TECHONQUER • AI-INTEGRATED CYBER DEFENSE TRAINING

Security Operations Center (SOC) Course Syllabus

Techonquer Certified SOC Analyst (TCSA)

Master Cyber Defense with AI-Powered Tools & Real-World SOC Operations

9	20+	AI	TCSA
Modules	Industry Tools	Integrated Curriculum	Certification

---

www.techonquer.org

About the Program

The Techonquer Certified SOC Analyst (TCSA) program is a job-oriented, hands-on training track built for aspiring and practicing SOC Analysts. The curriculum blends foundational blue-team skills with real SOC tooling across nine progressive modules, culminating in a dedicated AI-Powered SOC Operations module, so learners graduate ready to work alongside modern, AI-augmented security stacks from day one.

Who Should Enroll

- Freshers targeting SOC Analyst (L1/L2) roles
- IT professionals transitioning into cybersecurity
- Security enthusiasts preparing for SIEM, threat hunting, and incident response careers
- Working analysts who want to upskill on AI-assisted SOC workflows

Career Outcomes

Graduates are prepared for the following industry roles:

- SOC Analyst (L1 / L2 / L3)
- Threat Hunter
- Incident Response Analyst
- SIEM Engineer
- Cloud Security Analyst
- AI-Augmented Security Analyst

Course Modules

A complete, tool-first curriculum covering SOC fundamentals through advanced AI-powered defense operations. Nine modules, each built around real tools and hands-on labs.

01 SOC Fundamentals

Build the foundation of modern SOC operations, from structure to success metrics.

- SOC importance in enterprise cyber defense and today's evolving threat landscape
- SOC models: in-house, managed (MSSP), hybrid, and virtual SOC
- SOC tiers explained: L1 Triage Analyst, L2 Incident Responder, L3 Threat Hunter / Lead
- Daily SOC workflows: shift handovers, escalation paths, and ticketing discipline
- Performance Monitoring: KPIs and metrics, including MTTD, MTTR, alert-to-incident ratio, and false-positive rate

Tools & Labs: SOC workflow simulation, ticketing walkthrough

02 Threat Hunting and Threat Intelligence

Move from reactive alerting to proactive, intelligence-led defense.

- Types of Threat Intelligence: tactical, operational, and strategic, and how each drives decisions
- Threat Intel lifecycle: collection, processing, analysis, and dissemination
- MITRE ATT&CK framework: mapping attacker tactics, techniques, and procedures (TTPs)
- Threat Hunting methodologies: hypothesis-driven hunting and behavioral baseline analysis
- Identifying and pivoting on IoCs: hashes, domains, IPs, and URLs
- Building and consuming threat intel feeds: OSINT, MISP, and commercial sources

Tools & Labs: MITRE ATT&CK Navigator, MISP, IoC pivoting exercise

03 Mastering SIEM Tools

Turn raw logs into actionable, high-fidelity detections.

- SIEM architecture: log sources, ingestion pipelines, normalization, and correlation engines
- Writing and tuning correlation rules for real-world detection use cases
- Alert management: severity classification, deduplication, and noise reduction
- Building dashboards and reports for SOC leadership and stakeholders
- Hands-on rule creation and log search in IBM QRadar and Splunk

Tools & Labs: IBM QRadar, Splunk (SPL basics)

04 Proactive Vulnerability Management

Find and fix weaknesses before attackers exploit them.

- Vulnerability management lifecycle: scan, assess, prioritize, remediate, verify
- Network Scans: open ports, misconfigurations, and outdated services
- Web Scans: OWASP Top 10-aligned web application vulnerability assessment
- Cloud Scans: misconfigurations across AWS, Azure, and GCP infrastructure
- Risk scoring and remediation prioritization using CVSS

Tools & Labs: Nessus, OpenVAS, Scout Suite

05 Incident Response and EDR

Detect, contain, and recover from real security incidents with confidence.

- Preparation: IR playbooks, team roles, and communication plans
- Detection: correlating SIEM and EDR signals to confirm true incidents
- Containment: endpoint isolation, network segmentation, short- vs long-term response
- Eradication & Recovery: safely removing threats and restoring systems
- Post-Incident Review: root-cause analysis and lessons-learned documentation
- EDR deep-dive: endpoint telemetry, process trees, and behavioral detection rules

Tools & Labs: Wazuh, Sophos EDR console walkthrough

06 Network Security Monitoring and Automation

See every packet, catch every anomaly, and automate the response.

- Packet-level traffic analysis using Wireshark and Tcpdump
- IDS/IPS deployment and tuning with Snort and Suricata
- Writing custom detection signatures for network-based threats
- SOAR fundamentals: automating alert triage and response playbooks
- Reducing analyst fatigue with automation-first SOC workflows

Tools & Labs: Wireshark, Tcpdump, Snort, Suricata, SOAR playbook design

07 Securing Cloud Environments

Extend SOC visibility and control into AWS, Azure, and GCP.

- Shared Responsibility Model across major cloud providers
- Common cloud-native threats: misconfigured storage, IAM privilege escalation, exposed APIs
- Cloud security assessment with Scout Suite, Prowler, and Pacu
- Centralized logging and monitoring using AWS CloudTrail and Azure Monitor
- Building cloud-specific detection use cases inside the SOC

Tools & Labs: Scout Suite, Prowler, Pacu, AWS CloudTrail

08 AI-Powered SOC Operations (NEW)

Work the way modern SOCs actually work: alongside AI, not without it.

- AI-driven threat detection: ML-based anomaly and behavioral detection inside SIEM/EDR pipelines
- Generative AI for alert triage: using AI copilots to summarize, correlate, and prioritize high-volume alerts
- AI-assisted threat intelligence: automated IOC enrichment, correlation, and report generation
- Prompt engineering for analysts: structuring prompts for log analysis, incident summaries, and documentation
- AI-augmented SOAR: integrating AI decision layers into automated response playbooks
- AI risk & governance: prompt injection, data leakage, and OWASP LLM Top 10 fundamentals for defenders

Tools & Labs: AI copilot-assisted alert triage lab, LLM-assisted log analysis exercise

09 SOC Tools Mastery (Capstone)

Bring every skill together in one consolidated, tool-driven simulation.

- SIEM: IBM QRadar, Splunk
- Vulnerability Scanning: Nessus, OpenVAS, Scout Suite
- Threat Hunting: MITRE ATT&CK Navigator, MISP
- EDR: Wazuh, Sophos
- Capstone simulation: multi-tool incident combining detection, triage, and response

Tools & Labs: Full SOC toolchain, capstone incident simulation

Get in Touch

Ready to start your SOC career journey? Reach out to the Techonquer team.

Email
team@techonquer.org

Phone
+91 6367098233

Website
www.techonquer.org

Location
Techonquer Pvt Ltd, Bengaluru, Jaipur, India