Techonquer

Techonquer Certified SOC Analyst (TCSA) Training

From Beginner to Job-Ready SOC Professional in 3 Months

- Introduction to Cybersecurity
- Network & Security
- Security Operations Centre Fundamentals (SIEM/SOC)
- Phishing Analysis &Threat Intelligence

Join the course today!

https://techonquer.org/Soc-course

Class Details &Training Details

Class Details

- **Classes per Week: 3 Days**
- **Training Duration: 2 to 3 Months**
- **Class Timings: 8:00 PM – 9:30 PM (IST)**

Training Mode

- **100% Live Instructor-Led Classes**
- **Lifetime Recording Access for all sessions**
- **If you miss any live session, you can cover the complete class using recordings anytime**
- **Sessions are designed to be interactive and practical-focused**

Join our Course Today

https://techonquer.org/Soc-course

Class Details &Training Details

Mentorship & Support

- **Dedicated Mentor Support throughout the training**
- **1-to-1 mentor doubt-solving sessions**
- **Continuous guidance and coordination support during the course**
- **Mentor assistance for concept clarity, hands-on practice, and career guidance**

Tools Covered (Hands-On)

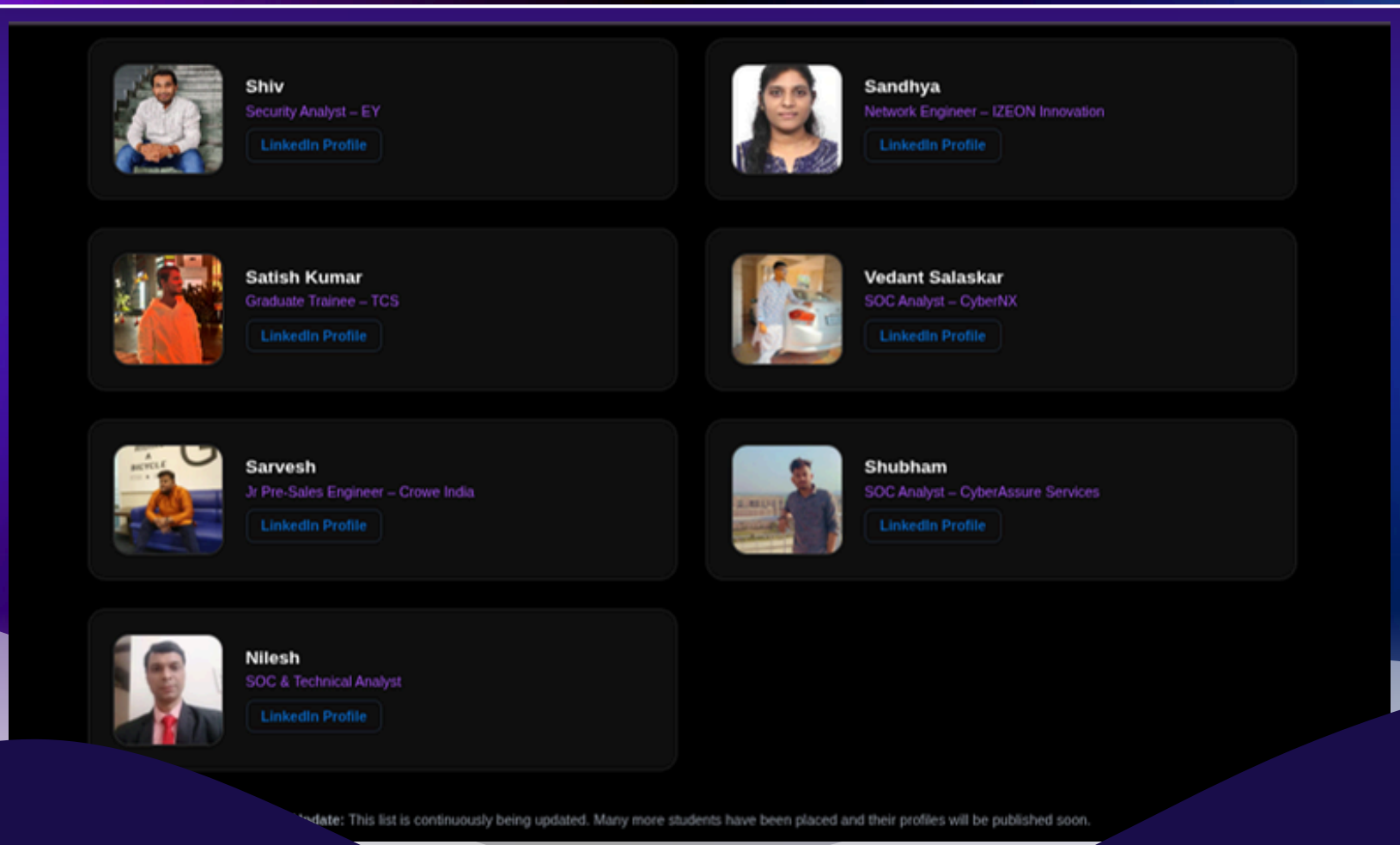
- **SIEM Tools (Practical Exposure):**
  - **ArcSight**
  - **Seceon**
  - **Splunk**

Join our Course Today

https://techonquer.org/Soc-course

Our Placed Students

Success stories of learners who transformed their careers through Techonquer's trainings



Techonquer

Module 1

Introduction to Cybersecurity

- Need of Cybersecurity, CIA Triad, Threat, Vulnerability, Exploit and Risk
- Vulnerability Management and Risk Management
- Hacking and its types
- Types of Threats
- Security Controls: Preventive vs. Detective
- Defense in Depth, Offensive Security & Defensive Security

Join the course today!

https://techonquer.org/Soc-course

Techonquer

Module 2

Introduction to Network & Security

- Introduction to OSI Model
- Overview of TCP/IP Model
- Understanding LAN and WAN Networks with Routers and Switches
- Working of Common Network Protocols (ARP, DNS, HTTP, TCP/IP)
- Concept of Firewalls including Stateful and Next-Generation Firewalls
- Understanding Web Application Firewall (WAF)
- Difference Between IDS and IPS

Join the course today!

https://techonquer.org/Soc-course

Techonquer

Module 3

Security Operations Centre Fundamentals (SIEM/SOC)

- People, Processes, and Technology
- Understand the Implementation of SOC
- Understand the SOC

SIEM Fundamentals & Architectures (ArcSight, Splunk, Seceon)

- Overview of SIEM architecture: log collection, parsing, normalization, correlation, and alerting.
- Hands-on understanding of enterprise SIEM tools such as ArcSight, Splunk, and Seceon.
- Creating and tuning correlation rules to reduce false positives.
- Integrating SIEM with EDR, threat intelligence feeds, and SOAR platforms for advanced detection and response.

Join the course today!

https://techonquer.org/Soc-course

Techonquer

Module 4

Linux Logs Analysis

- Introduction to Log Management in Linux
- Understanding Linux Log Architecture
- Common Linux Log Files (/var/log)
- Authentication Logs Analysis
- System Logs and Service Logs
- Kernel Logs and Boot Logs
- SSH Logs and Brute Force Detection
- Web Server Logs (Apache / Nginx)
- Log Correlation in Linux Environment
- Identifying Suspicious Activities from Linux Logs
- Basics of Log Correlation for SOC Use Cases

Join the course today!

https://techonquer.org/Soc-course

Techonquer

Module 5

Windows Logs Analysis

- Introduction to Windows Log Management
- Understanding Windows Event Logging
- Types of Windows Logs (Security, System, Application)
- Windows Event IDs and Their Importance
- Authentication & Logon Event Analysis
- Privilege Escalation Indicators in Windows Logs
- Process Creation and Command Execution Logs
- PowerShell and Script Activity Logs
- Alert Generation and Alert Triage in SIEM
- SOC Terminologies Related to Windows Logs
- Correlating Windows Logs for Threat Detection

Join the course today!

https://techonquer.org/Soc-course

Techonquer

Module 6

Phishing Analysis

- Types of Phishing Attacks
- How Phishing Works
- How to Analyze a Phishing Email
- Email Phishing Analysis
- Phishing Attack Types
- Phishing Attack Techniques
- Phishing Attack Analysis Methodology

Join the course today!

https://techonquer.org/Soc-course

Techonquer

Module 7

Endpoint Security Fundamentals

- Introduction to Endpoint Security and its role in SOC operations
- Understanding endpoint threats: malware, ransomware, fileless attacks
- Basics of EDR/XDR and endpoint visibility
- Endpoint monitoring, logging, and alert generation
- Importance of endpoint security in incident response

Join the course today!

https://techonquer.org/Soc-course

Techonquer

Module 8

Networks Analysis

- Fundamentals of network traffic analysis and packet inspection
- Understanding protocols, logs, and network flow data
- Detecting anomalies, threats, and suspicious activities
- Hands-on analysis using real-world network scenarios and tools

Join the course today!

https://techonquer.org/Soc-course

Techonquer

Module 9

Windows Endpoint & Process Analysis

- Windows OS architecture overview for SOC analysts
- Understanding Windows core processes (svchost.exe, lsass.exe, winlogon.exe, explorer.exe)
- Windows process analysis for detecting malicious activity
- Identifying suspicious parent-child process relationships
- Practical use cases: detecting malware and persistence techniques on endpoints

Join the course today!

https://techonquer.org/Soc-course

Techonquer

Module 10

Threat Intelligence

- Introduction to Threat Intelligence
- TYPES OF THREAT INTELLIGENCE
- THREAT HUNTING METHODOLOGIES
- THREAT INTELLIGENCE LIFECYCLE
- SOURCES OF THREAT INTELLIGENCE
- Indicators of Compromise (IOCs)
- Indicators of Attack (IOAs)
- Tactics, Techniques, and Procedures (TTPs)

Join the course today!

https://techonquer.org/Soc-course

Techonquer

Module 11

MITRE ATT&CK Framework

- Understand the MITRE ATT&CK Framework to map real-world attacker tactics, techniques, and procedures (TTPs).
- Learn how threat intelligence use cases help SOC analysts detect, analyze, and respond to advanced cyber attacks.
- Apply ATT&CK mapping with SIEM, EDR, and XDR tools to improve detection accuracy and reduce false positives.
- Gain hands-on experience in correlating threat intelligence feeds with ATT&CK techniques for proactive defense.

Join the course today!

https://techonquer.org/Soc-course

Techonquer

Module 12

CTFs & Interview Preparation

- Format: Live hands-on CTF challenges + guided interview prep sessions
- Content: Real-world attack & defense scenarios, problem-solving challenges, and security use cases
- Focus Areas: Web, network, and basic cloud security challenges
- Interview Prep: Technical questions, scenario-based discussions, and resume guidance
- Outcome: Improved practical skills, confidence, and job-ready cybersecurity mindset

Join the course today!

https://techonquer.org/Soc-course

Techonquer

Module 13

Examination & Certification

- **Formats: Live OR remote-proctored exam**
- **Content: MCQs, case-based questions**
- **Requirements: ≥ 85% pass mark (approx. 60–90 questions)**

Join the course today!

https://techonquer.org/Soc-course

Contact us


+916367098233


info@techonquer.org


https://techonquer.org/Soc-course

Join the course today!

https://techonquer.org/Soc-course