SIEM XPERT
Learn. Secure. Succeed.

SPLUNK ADMIN & SPLUNK ENTERPRISE SECURITY SYLLABUS

SIEM XPERT

Best Cyber Security Institution in India

Committed to QUALITY, Committed to YOU.

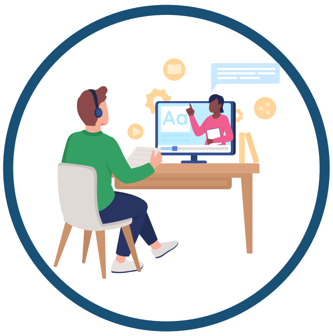
trainings@siemxpert.com • www.siemxpert.com • +91 9108318017

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

WHO CAN **JOIN THE COURSE?**

SIEM XPERT was created 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.

People who are looking to Switch their career to Cyber Security and SIEM or wants to enhance their knowledge on Splunk Enterprise Security.

People who have gap in their career and want to get high paying Jobs in MNCs.

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 wants to enhance their knowledge in SIEM and SOC.

SIEM XPERT
Learn. Secure. Succeed.

WHAT **YOU'LL BE LEARNING** IN THIS COURSE?

- Trainer has 10+ Years of experience in Cyber Security and has done end to end deployment of many SIEM like Splunk, Qradar, ArcSight, McAfee and other Security tools for many companies.

- Our training is completely real-time Job oriented training what exactly experienced people are doing in the company on the Splunk all we are going to cover here and you are going to the hands-on practice on the lab environment so that confidently you can work as an experienced.

- Hands-on lab access for 45- days on Splunk Environment.

- Customized documents will be shared for Splunk Admin so that you can work in the companies without any issues.

- It’s completely interactive Splunk tutorial training, happens though videos conferencing, trainer will be Infront of you, you will feel like physical class, you can ask n-number of questions.

- You should be having hands-on on Splunk Enterprise and searching &reporting or attended hands-on training on Spunk Admin and knows searching and reporting on Splunk.

SPLUNK ADMINISTRATION TRAINING (SYLLABUS)

1. Splunk Administration Training

- Use of Splunk as a Data Analytics and as a Splunk SIEM.
- Products of Splunk
- Splunk Enterprise
- Splunk Cloud

2. Understanding of various components of SPLUNK

- Splunk Forwarders
- Universal forwarder
- Heavy Forwarder
- Indexer
- Search head

3. Splunk Deployment Architecture

- Single instance All-in on Architecture of Splunk
- Distributed Architecture of Splunk
- License master
- Deployment server

SPLUNK ADMINISTRATION TRAINING (SYLLABUS)

4. Splunk Licensing

- Identify license types
- License requirement of each component of Splunk
- Understand of license violations
- Estimation of license requirements

5. Designing real-time Splunk Architecture for a customer

- Evaluate the core functionality of the SIEM customer is looking for
- Understand the customer data center and devices distribution
- Collect the device list based on required format
- Calculation of estimate EPS
- Evaluation of license requirement
- Evaluation of type Splunk Architecture Requirement
- Evaluate which data center which components have to be deployed
- Evaluation of Storage requirement
- Evaluation of Server operating system requirement
- Evaluation of RAM and CPU requirement
- Installation of Splunk Components
- Installation of Splunk Components

SPLUNK ADMINISTRATION TRAINING (SYLLABUS)

- Installation of Search Head
- Installation of Heavy Forwarder
- Configuring License Master
- Configuring the communication between all components of Splunk

6. Introduction of Splunk GUI

- Overview of Splunk Web
- Understanding Various options available on Splunk Web

7. Splunk Configuration Files

- Understanding Splunk Configuration Directory structure
- Understanding different configuration files in Splunk
- How to change configuration using configuration files
- Using Btool to validate configuration setting Splunk Apps and Addon
- Understand the use of Splunk Addon
- Understand the use of Splunk Apps
- Installation and configuration of Addon & Apps

SPLUNK ADMINISTRATION TRAINING (SYLLABUS)

8. Data Source Onboarding/Integration in Splunk – real-time on the lab practical

- Three-phase of the Splunk Indexing process
- Understanding Microsoft Windows Integration
- Integration of Windows devices using WMI mechanism
- Integration of Windows Device Using Universal forwarder
- Installation of Universal Forwarder
- Understanding of Syslog Integration with Splunk
- Integration of Linux devices
- Integration of Firewalls
- Understanding the Integration of any kind of devices with Splunk from SIEM perspective
- Understand HTTP event collector
- Understand scripted input

9. Splunk Indexes

- What is Index in Splunk
- What is bucket and type of buckets in Splunk
- Describe Index structure

SPLUNK ADMINISTRATION TRAINING (SYLLABUS)

- Check index data integrity
- Describe index.conf options
- Applying data retention policies
- Distributed Search In Splunk
- Understand how distributed search works
- Understand the role of the search head & search peers
- Configuring a distributed search group
- Understand search head scaling option

10. Configuring Forwarders

- Understand the use of Deployment management
- Describe Splunk Deployment Server
- Managing Forwarders by deployment apps
- Configuring deployment clients
- Configuring clients groups
- Configuring clients groups

11. Splunk Forwarder Management

- Configure Forwarders
- Understand additional Forwarder options

SPLUNK ADMINISTRATION TRAINING (SYLLABUS)

12. Splunk User Management

- Understanding Splunk User Roles
- Creating Custom Roles
- Creating new users and Assigning Roles

13. Searching and Reporting in Splunk

- Plunk searching Modes
- Using Field Search
- Using Operators Search
- Using SPL commands
- Creating Reports
- Creating Alerts In Splunk Alert Actions
- Creating Dashboards

14. Splunk Knowledge Objects

- Event types creation and permission
- Event types Use Cases
- Tags Creation
- Lookups Creation in Splunk
- Lookups Use Case Example

SPLUNK ADMINISTRATION TRAINING (SYLLABUS)

15. Splunk Troubleshooting

- Troubleshooting of Splunk enterprise
- Troubleshooting of Log Stoppage issues
- Well known issues in Splunk

SPLUNK ENTERPRISE SECURITY (SYLLABUS)

- Why do we need Splunk Enterprise Security Application/ Splunk SIEM?
- Overview of Splunk enterprise Security console
- Planning of Splunk Enterprise Deployment
- Downloading Splunk Enterprise Security from Splunk website
- Deploying enterprise security app over the search head
- Configuration of Enterprise Security App

SIEM XPERT
Learn. Secure. Succeed.

SPLUNK ENTERPRISE SECURITY (SYLLABUS)

- Overview of various out of the box dashboards in Splunk Enterprise Security
- Understanding and creating Correlation
- Searches/Correlation Rules in Splunk
- Looking at the various options available in Correlation searches
- Understanding and creating Adaptive response action in Splunk Enterprise Security
- Monitoring real-time security incidents
- Analyzing security incidents
- Moving the incidents to investigation tabs and dig down the investigation
- Verifying whether the incident is true positive or false positive
- Creating the incidents on Service Now ticketing tool
- Reporting the incidents over the email
- Understanding the Shift Handover
- Understanding the various report being created and sent to the clients
- Understand daily reporting and monthly reporting in SOC
- Understanding and creating SOC shift handover
- And much more...

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.

SIEM XPERT
Learn. Secure. Succeed.

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.

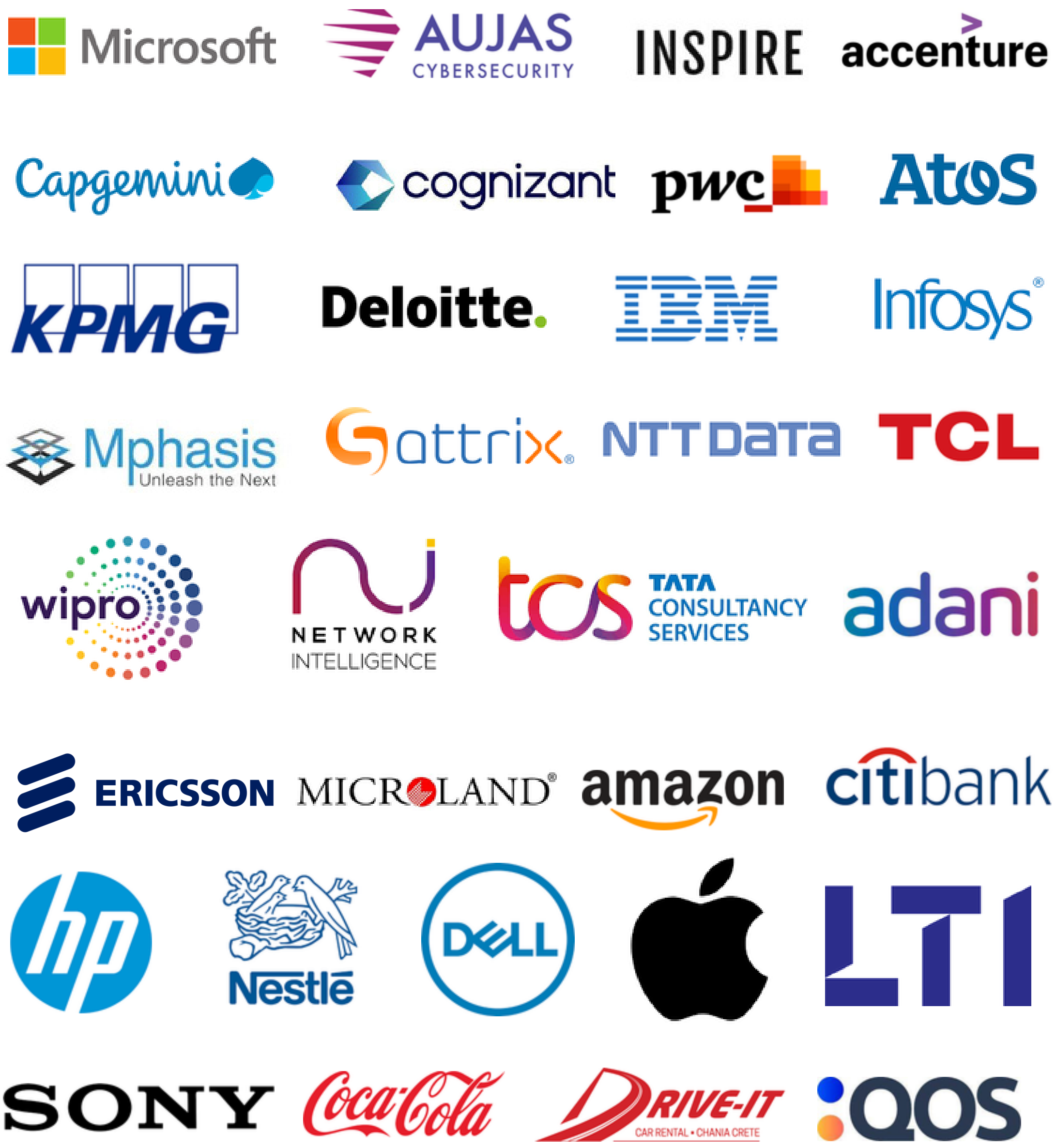
SULABH MISHRA

CEO, Cyber Security Trainer & Solution Architect

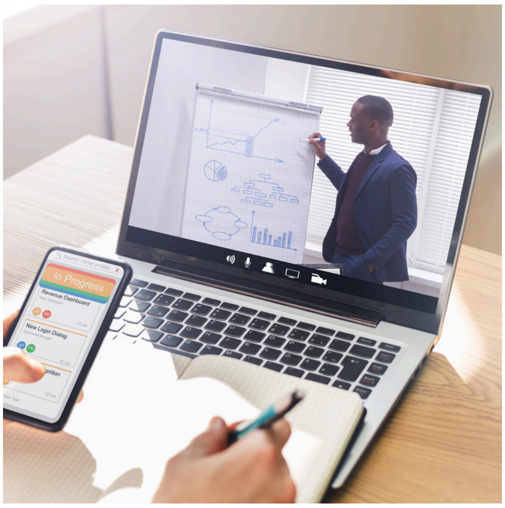
Sulabh Mishra has around 12+ years of experience in Cyber Security. He worked as Security tool administrator, Technical Consultant, Solutions Architect in the companies like Altisource, Accenture, Ericsson etc. Sulabh is Certified expert for Arcsight, Splunk, McAfee, Qradar and other SIEM tools as well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

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

CEH Certified Ethical Hacker

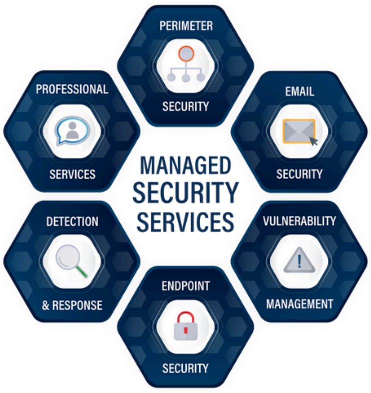
CISSP Certified Information Systems Security Professional

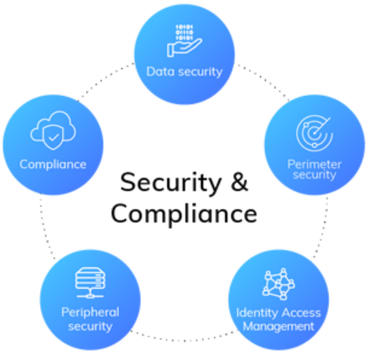
CISA Certified Information Systems Auditor. An ISACA Certification

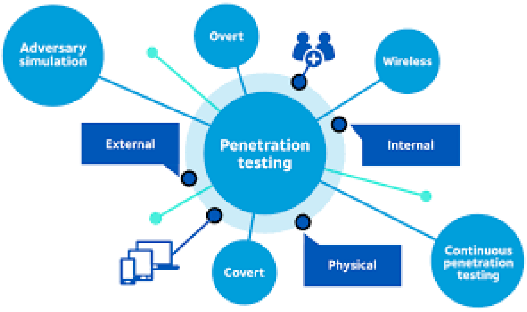
SIEM XPERT
Learn. Secure. Succeed.

CYBER SECURITY SERVICES

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

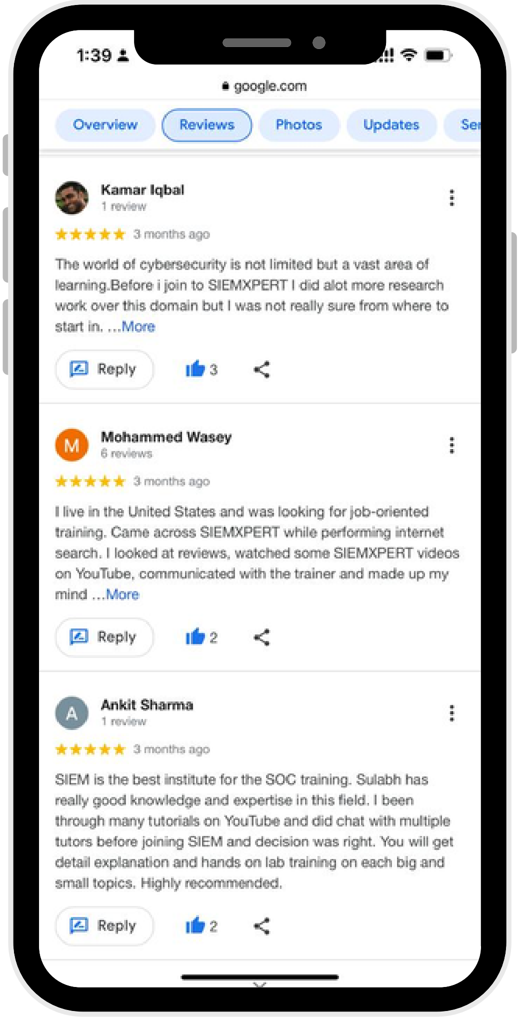






WHAT OUR **TRAINEES** ARE SAYING

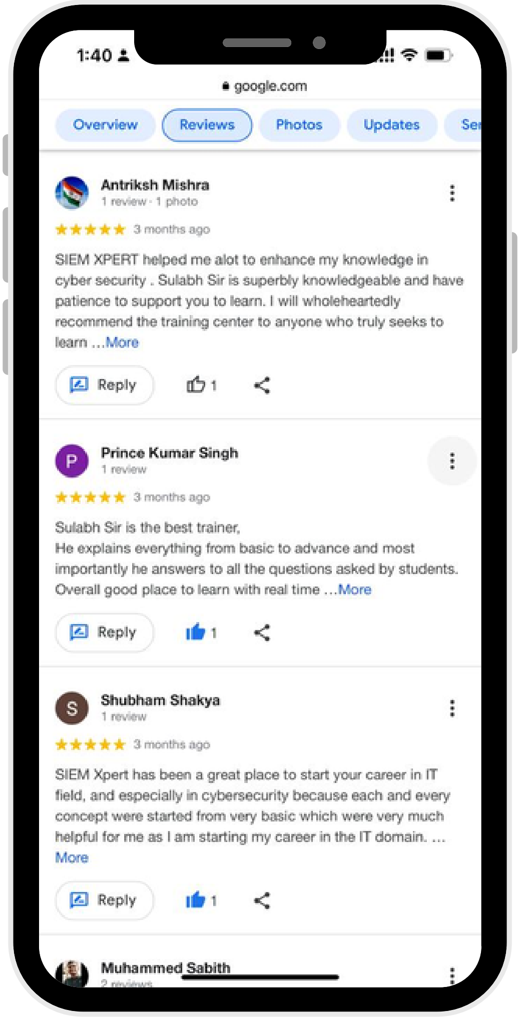
4.8 ★★★★★ **2031 Google reviews**


1:39
google.com
Overview | Reviews | Photos | Updates | Se

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
Reply 👍 3

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
Reply 👍 2

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.
Reply 👍 2


1:40
google.com
Overview | Reviews | Photos | Updates | Se

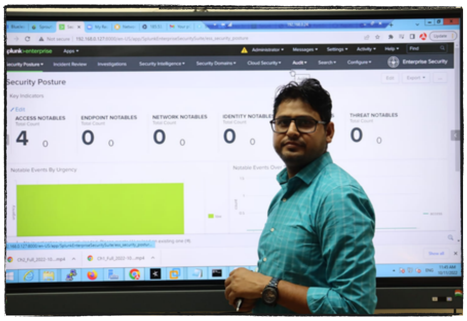
Antriksh Mishra
1 review · 1 photo
★★★★★ 3 months ago
SIEM XPERT helped me alot to enhance my knowledge in cyber security . Sulabh Sir is superbly knowledgeable and have patience to support you to learn. I will wholeheartedly recommend the training center to anyone who truly seeks to learn ...More
Reply 👍 1

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
Reply 👍 1

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
Reply 👍 1

Muhammed Sabith
2 reviews

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