jain
Aujas Cybersecurity
(13.5 LPA)

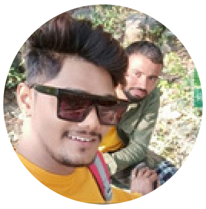
Vikram Rawat
KPMG
(32 LPA)

Arti Dekate
MappleCloud Technologies
(8.5 LPA)



Meenu Bhatt
TCS
(22.4 LPA)

Dheeraj Kumar
CMSIT
(7.5 LPA)



Sanjay Kumar
QOSTechnologies
(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

Get trained today !

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