SIEM XPERT
Learn. Secure. Succeed.

Microsoft Sentinel

MICROSOFT SENTINEL 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.

- **Cybersecurity Professionals** – SOC analysts, incident responders, and threat hunters looking to enhance their SIEM and SOAR skills.
- **IT Administrators & Security Engineers** – Professionals managing security operations and infrastructure who want to integrate Microsoft Sentinel into their security stack.
- **Beginners in Cybersecurity** – Individuals looking to start a career in security operations and SIEM with no prior experience required.
- **Cloud & Network Security Specialists** – Those working with Azure and cloud security who want to leverage Sentinel for threat detection and response.
- **Penetration Testers & Red Teamers** – Professionals interested in understanding how organizations monitor, detect, and respond to attacks.

SIEM XPERT
Learn. Secure. Succeed.

MICROSOFT SENTINEL TRAINING (SYLLABUS)

Module 1: Introduction to Cloud & Azure Fundamentals

- What is Cloud Computing?
- Cloud Service Models: IaaS, PaaS, SaaS
- Public, Private, and Hybrid Cloud
- Why Cloud Security Matters?
- Security Challenges in Cloud Environments
- Introduction to Microsoft Azure
- Key Azure Services: Azure AD, Azure Security Center, Azure Monitor
- Azure Resource Management & Role-Based Access Control (RBAC)
- Hands-on Practice
- Creating a Free Azure Account
- Navigating the Azure Portal

Module 2: Introduction and understanding of Microsoft Sentinel Architecture

- What is Microsoft Sentinel?
- SIEM vs. SOAR – Understanding the Differences
- How Microsoft Sentinel Fits into Azure Security

SIEM XPERT
Learn. Secure. Succeed.

- Microsoft Sentinel Architecture & Components
- Understanding Data Connectors & Log Ingestion
- Hands-on Lab: Setting Up a Microsoft Sentinel Workspace

Module 3: Data Ingestion & Log Sources

- Understanding Data Connectors & Log Ingestion
- Connecting Data Sources to Microsoft Sentinel
- Integrating Microsoft Defender, O365, Azure AD, & Other Logs
- Syslog & CEF (Common Event Format) Integration
- Custom Data Collection (APIs & Log Analytics Agent)
- Best Practices for Data Retention & Cost Optimization
- Hands-on Practice: Configuring & Managing Data Connectors

Module 4: Kusto Query Language (KQL) for Sentinel

- Introduction to KQL & Log Analytics
- Writing Basic KQL Queries
- Advanced KQL: Joins, Aggregations & Time-Series Analysis
- Creating Custom Dashboards with KQL
- Hands-on Practice: Writing KQL Queries for Threat Investigation

SIEM XPERT
Learn. Secure. Succeed.

Module 5: Creating & Managing Analytics Rules

- Introduction to Detection Rules in Sentinel
- Scheduled vs. Near Real-Time Rules
- Custom Rule Creation & Alert Tuning
- Hands-on Practice: Creating Analytics Rules for Threat Detection

Module 6: Incident Management & Investigation

- How Sentinel Detects & Correlates Security Incidents
- Investigating Alerts & Incidents in Sentinel
- Managing False Positives & Incident Prioritization
- Threat Intelligence Integration with Sentinel
- Hands-on Practice: Investigating Security Incidents in Sentinel

Module 7: Automation & SOAR with Sentinel Playbooks (Advanced Level)

- Introduction to Sentinel Automation (SOAR)
- Using Logic Apps for Automated Incident Response
- Creating & Managing Playbooks in Microsoft Sentinel

- Automating Incident Response with Power Automate & Azure Functions
- Hands-on Practice: Developing & Deploying a Sentinel Playbook

Module 8: Threat Hunting in Sentinel

- Understanding Threat Hunting in a SIEM Environment
- Using KQL for Proactive Threat Hunting
- Hunting for Anomalous Behaviors & Insider Threats
- Hands-on Practice: Conducting a Threat Hunt in Sentinel

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 50000 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.

SIEM XPERT
Learn. Secure. Succeed.

SULABH MISHRA

CEO, Cyber Security Trainer & Solution Architect

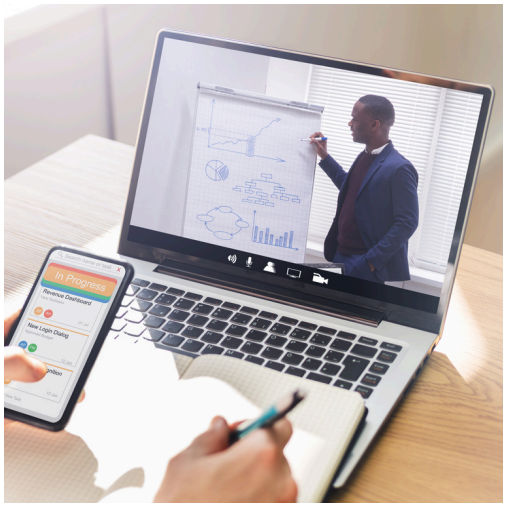
Sulabh Mishra has around 12+ years of experience in Cyber Security. He worked as Security tool administrator, Technical Consultant, Solutions Architect in the companies like Altisource, Accenture, Ericsson etc. Sulabh is Certified expert for Arcsight, Splunk, McAfee, Qradar and other SIEM tools as well 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 Admin & Enterprise Security
- CrowdStrike EDR
- Cortex XSOAR
- Microsoft Azure Sentinel
- IBM Qradar
- Certified Ethical Hacking (CEH)
- CISSP, CISA and many more

splunk> ArcSight Azure Sentinel IBM QRadar

C|EH Certified Ethical Hacker

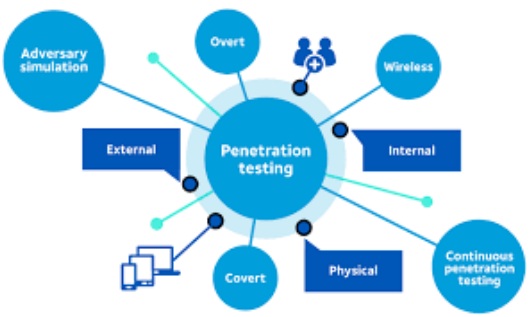
CISSP Certified Information Systems Security Professional

CISA Certified Information Systems Auditor. An ISACA Certification

SIEM XPERT
Learn. Secure. Succeed.

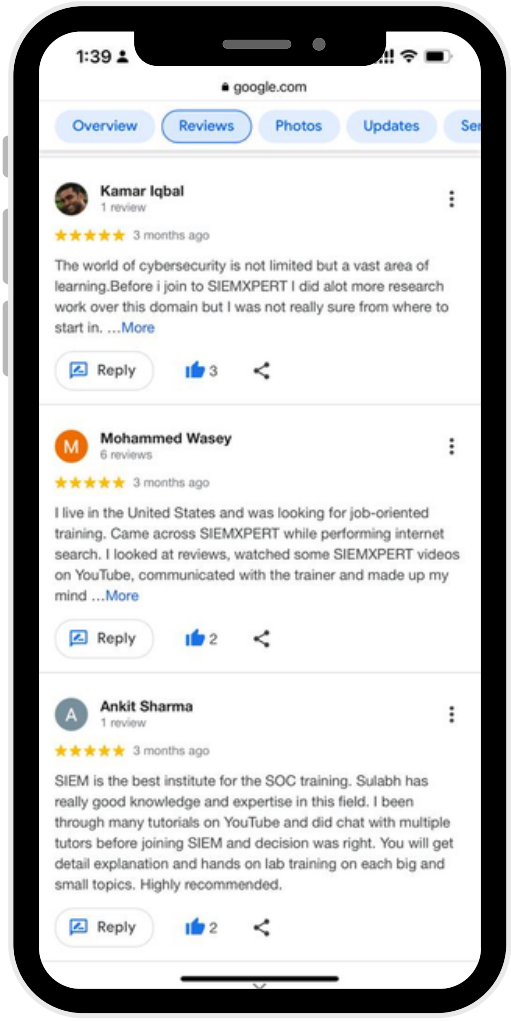
CYBER SECURITY SERVICES

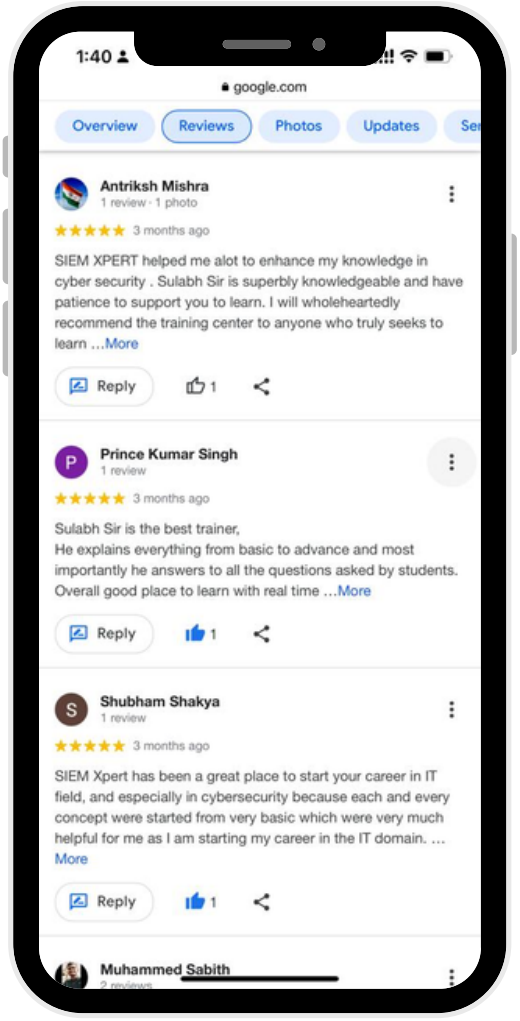
- Managed SOC Services
- Penetration services
- Security compliance and governance services
- and many more



WHAT OUR **TRAINEES** ARE SAYING

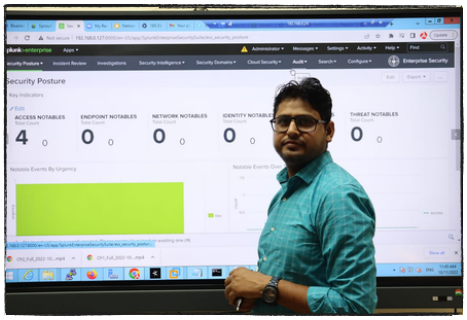
4.8 ★★★★★ **2031 Google reviews**





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