Tushar Santosh Patil

SECURITY ANALYST

tushar.patil.5202@gmail.com 9359021293 Tushar Patil Mumbai Portfolio

PROFILE

Cybersecurity Manager with extensive experience in SOC leadership, threat intelligence strategy, security governance, and risk management. Proven ability to optimize SIEM efficiency, enforce compliance (ISO 27001, PCI-DSS, GDPR), and lead cybersecurity teams to enhance threat detection and mitigation. Expertise in security policy development, vulnerability management, incident response, and automation of security workflows to minimize organizational risk. Passionate about building resilient security infrastructures and training teams to combat evolving cyber threats.

WORK EXPERIENCE

Deputy Manager 01/2025 – present

Kotak Mahindra Bank

- **Led and managed a high-performing SOC team**, enhancing threat detection, incident response, and vulnerability management efficiency.
- **Developed and enforced security governance policies**, ensuring compliance with **ISO 27001, NIST, RBI Guidelines, PCI-DSS, and GDPR**.
- **Orchestrated cross-functional collaboration** with IT, compliance, and executive leadership to align cybersecurity initiatives with business objectives.
- **Spearheaded proactive threat intelligence initiatives**, leading to a **25% reduction in cybersecurity incidents** and improved mitigation strategies.
- **Implemented advanced security automation frameworks**, reducing manual intervention in SOC workflows and increasing efficiency by **35%**.
- **Drove security awareness and training programs**, fostering a strong security-first culture among employees, reducing social engineering risks.
- **Led post-incident forensic investigations**, ensuring root cause analysis and lessons learned were effectively implemented to prevent recurrence.

Soc Analyst L2 10/2024 – 01/2025

Network Techlab India Private Limited Thane

- Led **SOC operations**, managing real-time **threat detection, triaging security incidents, and implementing remediation strategies**.
- Conducted in-depth **incident response investigations**, ensuring threats were contained, eradicated, and recovery processes were initiated efficiently.
- Configured and optimized **SIEM platforms** (Splunk, Seceon, QRadar) to improve threat intelligence and event correlation accuracy.
- Strengthened **firewall policies and intrusion detection systems**, reducing unauthorized access incidents by **20%**.
- Provided **security recommendations** to senior management, contributing to strategic risk reduction initiatives.

SOC Executive 06/2024 – 10/2024

Synergistic Financial Networks Pvt Ltd (Mosambee) Andheri, Mumbai

- Monitored and analyzed **security events** across the enterprise network, proactively identifying and mitigating **potential threats**.
- Conducted **forensic investigations** on security breaches, preparing comprehensive reports for senior management and incident response teams.
- Enhanced **SIEM configurations**, fine-tuning rule sets to reduce **false positives by 25%** while improving **threat detection capabilities**.
- Assisted in the **implementation of security controls**, ensuring compliance with organizational cybersecurity policies.

SOC ANALYST Lvl 1 01/2023 – 05/2024
SAMAY INFOSOLUTION PVT LTD Vikhroli, Mumbai

- Performed real-time monitoring of over 200+ daily **security alerts**, identifying and responding to critical incidents using **SIEM** tools.
- Implemented and managed **Endpoint Detection and Response (EDR)** solutions, improving endpoint security by 30%.
- Conducted log analysis and security event correlation to detect advanced persistent threats (APT), minimizing false positives by 25%.
- Managed firewall configurations using **Sophos**, ensuring compliance with corporate security policies and reducing unauthorized access attempts.
- Deployed **Privileged Access Management (PAM)** tools like **Fudo Security** to safeguard privileged accounts, reducing insider threats by 15%.
- Participated in the enhancement of security policies and procedures, ensuring alignment with industry standards like **NIST** and **ISO 27001**.
- Delivered comprehensive security reports and recommendations for risk mitigation to senior management on a monthly basis.

INTERNSHIP

SECURITY ANALYST INTERN 09/2022 – 12/2022
SAMAY INFOSOLUTION PVT LTD Vikhroli, Mumbai

- Assisted in **real-time threat monitoring**, working alongside SOC analysts to mitigate **potential security breaches**.
- Gained hands-on experience with **SIEM platforms** and **EDR deployment projects**, supporting **log analysis and forensic investigations**.
- Contributed to the **creation of security playbooks**, improving response efficiency for common security incidents.

JUNIOR NETWORK ENGINEER 05/2017 – 06/2017
C.S.INFOCOMM Mulund, Mumbai

- Assisted in configuring and maintaining **enterprise network infrastructure**, including **firewall rule implementations**.
- Supported network troubleshooting and **connectivity issue resolution** to improve operational efficiency.

SKILLS

- **Security Operations & Threat Monitoring:** SIEM (Seceon, Splunk, QRadar, SISA SIEM), SOAR (Phantom, Demisto), Azure Sentinel, IBM QRadar, ArcSight
- **Endpoint Security & Incident Response:** CrowdStrike, Seceon EDR, Sophos MDR, Carbon Black, Microsoft Defender ATP
- **Firewall Management & Network Security:** Palo Alto, Sophos, Fortinet, Cisco ASA, Check Point
- **Threat Intelligence & OSINT:** Shodan, AlienVault, VirusTotal, MISP, ThreatConnect
- **Vulnerability Assessment & Risk Management:** Nmap, Nessus, OpenVAS, Qualys, Tenable.sc
- **Privileged Access & Identity Management:** FUDO Security, CyberArk, Okta, SailPoint
- **Penetration Testing & Ethical Hacking:** Metasploit, Burp Suite, Kali Linux, Cobalt Strike, BloodHound
- **Log & Traffic Analysis:** Elastic Stack (ELK), Graylog, Wireshark, tcpdump, Zeek (Bro)
- **Automation & Security Monitoring:** Wazuh FIM, Site24x7, Nagios, Ansible, Python for Security Automation
- **Cloud Security & Compliance:** AWS Security, Azure Security, Google Cloud Security, CloudTrail, GuardDuty, Prisma Cloud
- **Compliance & Governance:** ISO 27001, NIST, CIS Benchmarks, GDPR, RBI Guidelines, PCI-DSS, SOX

EDUCATION

Bachelor of Engineering in Cyber Securtiy 2021 – 2024
Shah And Anchor Kutchhi Engineering College

Diploma in Computer Engineering 2017 – 2021
Government Polytechnic, Malvan

CERTIFICATES

ADVANCED PROGRAM IN FULL STACK SOFTWARE ENGINEERING
Certificate Number: *22AAZZZZZ983*

CERTIFIED ETHICAL HACKER (MASTER)
Certification Number: *ECC3475982016*

CERTIFIED PRACTICAL NETWORK PENETRATION TESTER™ (PNPT)
Certification Number: *101056624*

ACHIEVEMENTS

Mentored the winning team – Smart India Hackathon (SIH) 2024 12/2024
Guided a team to victory through technical expertise and strategic mentorship.

SMART INDIA HACKATHON (2023) 12/2023
National Level Competition Winner

CERTIFIED SECEON PROFESSIONAL 10/2023
Certification ID: *SECQ423106*

BEFOJJI OPSEC NGO 12/2022
Co-Lead Intern

Anti Cyber Crime Society 10/2022
Anti-Phishing Volunteer

PROJECTS

- **LAN-Based Examination System**: Developed a system using Java for efficient examination processes.
  - **Triple DES Encryption System**: Created a desktop application in Python to enhance data security through Triple DES encryption.
  - **Steganography**: Designed and implemented an image steganography desktop application to conceal information within digital media.
  - **INFOSINT**: Developed a Python-based OSINT information-gathering tool.
  - **ScanViz**: Built a tool for handling large **Nmap** output data efficiently using Python.