Shubh Patel

Phone: +91 7016104533 | Email: shubhpatel9351@gmail.com | LinkedIn: linkedin.com/in/CTFxShubh | GitHub: github.com/CTFxShubh

Summary

A Security Operations Center Analyst with expertise in threat intelligence, SIEM analysis, log analysis, and incident response. Passionate about cybersecurity, vulnerability assessment, and malware analysis. Adept at securing enterprise environments and mitigating cyber threats. Always curious, I stay updated on new cyber threats to strengthen security.

Technical Skills

Tools: Splunk, Seceon, IBM X-Force Exchange, Wireshark, Nmap, VirusTotal, Ghidra

Skills: SIEM (Security Information & Event Management), Log Analysis, Threat Hunting, Incident Response, Digital Forensics, Malware Analysis, Endpoint Security, Vulnerability Assessment

Operating Systems: Linux, Windows

Networking: TCP/IP, Firewalls, IDS/IPS

Projects

Net Probe 01/2023 – 06/2023
Cybersecurity Tool

- Developed a C-based cybersecurity tool that automated network device discovery, port scanning, and vulnerability assessment, increasing scanning efficiency by 40%.
- Integrated multiple scanning techniques to enhance security analysis.
- Generated detailed vulnerability reports for security audits.

Experience

Security Operations Center Analyst Intern 12/2024 – Present
TechDefenceLabs Solutions Limited *India, On-Site*

- Proactively hunted 50+ security threats using SIEM logs and threat intelligence tools.
- Analyzed 5,000+ logs/day, detecting 30+ security incidents per month and improving incident response efficiency by 20%.
- Investigated and mitigated malware infections, phishing attacks, and unauthorized access attempts, ensuring cybersecurity threat prevention and incident response.

Cyber Security Intern 09/2024 – 10/2024
HackWithEthics *India, Remote*

- Conducted network security scans identifying 10+ vulnerabilities weekly.
- Led investigation & response for 50+ security incidents, reducing MTTD (Mean Time to Detect) by 25%.
- Monitored real-time security alerts and analyzed network traffic to detect and prevent potential security breaches.

Cyber Security Intern 10/2024 – 11/2024
Code Alpha *India, Remote*

- Analyzed security logs to detect anomalies, identify threats, and enhance system defenses.
- Identified, analyzed, and removed malware to maintain system security and operational integrity.
- Monitored and analyzed phishing attempts to prevent unauthorized access and mitigate data breaches.

Education

Parul University Vadodara, GJ
B.Tech in Computer Science and Engineering (Cybersecurity) — CGPA: 7.0/10 *06/2021 – Present*
Kokilaben Dhirubhai Ambani Reliance Foundation School Jamnagar, GJ
Higher Secondary Certificate (HSC) — Percentage: 71% *07/2020 – 07/2021*
BAPS Swaminarayan Chhatralaya Vadodara, GJ
Secondary Education — Percentile: 77.7 *03/2018 – 03/2019*

Certifications

- Q1 2025 Innovation & Certification Days – Seceon
- CompTIA Cybersecurity Analyst (CySA+) – Cybrary
- Access Controls Certification – Cybrary
- Introduction to Zero Trust – The Linux Foundation
- Networking Essentials Certification – Cisco Networking Academy
- Networking and Web Technology Certification – Infosys

Publications

- Patel, S., Raj, K., Christian, P., Mistry, K., & Raithatha, H. (2024). Enhancing Network Security with Advanced Network Scanning Tools. IEEE. DOI: **10.1109/PICET60765.2024.10716055.**

Web Links

- TryHackMe Profile: https://tryhackme.com/r/p/CTFxShubh
- Portfolio: http://cybersecurityanalyst.me/
- LinkedIn: linkedin.com/in/CTFxShubh
- GitHub: github.com/CTFxShubh

Soft Skills

- Analytical thinking for security incident analysis.
- Strong team collaboration in cybersecurity investigations.
- Quick adaptability to new cyber threats and security tools.
- Effective time management in incident response.
- Clear documentation for threat reporting and analysis.