SIEM XPERT
Learn. Secure. Succeed.

COMPTIA SECURITY+ SY0-701 TRAINING

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.

Beginner-level to Mid-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 certification can enroll in this course.

People who are working inother industry and want to get into cybersecurity or switch jobs to get a higher payout.

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

Domain 1: Threats, Attacks, and Vulnerabilities

1.1 Compare and contrast different types of social engineering techniques.

- Phishing
- Smishing
- Vishing
- Spam
- Spam over instant messaging (SPIM)
- Spear phishing
- Dumpster diving
- Shoulder surfing
- Pharming
- Tailgating
- Eliciting information
- Whaling
- Prepending
- Identity fraud
- Invoice scams
- Credential harvesting
- Reconnaissance
- Hoax
- Impersonation

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Watering hole attack
- Typosquatting
- Pretexting
- Influence campaigns
  - Hybrid warfare
  - Social media
- Principles (reasons for effectiveness)
  - Authority
  - Intimidation
  - Consensus
  - Scarcity
  - Familiarity
  - Trust
  - Urgency

1.2 Given a scenario, analyze potential indicators to determine the type of attack.

- Malware
  - Ransomware
  - Trojans
  - Worms
  - Potentially unwanted programs (PUPs)
  - Fileless virus
  - Command and control
  - Bots

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Cryptomalware
- Logic bombs
- Spyware
- Keyloggers
- Remote access Trojan (RAT)
- Rootkit
- Backdoor

- **Password attacks**
  - Spraying
  - Dictionary
  - Brute force
  - Offline
  - Online
  - Rainbow table
  - Plaintext/unencrypted
- **Physical attacks**
  - Malicious Universal Serial Bus (USB) cable
  - Malicious flash drive
  - Card cloning
  - Skimming
- Adversarial artificial intelligence (AI)
  - Tainted training data for machine learning (ML)
  - Security of machine learning algorithms
- Supply-chain attacks
- Cloud-based vs. on-premises attacks

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Cryptographic attacks
  - Birthday
  - Collision
  - Downgrade

1.3 Given a scenario, analyze potential indicators associated with application attacks.

- Privilege escalation
- Cross-site scripting
- Injections
  - Structured query language (SQL)
  - Dynamic-link library (DLL)
  - Lightweight Directory
- Access Protocol (LDAP)
  - Extensible Markup Language (XML)
- Pointer/object dereference
- Directory traversal
- Buffer overflows
- Race conditions
  - Time of check/time of use
- Error handling
- Improper input handling
- Replay attack
  - Session replays
- Integer overflow

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Request forgeries
  - Server-side
  - Cross-site
- Application programming interface (API) attacks
- Resource exhaustion
- Memory leak
- Secure Sockets Layer (SSL) stripping
- Driver manipulation
  - Shimming
  - Refactoring
- Pass the hash

1.4 Given a scenario, analyze potential indicators associated with network attacks.

- Wireless
  - Evil twin
  - Rogue access point
  - Bluesnarfing
  - Bluejacking
  - Disassociation
  - Jamming
  - Radio frequency identification (RFID)
  - Near-field communication (NFC)
  - Initialization vector (IV)

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- On-path attack (previously known as man-in-the-middle attack/ man-in-the-browser attack)
- Layer 2 attacks
  - Address Resolution Protocol (ARP) poisoning
  - Media access control (MAC) flooding
  - MAC cloning
- Domain name system (DNS)
  - Domain hijacking
  - DNS poisoning
  - Uniform Resource Locator (URL) redirection
  - Domain reputation
- Distributed denial-of-service (DDoS)
  - Network
  - Application
  - Operational technology (OT)
- Malicious code or script execution
  - PowerShell
  - Python
  - Bash
  - Macros
  - Visual Basic for Applications (VBA)

1.5 Explain different threat actors, vectors, and intelligence sources.

- Actors and threats
  - Advanced persistent threat (APT)

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

  - Insider threats
  - State actors
  - Hacktivists
  - Script kiddies
  - Criminal syndicates
  - Hackers
  - Authorized
  - Unauthorized
  - Semi-authorized
  - Shadow IT
  - Competitors
- Attributes of actors
  - Internal/external
  - Level of sophistication/capability
  - Resources/funding
  - Intent/motivation
- Vectors
  - Direct access
  - Wireless
  - Email
  - Supply chain
  - Social media
  - Removable media
  - Cloud
- Threat intelligence sources
  - Open-source intelligence (OSINT)

SECURITY+ CERTIFICATION (SYLLABUS)

- Closed/proprietary
- Vulnerability databases
- Public/private information- sharing centers
- Dark web
- Indicators of compromise
- Automated Indicator Sharing (AIS)
- Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Intelligence Information (TAXII)
- Predictive analysis
- Threat maps
- File/code repositories

• Research sources
- Vendor websites
- Vulnerability feeds
- Conferences
- Academic journals
- Request for comments (RFC)
- Local industry groups
- Social media
- Threat feeds
- Adversary tactics, techniques, and procedures (TTP)

1.6 Explain the security concerns associated with various types of vulnerabilities

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Cloud-based vs. on-premises vulnerabilities
- Zero-day
- Weak configurations
  - Open permissions
  - Unsecure root accounts
  - Errors
  - Weak encryption
  - Unsecure protocols
  - Default settings
  - Open ports and services
- Third-party risks
  - Vendor management
  - System integration
  - Lack of vendor support
  - Supply chain
  - Outsourced code development
  - Data storage
- Improper or weak patch management
  - Firmware
  - Operating system (OS)
  - Applications
- Legacy platforms
- Impacts
  - Data loss
  - Data breaches
  - Data exfiltration

SECURITY+ CERTIFICATION (SYLLABUS)

- Identity theft
- Financial
- Reputation
- Availability loss

1.7 Summarize the techniques used in security assessments

- Threat hunting
  - Intelligence fusion
  - Threat feeds
  - Advisories and bulletins
  - Maneuver
- Vulnerability scans
  - False positives
  - False negatives
  - Log reviews
  - Credentialed vs. non-credentialed
  - Intrusive vs. non-intrusive
  - Application
  - Web application
  - Network
  - Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS)
  - Configuration review
- Syslog/Security information and event management (SIEM)
  - Review reports

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

  - Packet capture
  - Data inputs
  - User behavior analysis
  - Sentiment analysis
  - Security monitoring
  - Log aggregation
  - Log collectors
- Security orchestration, automation, and response (SOAR)

1.8 Explain the techniques used in penetration testing

- Penetration testing
  - Known environment
  - Unknown environment
  - Partially known environment
  - Rules of engagement
  - Lateral movement
  - Privilege escalation
  - Persistence
  - Cleanup
  - Bug bounty
  - Pivoting
- Passive and active reconnaissance
  - Drones
  - War flying
  - War driving
  - Footprinting

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

  - OSINT
- Exercise types
  - Red-team
  - Blue-team
  - White-team
  - Purple-team

Domain 2: Architecture and Design

2.1 Explain the importance of security concepts in an enterprise environment.

- Configuration management
  - Diagrams
  - Baseline configuration
  - Standard naming conventions
  - Internet protocol (IP) schema
- Data sovereignty
- Data protection
  - Data loss prevention (DLP)
  - Masking
  - Encryption
  - At rest
  - In transit/motion
  - In processing
  - Tokenization

SECURITY+ CERTIFICATION (SYLLABUS)

  - Rights management
- Geographical considerations
- Response and recovery controls
- Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection
- Hashing
- API considerations
- Site resiliency
  - Hot site
  - Cold site
  - Warm site
- Deception and disruption
  - Honeypots
  - Honeyfiles
  - Honeynets
  - Fake telemetry
  - DNS sinkhole

2.2 Summarize virtualization and cloud computing concepts.

- Cloud models
  - Infrastructure as a service (IaaS)
  - Platform as a service (PaaS)
  - Software as a service (SaaS)
  - Anything as a service (XaaS)
  - Public

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

  - Community
  - Private
  - Hybrid
- Cloud service providers
- Managed service provider (MSP)/ managed security service provider (MSSP)
- On-premises vs. off-premises • Fog computing • Edge computing
- Thin client
- Containers
- Microservices/API
- Infrastructure as code
  - Software-defined networking (SDN)
  - Software-defined visibility (SDV)
- Serverless architecture
- Services integration
- Resource policies
- Transit gateway
- Virtualization
  - Virtual machine (VM) sprawl avoidance
  - VM escape protection

2.3 Summarize secure application development, deployment, and automation concepts

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Environment
  - Development
  - Test
  - Staging
  - Production
  - Quality assurance (QA)
- Provisioning and deprovisioning
- Integrity measurement
- Secure coding techniques
  - Normalization
  - Stored procedures
  - Obfuscation/camouflage
  - Code reuse/dead code
  - Server-side vs. client-side execution and validation
  - Memory management
  - Use of third-party libraries and software development kits (SDKs)
  - Data exposure
- Open Web Application Security Project (OWASP)
- Software diversity
  - Compiler
  - Binary
- Automation/scripting
  - Automated courses of action
  - Continuous monitoring
  - Continuous validation

SECURITY+ CERTIFICATION (SYLLABUS)

  - Continuous integration
  - Continuous delivery
  - Continuous deployment
- Elasticity
- Scalability
- Version control

2.4 Summarize authentication and authorization design concepts.

- Authentication methods
  - Directory services
  - Federation
  - Attestation
  - Technologies
  - Time-based one- time password (TOTP)
  - HMAC-based one-time password (HOTP)
  - Short message service (SMS)
  - Token key
  - Static codes
  - Authentication applications
  - Push notifications
  - Phone call
  - Smart card authentication
- Biometrics
  - Fingerprint
  - Retina

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

  - Iris
  - Facial
  - Voice
  - Vein
  - Gait analysis
  - Efficacy rates
  - False acceptance
  - False rejection
  - Crossover error rate
- Multifactor authentication (MFA) factors and attributes
  - Factors
    - Something you know
    - Something you have
    - Something you are
  - Attributes
    - Somewhere you are
    - Something you can do
    - Something you exhibit
    - Someone you know
- Authentication, authorization, and accounting (AAA)
- Cloud vs. on-premises requirements

2.5 Given a scenario, implement cybersecurity resilience

- Redundancy
  - Geographic dispersal
  - Disk - Redundant array of inexpensive disks (RAID) levels

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

  - Multipath
  - Network
  - Load balancers
  - Network interface card (NIC) teaming
  - Power
  - Uninterruptible power supply (UPS)
  - Generator
  - Dual supply
  - Managed power distribution units (PDUs)
- Replication
  - Storage area network
  - VM
- On-premises vs. cloud
- Backup types
  - Full
  - Incremental
  - Snapshot - Differential
  - Tape - Disk
  - Copy
  - Network-attached storage (NAS)
  - Storage area network
  - Cloud - Image
  - Online vs. offline
  - Offsite storage
  - Distance considerations

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Non-persistence
  - Revert to known state
  - Last known-good configuration
  - Live boot media
- High availability
  - Scalability
- Restoration order
- Diversity
  - Technologies
  - Vendors
  - Crypto
  - Controls

2.6 Explain the security implications of embedded and specialized systems

- Embedded systems
  - Raspberry Pi
  - Field-programmable gate array (FPGA)
  - Arduino • Supervisory control and data acquisition (SCADA)/industrial control system (ICS)
  - Facilities
  - Industrial
  - Manufacturing
  - Energy
  - Logistics

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Internet of Things (IoT)
  - Sensors
  - Smart devices
  - Wearables
  - Facility automation
  - Weak defaults
- Specialized
  - Medical systems
  - Vehicles
  - Aircraft
  - Smart meters
- Voice over IP (VoIP)
- Heating, ventilation, air conditioning (HVAC)
- Drones
- Multifunction printer (MFP)
- Real-time operating system (RTOS)
- Surveillance systems
- System on chip (SoC)
- Communication considerations
  - 5G - Narrow-band
  - Baseband radio
  - Subscriber identity module (SIM) cards
  - Zigbee
- Constraints
  - Power

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Locks
- Biometrics
- Electronic
- Physical
- Cable locks
- USB data blocker
- Lighting
- Fencing
- Fire suppression
- Sensors
  - Motion detection
  - Noise detection
  - Proximity reader
  - Moisture detection
  - Cards - Temperature
- Drones
- Visitor logs
- Faraday cages
- Air gap
- Screened subnet (previously known as demilitarized zone)
- Protected cable distribution
- Secure areas
  - Air gap
  - Vault

SECURITY+ CERTIFICATION (SYLLABUS)

  - Safe
  - Hot aisle
  - Cold aisle
- Secure data destruction
  - Burning
  - Shredding
  - Pulping
  - Pulverizing
  - Degaussing
  - Third-party solutions

2.8 Summarize the basics of cryptographic concepts.

- Digital signatures
- Key length
- Key stretching
- Salting
- Hashing
- Key exchange
- Elliptic-curve cryptography
- Perfect forward secrecy
- Quantum
  - Communications
  - Computing
- Post-quantum
- Ephemeral

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Modes of operation
  - Authenticated
  - Unauthenticated
  - Counter
- Blockchain
  - Public ledgers
- Cipher suites
  - Stream
  - Block
- Symmetric vs. asymmetric
- Lightweight cryptography
- Steganography
  - Audio
  - Video
  - Image
- Homomorphic encryption
- Common use cases
  - Low power devices
  - Low latency
  - High resiliency
  - Supporting confidentiality
  - Supporting integrity
  - Supporting obfuscation
  - Supporting authentication
  - Supporting non-repudiation

SECURITY+ CERTIFICATION (SYLLABUS)

- Limitations
  - Speed
  - Size
  - Weak keys
  - Time
  - Longevity
  - Predictability
  - Reuse
  - Entropy
  - Computational overheads
  - Resource vs. security constraints

Domain 3: Implementation

3.1 Given a scenario, implement secure protocols.

- Protocols
  - Domain Name System Security Extensions (DNSSEC)
  - SSH - Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Secure Real-time Transport Protocol (SRTP)
  - Lightweight Directory Access Protocol Over SSL (LDAPS)
  - File Transfer Protocol, Secure (FTPS)
  - SSH File Transfer Protocol (SFTP)

SECURITY+ CERTIFICATION (SYLLABUS)

  - Simple Network Management Protocol, version 3 (SNMPv3)
  - Hypertext transfer protocol over SSL/TLS (HTTPS)
  - IPSec - Authentication header (AH)/ Encapsulating Security Payloads (ESP)
  - Tunnel/transport
  - Post Office Protocol (POP)/ Internet Message Access Protocol (IMAP)
- Use cases
  - Voice and video
  - Time synchronization
  - Email and web
  - File transfer
  - Directory services
  - Remote access
  - Domain name resolution
  - Routing and switching
  - Network address allocation
  - Subscription services

3.2 Given a scenario, implement host or application security solutions.

- Endpoint protection
  - Antivirus
  - Anti-malware
  - Endpoint detection and response (EDR)

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

  - DLP
  - Next-generation firewall (NGFW)
  - Host-based intrusion prevention system (HIPS)
  - Host-based intrusion detection system (HIDS)
  - Host-based firewall
- Boot integrity
  - Boot security/Unified Extensible Firmware Interface (UEFI)
  - Measured boot
  - Boot attestation
- Database
  - Tokenization
  - Salting
  - Hashing
- Application security
  - Input validations
  - Secure cookies
  - Hypertext Transfer Protocol (HTTP) headers
  - Code signing
  - Allow list
  - Block list/deny list
  - Secure coding practices
  - Static code analysis
  - Manual code review
  - Dynamic code analysis
  - Fuzzing

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Hardening
  - Open ports and services
  - Registry
  - Disk encryption
  - OS
  - Patch management
  - Third-party updates
  - Auto-update
- Self-encrypting drive (SED)/ full-disk encryption (FDE)
  - Opal
- Hardware root of trust
- Trusted Platform Module (TPM)
- Sandboxing

3.3 Given a scenario, implement secure network designs.

- Load balancing
  - Active/active
  - Active/passive
  - Scheduling
  - Virtual IP
  - Persistence
- Network segmentation
  - Virtual local area network (VLAN)
  - Screened subnet (previously known as demilitarized zone)

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

  - East-west traffic
  - Extranet
  - Intranet
  - Zero Trust
- Virtual private network (VPN)
  - Always-on
  - Split tunnel vs. full tunnel
  - Remote access vs. site-to-site
  - IPSec
  - SSL/TLS
  - HTML5
  - Layer 2 tunneling protocol (L2TP)
- DNS
- Network access control (NAC)
  - Agent and agentless
- Out-of-band management
- Port security
  - Broadcast storm prevention
  - Bridge Protocol Data Unit (BPDU) guard
  - Loop prevention
  - Dynamic Host Configuration Protocol (DHCP) snooping
  - Media access control (MAC) filtering
- Network appliances
  - Jump servers
  - Proxy servers
  - Forward

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

  - Reverse
  - Network-based intrusion detection system (NIDS) /network-based intrusion prevention system (NIPS)
  - Signature-based
  - Heuristic/behavior
  - Anomaly
  - Inline vs. passive
  - HSM
  - Sensors
  - Collectors
  - Aggregators
  - Firewalls
  - Web application firewall (WAF)
  - NGFW
  - Stateful
  - Stateless
  - Unified threat management (UTM)
  - Network address translation (NAT) gateway
  - Content/URL filter
  - Open-source vs. proprietary
  - Hardware vs. software
  - Appliance vs. host-based vs. virtual
- Access control list (ACL)
- Route security
- Quality of service (QoS)

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Implications of IPv6
- Port spanning/port mirroring
  - Port taps
- Monitoring services
- File integrity monitors

3.4 Given a scenario, install and configure wireless security settings.

- Cryptographic protocols
  - WiFi Protected Access 2 (WPA2)
  - WiFi Protected Access 3 (WPA3)
  - Counter-mode/CBC-MAC Protocol (CCMP)
  - Simultaneous Authentication of Equals (SAE)
- Authentication protocols
  - Extensible Authentication Protocol (EAP)
  - Protected Extensible Authentication Protocol (PEAP)
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS
  - IEEE 802.1X
  - Remote Authentication Dial-in User Service (RADIUS) Federation
- Methods
  - Pre-shared key (PSK) vs. Enterprise vs. Open
  - WiFi Protected Setup (WPS)

SECURITY+ CERTIFICATION (SYLLABUS)

  - Captive portals
- Installation considerations
  - Site surveys
  - Heat maps
  - WiFi analyzers
  - Channel overlaps
  - Wireless access point (WAP) placement
  - Controller and access point security

3.5 Given a scenario, implement secure mobile solutions

- Connection methods and receivers
  - Cellular
  - WiFi
  - Bluetooth
  - NFC
  - Infrared
  - USB
  - Point-to-point
  - Point-to-multipoint
  - Global Positioning System (GPS)
  - RFID
- Mobile device management (MDM)
  - Application management
  - Content management
  - Remote wipe

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Geofencing
- Geolocation
- Screen locks
- Push notifications
- Passwords and PINs
- Biometrics
- Context-aware authentication
- Containerization
- Storage segmentation
- Full device encryption

- Mobile devices
  - MicroSD hardware security module (HSM)
  - MDM/Unified Endpoint Management (UEM)
  - Mobile application management (MAM)
  - SEAndroid
- Enforcement and monitoring of:
  - Third-party application stores
  - Rooting/jailbreaking
  - Sideloading
  - Custom firmware
  - Carrier unlocking
  - Firmware over-the-air (OTA) updates
  - Camera use
  - SMS/Multimedia Messaging Service (MMS)/Rich Communication Services (RCS)
  - External media

SECURITY+ CERTIFICATION (SYLLABUS)

  - USB On-The-Go (USB OTG)
  - Recording microphone
  - GPS tagging
  - WiFi direct/ad hoc
  - Tethering
  - Hotspot
  - Payment methods
- Deployment models
  - Bring your own device (BYOD)
  - Corporate-owned personally enabled (COPE)
  - Choose your own device (CYOD)
  - Corporate-owned
  - Virtual desktop infrastructure (VDI)

3.6 Given a scenario, apply cybersecurity solutions to the cloud.

- Cloud security controls
  - High availability across zones
  - Resource policies
  - Secrets management
  - Integration and auditing
  - Storage
  - Permissions
  - Encryption
  - Replication
  - High availability

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

  - Network
  - Virtual networks
  - Public and private subnets
  - Segmentation
  - API inspection and integration
  - Compute
  - Security groups
  - Dynamic resource allocation
  - Instance awareness
  - Virtual private cloud (VPC) endpoint
  - Container security
- Solutions
  - CASB
  - Application security
  - Next-generation secure web gateway (SWG)
  - Firewall considerations in a cloud environment
  - Cost
  - Need for segmentation
  - Open Systems Interconnection (OSI) layers
- Cloud native controls vs. third-party solutions

3.7 Given a scenario, implement identity and account management controls.

- Identity
  - Identity provider (IdP)
  - Attributes

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Certificates
- Tokens
- SSH keys
- Smart cards

- Account types
  - User account
  - Shared and generic accounts/credentials
  - Guest accounts
  - Service accounts
- Account policies
  - Password complexity
  - Password history
  - Password reuse
  - Network location
  - Geofencing
  - Geotagging
  - Geolocation
  - Time-based logins
  - Access policies
  - Account permissions
  - Account audits
  - Impossible travel time/risky login
  - Lockout
  - Disablement

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

3.8 Given a scenario, implement authentication and authorization solutions.

- Authentication management
  - Password keys
  - Password vaults
  - TPM
  - HSM
  - Knowledge-based authentication
- Authentication/authorization
  - EAP
  - Challenge-Handshake Authentication Protocol (CHAP)
  - Password Authentication Protocol (PAP)
  - 802.1X
  - RADIUS
  - Single sign-on (SSO)
  - Security Assertion Markup Language (SAML)
  - Terminal Access Controller Access Control System Plus (TACACS+)
  - OAuth
  - OpenID
  - Kerberos
- Access control schemes
  - Attribute-based access control (ABAC)
  - Role-based access control
  - Rule-based access control
  - MAC

SECURITY+ CERTIFICATION (SYLLABUS)

- Discretionary access control (DAC)
- Conditional access
- Privileged access management
- Filesystem permissions

3.9 Given a scenario, implement public key infrastructure.

- Public key infrastructure (PKI)
  - Key management
  - Certificate authority (CA)
  - Intermediate CA
  - Registration authority (RA)
  - Certificate revocation list (CRL)
  - Certificate attributes
  - Online Certificate Status Protocol (OCSP)
  - Certificate signing request (CSR)
  - CN
  - Subject alternative name
  - Expiration
- Types of certificates
  - Wildcard
  - Subject alternative name
  - Code signing
  - Self-signed
  - Machine/computer
  - Email
  - User

SECURITY+ CERTIFICATION (SYLLABUS)

  - Root
  - Domain validation
  - Extended validation
- Certificate formats
  - Distinguished encoding rules (DER)
  - Privacy enhanced mail (PEM)
  - Personal information exchange (PFX)
  - .cer
  - P12
  - P7B
- Concepts
  - Online vs. offline CA
  - Stapling
  - Pinning
  - Trust model
  - Key escrow
  - Certificate chaining

Domain 4: Operations and Incident Response

4.1 Given a scenario, use the appropriate tool to assess organizational security.

- Network reconnaissance and discovery
  - tracert/traceroute
  - nslookup/dig

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- ipconfig/ifconfig
- nmap
- ping/pathping
- hoping
- netstat
- netcat
- IP scanners
- arp
- route
- curl
- theHarvester
- sn1per
- scanless
- dnsenum
- Nessus
- Cuckoo

- File manipulation
  - head
  - tail
  - cat
  - grep
  - chmod
  - logger
- Shell and script environments
  - SSH
  - PowerShell

SECURITY+ CERTIFICATION (SYLLABUS)

  - Python
  - OpenSSL
- Packet capture and replay
  - Tcpreplay
  - Tcpdump
  - Wireshark
- Forensics
  - dd
  - Memdump
  - WinHex
  - FTK imager
  - Autopsy
- Exploitation frameworks
- Password crackers
- Data sanitization

4.2 Summarize the importance of policies, processes, and procedures for incident response.

- Incident response plans
- Incident response process
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons learned

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Exercises
  - Tabletop
  - Walkthroughs
  - Simulations
- Attack frameworks
  - MITRE ATT&CK
  - The Diamond Model of Intrusion Analysis
  - Cyber Kill Chain
- Stakeholder management
- Communication plan
- Disaster recovery plan
- Business continuity plan
- Continuity of operations planning (COOP)
- Incident response team
- Retention policies

4.3 Given an incident, utilize appropriate data sources to support an investigation.

- Vulnerability scan output
- SIEM dashboards
  - Sensor
  - Sensitivity
  - Trends
  - Alerts
  - Correlation

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Log files
  - Network
  - System
  - Application
  - Security
  - Web
  - DNS
  - Authentication
  - Dump files
  - VoIP and call managers
  - Session Initiation Protocol (SIP) traffic
- syslog/rsyslog/syslog-ng
- journalctl
- NXLog
- Bandwidth monitors
- Metadata
  - Email
  - Mobile
  - Web
  - File
- Netflow/sFlow
  - Netflow
  - sFlow
  - IPFIX
- Protocol analyzer output

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

4.4 Given an incident, apply mitigation techniques or controls to secure an environment.

- Reconfigure endpoint security solutions
  - Application approved list
  - Application blocklist/deny list
  - Quarantine
- Configuration changes
  - Firewall rules
  - MDM
  - DLP
  - Content filter/URL filter
  - Update or revoke certificates
- Isolation
- Containment
- Segmentation
- SOAR
  - Runbooks
  - Playbooks

4.5 Explain the key aspects of digital forensics.

- Documentation/evidence
  - Legal hold
  - Video
  - Admissibility
  - Chain of custody
  - Timelines of sequence of events

SECURITY+ CERTIFICATION (SYLLABUS)

- Time stamps
- Time offset
- Tags
- Reports
- Event logs
- Interviews

- Acquisition
  - Order of volatility
  - Disk
  - Random-access memory (RAM)
  - Swap/pagefile
  - OS
  - Device
  - Firmware
  - Snapshot
  - Cache
  - Network
  - Artifacts
- On-premises vs. cloud
  - Right-to-audit clauses
  - Regulatory/jurisdiction
  - Data breach notification laws
- Integrity
  - Hashing
  - Checksums
  - Provenance

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Preservation
- E-discovery
- Data recovery
- Non-repudiation
- Strategic intelligence/ counterintelligence

Domain 5: Governance, Risk, and Compliance

5.1 Compare and contrast various types of controls.

- Category
  - Managerial
  - Operational
  - Technical
- Control type
  - Preventive
  - Detective
  - Corrective
  - Deterrent
  - Compensating
  - Physical

5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Regulations, standards, and legislation
  - General Data Protection Regulation (GDPR)
  - National, territory, or state laws
  - Payment Card Industry Data Security Standard (PCI DSS)
- Key frameworks
  - Center for Internet Security (CIS)
  - National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)/Cybersecurity Framework (CSF)
  - International Organization for Standardization (ISO) 27001/27002/27701/31000
  - SSAE SOC 2 Type I/II
  - Cloud security alliance
  - Cloud control matrix
  - Reference architecture
- Benchmarks /secure configuration guides
  - Platform/vendor-specific guides
  - Web server
  - OS
  - Application server
  - Network infrastructure devices

5.3 Explain the importance of policies to organizational security.

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Personnel
  - Acceptable use policy
  - Job rotation
  - Mandatory vacation
  - Separation of duties
  - Least privilege
  - Clean desk space
  - Background checks
  - Non-disclosure agreement (NDA)
  - Social media analysis
  - Onboarding
  - Offboarding
  - User training
  - Gamification
  - Capture the flag
  - Phishing campaigns
  - Phishing simulations
  - Computer-based training (CBT)
  - Role-based training
- Diversity of training techniques
- Third-party risk management
  - Vendors
  - Supply chain
  - Business partners
  - Service level agreement (SLA)
  - Memorandum of understanding (MOU)

SECURITY+ CERTIFICATION (SYLLABUS)

  - Measurement systems analysis (MSA)
  - Business partnership agreement (BPA)
  - End of life (EOL)
  - End of service life (EOSL)
  - NDA
- Data
  - Classification
  - Governance
  - Retention
- Credential policies
  - Personnel
  - Third-party
  - Devices
  - Service accounts
  - Administrator/root accounts
- Organizational policies
  - Change management
  - Change control
  - Asset management

5.4 Summarize risk management processes and concepts.

- Risk types
  - External
  - Internal
  - Legacy systems
  - Multiparty

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

  - IP theft
  - Software compliance/licensing
- Risk management strategies
  - Acceptance
  - Avoidance
  - Transference
  - Cybersecurity insurance
  - Mitigation
- Risk analysis
  - Risk register
  - Risk matrix/heat map
  - Risk control assessment
  - Risk control self-assessment
  - Risk awareness
  - Inherent risk
  - Residual risk
  - Control risk
  - Risk appetite
  - Regulations that affect risk posture
  - Risk assessment types
  - Qualitative
  - Quantitative
  - Likelihood of occurrence
  - Impact
  - Asset value
  - Single-loss expectancy (SLE)

SECURITY+ CERTIFICATION (SYLLABUS)

  - Annualized loss expectancy (ALE)
  - Annualized rate of occurrence (ARO)
- Disasters
  - Environmental
  - Person-made
  - Internal vs. external
- Business impact analysis
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
  - Mean time to repair (MTTR)
  - Mean time between failures (MTBF)
  - Functional recovery plans
  - Single point of failure
  - Disaster recovery plan (DRP)
  - Mission essential functions
  - Identification of critical systems
  - Site risk assessment

5.5 Explain privacy and sensitive data concepts in relation to security.

- Organizational consequences of privacy and data breaches
  - Reputation damage
  - Identity theft
  - Fines
  - IP theft

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

- Notifications of breaches
  - Escalation
  - Public notifications and disclosures
- Data types
  - Classifications
  - Public
  - Private
  - Sensitive
  - Confidential
  - Critical
  - Proprietary
  - Personally identifiable information (PII)
  - Health information
  - Financial information
  - Government data
  - Customer data
- Privacy enhancing technologies
  - Data minimization
  - Data masking
  - Tokenization
  - Anonymization
  - Pseudo-anonymization
- Roles and responsibilities
  - Data owners
  - Data controller
  - Data processor

SIEM XPERT
Learn. Secure. Succeed.

SECURITY+ CERTIFICATION (SYLLABUS)

  - Data custodian/steward
  - Data protection officer (DPO)
- Information life cycle
- Impact assessment
- Terms of agreement
- Privacy notice

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 XPE
Learn. Secure. Succeed.

SULABH MISHRA

CEO, Cyber Security Trainer & Solution Architect

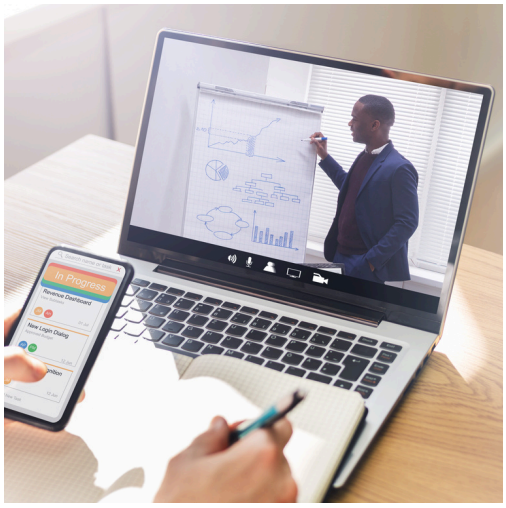
Sulabh Mishra has around 12+ years of experience in Cyber Security. He worked as Security tool administrator, Technical Consultant, Solutions Architect in the companies like Altisource, Accenture, Ericsson etc. Sulabh is Certified expert for Arcsight, Splunk, McAfee, Qradar and other SIEM tools as well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

CEH Certified Ethical Hacker

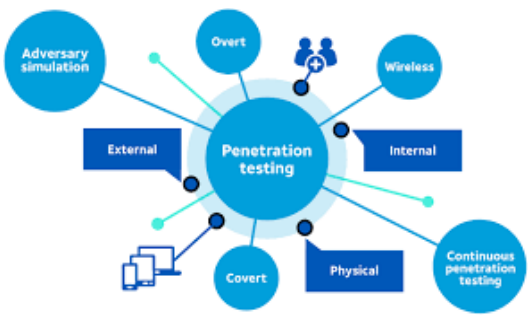
CISSP Certified Information Systems Security Professional

CISA Certified Information Systems Auditor. An ISACA Certification

SIEM XPERT
Learn. Secure. Succeed.

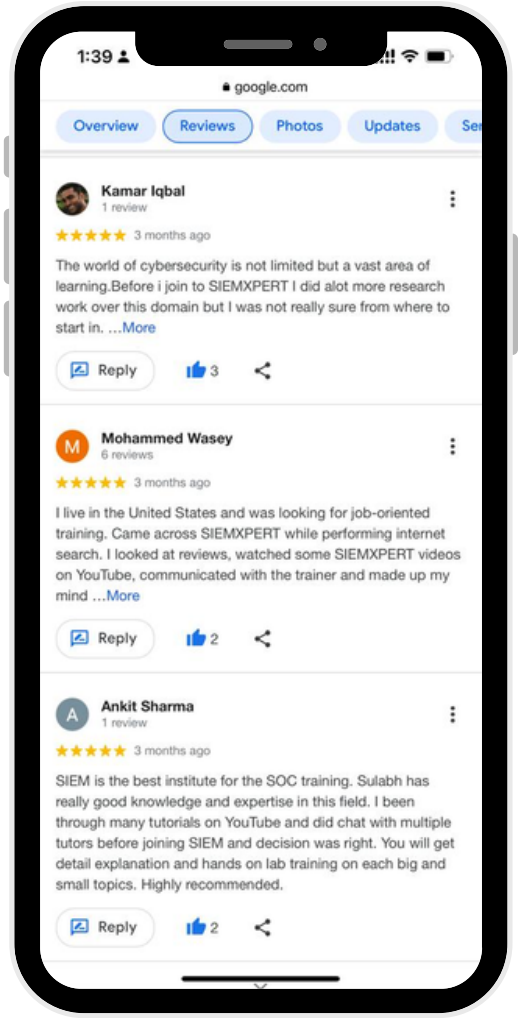
CYBER SECURITY SERVICES

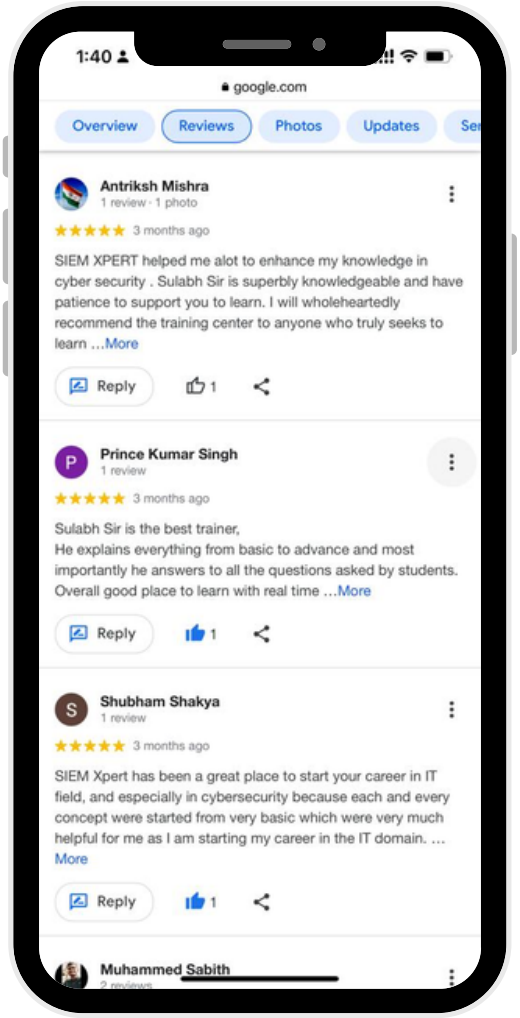
- Managed SOC Services
- Penetration services
- Security compliance and governance services
- and many more



WHAT OUR **TRAINEES** ARE SAYING

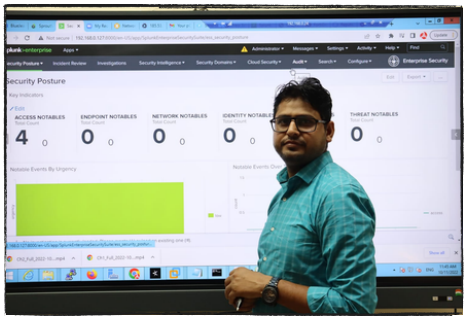
4.8 ★★★★★ **2031 Google reviews**





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