AMIT AMBEKAR

Senior SOC Team Lead | Cybersecurity Operations & Threat Detection Leader

Mumbai, India | +91-77200 10054 | amitambekar510@gmail.com
LinkedIn | GitHub | Medium | Hashnode | DEV.to | OTX AlienVault

PROFESSIONAL SUMMARY

Senior Security Operations Analyst and SOC Team Lead with **4+ years** of hands-on cybersecurity experience directing **24x7 SOC operations** for BFSI, brokerage, and enterprise clients. Proven track record building SOC functions from the ground up, leading teams of **10-24+ analysts**, and driving measurable outcomes: **30% faster incident resolution**, **25% MTTR reduction**, **40-45% false-positive reduction**, and client onboarding time cut from **4 weeks to 1 week**. Combines hands-on SIEM/EDR engineering and threat intelligence with vendor relationship and budget ownership, regulatory-driven SOC efficacy (**SEBI CSCRF, ISO 27001, PCI DSS**), and trusted incident command for CISOs and IT leadership. Currently targeting **Security Operations Manager / SOC management** roles.

CORE COMPETENCIES

✓ **SOC Leadership (24+ Analysts)**	✓ **Incident Response & Command**	✓ **SIEM Engineering (Elastic, XSIAM, Seceon)**
✓ **EDR/XDR Operations**	✓ **Threat Intelligence & Hunting**	✓ **VAPT Coordination**
✓ **SEBI CSCRF Compliance**	✓ **ISO 27001 / PCI DSS**	✓ **Client & CISO Stakeholder Mgmt.**

TECHNICAL SKILLS

SIEM	Elastic SIEM, Cortex XSIAM, Seceon SIEM
EDR/XDR	SentinelOne, CrowdStrike, Kaspersky EDR
Network Security	FortiGate, SonicWall
Threat Intelligence	Kaspersky TI, Qfeeds, GitHub Feeds, GitLab Threat Feeds
Log Analysis	Event Log Analyzer, Logify
Network Monitoring	Observium, ZOHO Services
Vulnerability & AppSec	Nessus, Burp Suite Pro, Postman, Acunetix, Mobexler, APK Easy Tool, MobSF, SecPod, Endpoint Central

PROFESSIONAL EXPERIENCE

Comtel Infosystem Private Limited | *Mumbai* — **Feb 2026 - Present**

SOC Team Lead

- **Lead a 10-analyst SOC team** supporting multiple brokerage clients in a high-volume, regulated security environment.
- Own end-to-end SOC operations across SIEM, EDR, and event analysis functions spanning diverse security toolsets.
- Coordinate SIEM operations end-to-end - log source onboarding, use-case development, and integration of new devices into the monitoring ecosystem.
- Partner with SIEM parsing teams to onboard new log sources and ensure accurate normalization and correlation.
- Develop and maintain **TOML-based detection rules** to strengthen threat detection coverage and reduce blind spots.
- Manage client onboarding end-to-end: requirement gathering, integration planning, and operational readiness.
- Lead recurring client meetings and stakeholder communications, aligning security posture and incident response strategy.
- Author SOC policies, processes, handbooks, playbooks, analytics graphs, and reporting templates as standard operating procedure.
- Built a **dedicated SOC room from the ground up**, covering infrastructure, tooling, and workflow design.
- Perform SOC efficacy assessments aligned with **SEBI CSCRF** regulatory frameworks.
- Run Vulnerability Assessment (VA) and Compliance Assessment (CA) for infrastructure supporting SOC operations.
- Drive alert-noise reduction initiatives across SIEM and EDR platforms, cutting false positives by **40-45%** and improving detection efficiency.
- Cut client onboarding timeline from **4 weeks to 1 week** by streamlining requirement gathering, integration planning, and readiness workflows.

- Sustain SLA and response-time commitments under a lean team structure by prioritizing automation and alert-fidelity improvements - an active focus area while scaling the team.
- Own vendor relationships for SIEM/EDR platforms and contribute to SOC tooling budget planning, resolving escalations and coordinating issue resolution directly with vendors.
- Maintain active engagement with a Europe-based Event Analysis Tool vendor and multiple Threat Intelligence vendors, authoring product-focused technical blogs and continuously evaluating emerging tools to track the cybersecurity market.
- Designed and deliver a structured **15-day analyst training program** (weekly cadence) covering escalation protocols and threat-hunting fundamentals - **6 analysts** trained to date.
- Contribute to platform rollout initiatives through vendor coordination and rollout planning, staging evaluation environments in partnership with the dedicated Engineering team.
- Present SOC performance and compliance reports to internal leadership on a recurring basis; serve as primary point of contact with auditors during audit cycles to resolve compliance findings.
- Liaise with law enforcement agencies to verify and investigate suspicious IPs linked to criminal activity.
- Represent the organization as an exhibitor at industry events, including ANMI Convention and Finbridge Expo.

Audix Techno Consulting Solutions | *Mumbai* Apr 2022 - Jan 2026

Senior Security Operations Analyst - SOC Team Lead | Apr 2024 - Jan 2026

- Led **24x7 SOC operations across Nashik & Mumbai**, managing a **24-member team** and ensuring continuous monitoring and incident handling.
- Improved incident resolution efficiency by **30%** and cut MTTR by **25%** through process optimization and refined triage workflows.
- Served as **Incident Commander** for P1/Critical security incidents, driving containment, recovery, and client communication.
- Implemented external threat intelligence ingestion using External Fabric, expanding proactive detection coverage.
- Acted as primary SOC point of contact for client CISOs and IT leadership during incidents, audits, and monthly governance reviews.
- Supported audit and compliance activity aligned with **ISO 27001, PCI DSS**, and regulatory SOC requirements.
- Conducted SOC efficacy assessments aligned with **SEBI CSCRF** guidelines.
- Coordinated across Firewall, Server, VAPT, GRC, and Dev teams to streamline response and remediation.
- Integrated critical and non-critical devices with SIEM platforms across client environments.
- Maintained SOC documentation: SOPs, runbooks, escalation matrices, and analyst knowledge bases.
- Coordinated with SIEM/EDR vendors on tool tuning, issue resolution, and feature optimization.
- Developed and enforced SOC policies and SOPs to support audit and certification readiness.

Cyber Security Analyst | Apr 2022 - Mar 2024

- Monitored SIEM/EDR alerts and performed triage, investigation, and escalation for 24x7 operations.
- Supported SOC shift scheduling, analyst onboarding, and workload distribution.
- Conducted hypothesis-driven threat hunting using SIEM and EDR telemetry to surface stealthy threats.
- Tracked and improved SOC KPIs, including MTTD, MTTR, alert volume, and SLA adherence.
- Designed, tuned, and optimized SIEM use cases to reduce false positives and improve detection accuracy.
- Conducted Black Box and Grey Box VAPT, application retesting, and remediation validation.
- Designed custom Nessus scan policies and vulnerability reports.
- Led client-facing SOC monthly review meetings and reporting.
- Traveled PAN-India for SOC onboarding and implementation engagements.

CERTIFICATIONS

- Certified Ethical Hacker (CEH) & Certified Incident Handler (CIH) - EC-Council
- ISO/IEC 27001:2022 Lead Auditor, ISO/IEC 27701:2025 Lead Auditor & ISO/IEC 42001:2023 Lead Auditor - Mastermind
- Cyber Threat Intelligence 101 - ArcX
- Certified Network Security Practitioner (CNSP), Certified Cloud Security Practitioner (CCSP) & Certified AppSec Practitioner (CAP) - The SecOps Group
- Certified AI Agent Security Specialist - Proofpoint
- SailPoint Identity Security Leader Credential - SailPoint Technologies
- FALCON 101: Falcon Platform Essentials - CrowdStrike University
- OT Security Expert (OOSE) - OPSWAT Academy
- Seceon OTM Advanced & Foundation Course Certified - Seceon
- PCI DSS Awareness - TUV SUD
- Microsoft Technology Associate - Certiport
- Certified Information Security Manager (CISM) - ISACA — In Progress; ISACA membership planned

EDUCATION

PGDBM in IT & Systems Management - Narsee Monjee Institute of Management Studies, Mumbai **2025**
Cyber Law - Symbiosis Centre for Distance Learning (SCDL), Pune **2021**

ACHIEVEMENTS

- Best Employee of the Month - Audix Techno Consulting Solutions
- Most Promising Newcomer - Audix Techno Consulting Solutions
- Bright Beginner Award - Audix Techno Consulting Solutions
- Industry Event Exhibitor & Representative - Comtel Infosystem Private Limited
- Active vendor collaborator with a Europe-based Event Analysis Tool provider and multiple Threat Intelligence brands, contributing product-focused technical content

PROJECTS & PUBLICATIONS

- Technical Blogger covering SOC operations and CISO-level security topics - Medium, Hashnode, DEV.to
- Threat Intelligence Pulse creation and curation - OTX AlienVault
- MITRE ATT&CK detection rule development (.toml) for Elastic/ELK - GitHub
- Linux system and FIO benchmark reporting script - GitHub
- Curated threat-intel repositories: malicious domains, malicious IPs, and malicious hash values (MD5/SHA-1/SHA-256)
- Advanced SIEM tooling playbooks - GitHub

LANGUAGES

English, Hindi, Marathi

DECLARATION

I, **Amit Ambekar**, hereby declare that the information furnished above has been verified with the same rigor I apply to validating a threat indicator before it reaches a SOC dashboard - accurate, evidence-based, and true to the best of my knowledge. I remain committed to upholding the highest standards of integrity, confidentiality, and vigilance that the cybersecurity profession demands.

Amit Ambekar
Mumbai, India