

Microsoft Security Operations Analyst (SC-200)

Microsoft Sentinel + Defender XDR

Complete Certification Preparation & Hands-On SOC Training



Course Content

SIEM XPERT

The Hub of Cyber Security Trainings

Committed to QUALITY, Committed to YOU.



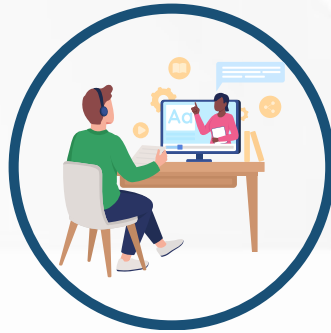
SIEM XPERT
Learn. Secure. Succeed.

OUR STATISTICS



50,000+

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?

Traditional learning often stops at theory, but cybersecurity demands more. At SIEM XPERT, we bridge the learning gap by integrating practical labs, real incident workflows, and industry-relevant skills. Our goal is simple, to ensure learners are not just educated, but truly prepared.

Freshers aiming to build their future career path in cyber security.

Individuals with career gaps who want to secure high-paying roles in leading MNCs.

Professionals from other fields who want to switch to Cyber Security.

This training helps you reshape your career and build the practical skills needed to perform with confidence at an industry-ready, professional level.

Cybersecurity professionals who are looking to enhance their expertise in SIEM and SOC operations.



MODULE 1 – Azure & Microsoft Security Fundamentals

1.1 Cloud Fundamentals

- Cloud computing fundamentals
- IaaS, PaaS and SaaS
- Public, private and hybrid cloud
- Shared responsibility model
- Cloud security challenges
- Cloud attack surface
- Zero Trust fundamentals

1.2 Azure Fundamentals

- Microsoft Azure overview
- Azure subscriptions
- Resource Groups
- Azure resources
- Azure Resource Manager
- Azure Portal
- Azure VMs
- Azure Storage
- Azure networking fundamentals
- NSG fundamentals
- Azure Activity Logs
- Diagnostic Settings

Total Duration: 40 hours .



1.3 Microsoft Identity Fundamentals

- Microsoft Entra ID
- Users and groups
- Authentication
- MFA
- Conditional Access – overview
- RBAC
- Entra sign-in logs
- Entra ID Protection – overview

Hands-on

- Create Resource Group
- Deploy/view Azure VM
- Configure basic NSG
- Create Log Analytics Workspace
- Review Azure Activity Logs
- Review Entra sign-in logs
- Understand RBAC

MODULE 2 – Microsoft Defender XDR & Security Operations

2.1 Defender XDR Architecture

- What is Microsoft Defender XDR?
- XDR vs EDR vs SIEM vs SOAR
- Microsoft Defender portal
- Microsoft Security ecosystem
- Microsoft Security Graph
- Security signals and correlation

2.2 Defender XDR Components

- Defender for Endpoint
- Defender for Office 365
- Defender for Identity
- Defender for Cloud Apps
- Defender Vulnerability Management
- Defender for Cloud
- Entra ID Protection
- Microsoft Purview security signals

2.3 Defender XDR Incidents

- Alerts
- Incidents
- Evidence
- Entities
- Users
- Devices



- IP addresses
- Files
- URLs
- Incident correlation
- Attack story
- Incident severity

2.4 XDR Operations

- Incident investigation
- Alert tuning
- Alert suppression
- Alert correlation
- Email notifications
- Threat analytics
- Action Center
- Automated Investigation and Response
- Automatic Attack Disruption
- Secure Score

Hands-on

Lab 1: Navigate Defender portal

Lab 2: Investigate a Defender XDR incident

Lab 3: Investigate entities/evidence

Lab 4: Review automated investigation

Lab 5: Review Action Center

MODULE 3 – Microsoft Defender for Endpoint

3.1 MDE Architecture

- Defender for Endpoint
- EDR
- Endpoint telemetry
- Sensors
- Microsoft Defender Antivirus
- Cloud-delivered protection
- Endpoint detection vs prevention

3.2 Device Onboarding

Overview of:

- Intune
- Group Policy
- Configuration Manager
- Local script
- Defender for Cloud
- Server onboarding

3.3 Endpoint Security Controls

- Attack Surface Reduction
- ASR rules
- Network Protection
- Web Protection
- Exploit Protection
- Tamper Protection



- Controlled Folder Access
- Device Control
- Antivirus policies

3.4 Endpoint Investigation

- Device inventory
- Device timeline
- Alerts
- Incidents
- Evidence
- Process tree
- File activity
- Network activity
- Registry activity
- Logon activity
- User activity

3.5 Endpoint Response

- Isolate device
- Collect investigation package
- Live Response
- Run commands
- Quarantine file
- Stop process
- Restrict application execution
- Investigate compromised device



3.6 Advanced Hunting

Core tables:

- DeviceProcessEvents
- DeviceNetworkEvents
- DeviceFileEvents
- DeviceLogonEvents
- DeviceRegistryEvents
- DeviceEvents

Hands-on Labs

Lab 1: Device onboarding

Lab 2: Investigate malware

Lab 3: Investigate PowerShell attack

Lab 4: Analyze process tree

Lab 5: Investigate network activity

Lab 6: Device isolation

Lab 7: Live Response

Lab 8: Advanced Hunting query

MODULE 4 – Defender for Office 365 + Defender for Identity

4.1 Microsoft Defender for Office 365

Topics

- Defender for Office 365 architecture
- Exchange Online Protection vs Defender for Office 365
- Anti-phishing
- Anti-spam
- Malware
- Safe Links
- Safe Attachments
- Impersonation protection
- Quarantine
- User submissions
- Threat Explorer
- Campaign views
- Email investigation

Investigation scenario

Phishing Email



Malicious URL



User clicks



Credential Theft



Entra Risk



Endpoint Compromise



XDR Incident

4.2 Microsoft Defender for Identity

Topics

- MDI architecture
- Sensors
- Domain Controller monitoring
- Identity reconnaissance
- LDAP reconnaissance
- Suspicious authentication
- Pass-the-Hash
- Pass-the-Ticket
- DCSync
- Lateral movement
- Privileged account compromise
- Identity investigation

Hands-on

- Investigate phishing alert
- Investigate suspicious identity activity
- Correlate user → endpoint → identity



MODULE 5 – Defender for Cloud Apps + Entra ID Protection + Purview

5.1 Defender for Cloud Apps

- CASB fundamentals
- Cloud Discovery
- Shadow IT
- Risky applications
- OAuth applications
- Application governance
- Conditional Access App Control
- Cloud application investigation

5.2 Entra ID Protection

- Identity risk
- Risky users
- Risky sign-ins
- Risk detection
- Investigation
- Remediation

5.3 Microsoft Purview

Only security-operation relevant areas:

- Audit
- Microsoft 365 activity
- DLP alerts
- Insider Risk awareness
- Investigation of security/compliance signals

Hands-on

- Investigate risky sign-in
- Investigate risky application
- Review M365 audit activity
- Investigate DLP alert

MODULE 6 – Microsoft Defender for Cloud

6.1 Defender for Cloud

- Defender for Cloud architecture
- Cloud Security Posture Management
- Secure Score
- Security recommendations
- Security controls
- Regulatory compliance

6.2 Defender Plans

Overview of:

- Defender for Servers
- Defender for Storage
- Defender for SQL
- Defender for Key Vault
- Defender for Resource Manager
- Defender for Containers
- Defender for App Service



6.3 Cloud Workload Security

- VM security
- Vulnerability assessment
- Security alerts
- Recommendations
- Cloud workload investigation

6.4 Integration

Azure Resource



Defender for Cloud



Security Recommendation / Alert



Defender XDR / Sentinel



SOC Investigation

Hands-on

- Enable/review Defender for Cloud
- Review Secure Score
- Investigate recommendations
- Investigate security alert
- Review VM security posture
- Send security information toward Sentinel



MODULE 7 – Microsoft Sentinel Architecture & Log Management

7.1 Sentinel Architecture

- What is Microsoft Sentinel?
- SIEM fundamentals
- SIEM vs XDR
- Sentinel architecture
- Log Analytics Workspace
- Tables
- Data connectors
- Content Hub
- Analytics rules
- Incidents
- Workbooks
- Automation

7.2 Data Sources

- Azure Activity Logs
- Entra ID
- Microsoft Defender XDR
- Microsoft 365
- Windows Security Events
- Syslog
- CEF
- Firewall logs
- DNS logs
- Network security logs



7.3 Log Ingestion

- Agent-based collection
- Azure Monitor Agent
- Data Collection Rules
- Syslog
- CEF
- API-based ingestion
- Data connector configuration

7.4 Log Management

- Tables
- Retention
- Data volume
- Cost optimization
- Basic troubleshooting
- Connector health

Hands-on

- Create Sentinel workspace
- Enable Sentinel
- Configure connectors
- Ingest logs
- Query tables
- Troubleshoot missing data

MODULE 8 – KQL & Sentinel Detection Engineering

8.1 KQL Fundamentals

where
project
extend
summarize
count
distinct
sort
top

8.2 Intermediate KQL

bin()
parse
extract
case
iff
join
lookup
union
let

8.3 Advanced KQL

arg_max()
make-series
time-series analysis



Security Queries

Students build queries for:

- Failed authentication
- Successful authentication
- Brute force
- Password spray
- PowerShell
- Suspicious process
- Privilege escalation
- Account creation
- Suspicious Azure activity
- Malware
- Network connections
- Impossible travel

8.4 Sentinel Detection Engineering

- Scheduled analytics rules
- Near Real-Time rules
- Threat Intelligence rules
- ML-based detection – awareness
- Custom detections
- Entity mapping
- Alert enrichment
- Severity
- MITRE ATT&CK mapping
- Detection tuning
- False positive reduction

Hands-on

Students create multiple analytics rules and investigate generated incidents.



MODULE 9 – Incident Response, Investigation & SOAR

9.1 Sentinel Incident Management

- Alert vs Incident
- Incident severity
- Incident status
- Incident ownership
- Incident assignment
- Entities
- Evidence
- Investigation graph
- Incident enrichment
- Comments
- False positives
- Incident closure

9.2 Defender XDR Incident Investigation

- XDR alerts
- Incident correlation
- Attack story
- Evidence
- Entities
- Device
- User
- IP
- File
- URL



9.3 Response

- Device isolation
- User containment
- File remediation
- Account remediation
- Threat blocking
- IOC blocking

9.4 SOAR

- Automation rules
- Logic Apps
- Playbooks
- Incident triggers
- Alert triggers
- Threat intelligence enrichment
- Email notifications
- Teams notification
- Ticket creation
- Automated containment

Hands-on

Lab 1: Investigate Sentinel incident

Lab 2: Investigate Defender incident

Lab 3: Enrich IOC

Lab 4: Build Logic App

Lab 5: Create Sentinel automation rule

Lab 6: Automated response workflow



MODULE 9 – Incident Response, Investigation & SOAR

10.1 Threat Hunting Fundamentals

- What is threat hunting?
- Reactive vs proactive investigation
- IOC vs IOA
- Threat hypotheses
- Threat hunting lifecycle
- Threat intelligence
- MITRE ATT&CK

10.2 Defender Advanced Hunting

- Core tables
- DeviceProcessEvents
- DeviceNetworkEvents
- DeviceFileEvents
- DeviceLogonEvents
- DeviceRegistryEvents
- DeviceEvents
- IdentityLogonEvents
- EmailEvents
- EmailUrlInfo
- EmailAttachmentInfo
- CloudAppEvents



Hunting scenarios

Hunt 1 – PowerShell

Find suspicious PowerShell execution.

Hunt 2 – Credential Access

Identify suspicious credential-related behavior.

Hunt 3 – Lateral Movement

Identify unusual authentication patterns.

Hunt 4 – Command & Control

Identify suspicious outbound connections.

Hunt 5 – Persistence

Look for suspicious registry/process activity.

Hunt 6 – Data Exfiltration

Identify abnormal network/data activity.

10.3 Sentinel Threat Hunting

- Hunting queries
- Hunting rules
- Bookmarks
- Investigation
- Threat intelligence
- Entity investigation
- Query-based hunting

10.4 MITRE ATT&CK Mapping

ABOUT SIEM XPERT

Company Profile

SIEM XPERT is a global leader in cybersecurity training and services, having headquartered in Bangalore (Karnataka) and empowering learners since 2016.

We've transformed the careers of over 50,000 professionals worldwide, helping them step into the high-demand, high-paying world of cybersecurity and create life-changing opportunities.

With strong partnerships across top organizations, we actively connect our trained students with potential employers, giving them a head start in the industry.

We offer a world-class, real-time lab environment equipped with industry-standard cybersecurity tools, allowing students to gain hands-on experience. This practical training ensures they are job-ready from day one, delivering high-quality performance that makes them highly valued by employers, who require minimal onboarding.

We also offer corporate training programs designed to upskill employees, strengthen organizational security, and build teams capable of tackling real-world cybersecurity challenges.



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 brings over 12 years of hands-on experience in Cyber Security, having played key roles as a Security Tool Administrator, Technical Consultant, and Solutions Architect at global companies like Altisource, Accenture, and Ericsson etc. Certified across multiple cutting-edge cybersecurity technologies, he knows exactly what it takes to thrive in this fast-paced industry. Passionate about bridging the skills gap, Sulabh empowers professionals to confidently take on the growing demand in cybersecurity and excel from day one.





SIEM XPERT
Learn. Secure. Succeed.

OUR STUDENTS WORK IN COMPANIES LIKE

The Best Companies



INSPIRE



OUR SPECIALIZED TRAINING PROGRAMS

Job - Oriented Trainings

- Next-Generation SOC Analyst Training with AI
- Splunk Administration Training
- Splunk Enterprise Security Training
- Splunk Administration + Splunk Enterprise Security Training
- CrowdStrike EDR Training
- IBM QRadar Training with Certification
- Bug Bounty Hunting Courses and Training Programs
- Identity and Access Management (IAM) Training
- AWS Cloud Practitioner Certification Training
- CyberArk Training Program Course and many more..



OUR SPECIALIZED TRAINING PROGRAMS

Certification based courses

- Certified Information Security Manager (CISM) Certification Training
- Certified SOC Analyst (CSA) Certification Training
- Certified Ethical Hacking (CEH v13 AI) Certification
- CISSP Online Training With Certification
- CCNA: Cisco Certified Network Associate (CCNA 200-301) Certification Training Course
- Certified Cloud Security Professional (CCSP) Training & Certification
- Certified Information Systems Auditor (CISA) Training & Certification
- CompTIA Security+ (Plus) Certification Training
- ISO 27001:2022 Lead Auditor Training and Certification





CYBER SECURITY SERVICES

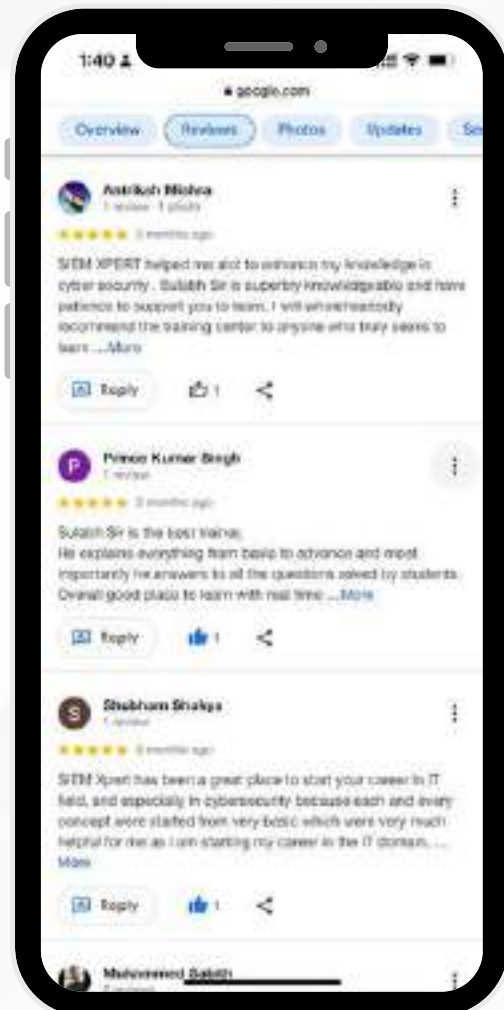
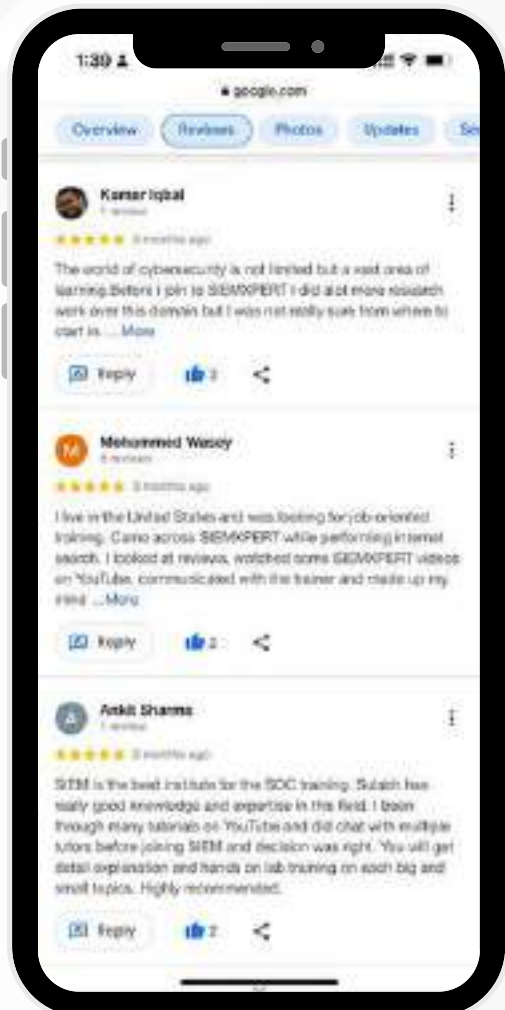
- Managed SOC Services
- Penetration services
- Security compliance and governance services
- and many more



WHAT OUR **TRAINEES** ARE SAYING

4.8 ★ ★ ★ ★ ★

2000+ Google reviews



SESSION-TIME AT SIEM XPERT



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)

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 Ramkrishan Dubey

Deloitte
(17 LPA)



Sattrix
(12.5 LPA)



SIEM XPERT

Learn. Secure. Succeed.

No.1 Cyber security Training & Consulting services in
India, US, UK & 30+ countries with 10+ years old
Excellence.

For real-time Cyber Security trainings, contact us-



+91 9108318017 or +91 8660550523



trainings@siemxpert.com



<https://www.siemxpert.com>



@siemxpert