Shubham Mane

Chicago, IL 60613
312-539-9755 • shubhammane56@gmail.com
linkedin.com/in/shubhmane

Professional Summary

Senior Security Analyst with 8+ years of experience leading complex security assessments, penetration testing, and incident response initiatives across enterprise environments. Proven expertise in applying NIST cybersecurity frameworks, managing robust vulnerability management programs, and optimizing SIEM solutions to reduce response time and improve threat detection. Adept at mentoring junior analysts, developing security policies, and collaborating cross-functionally to embed security best practices throughout the organization. Skilled in forensic investigations, threat intelligence, and cloud security with hands-on experience in scripting and automation.

Technical Skills

Networking: Packet Analysis (tcpdump, Wireshark), IDS (Bro, Snort), Splunk, Firewall, IDS/IPS, Access Control

Systems Administration: Active Directory, DNS, FTP, SSH, DHCP, SMB, HTTP, Virtualization

Vulnerability Assessment: Nmap, Nessus, Ettercap, Qualys, Metasploit, Honeypots (honeyD, inetSim), BurpSuite, Nexpose, Acunetix, IBM App Scan, HP Web Inspect

End Point Security: FortiNet, McAfee Suites (VSE, HIPS & HDLP), McAfee MOVE AV, Symantec, McAfee Email Security Gateways (GUI & CLI), McAfee Network DLP, McAfee NITRO SIEM, Cisco Security (AMP, Umbrella, Email Security), FireEye HX

Platforms & Applications: Continuous Monitoring, Vulnerability Management, Web Application Scanning, ThreatProtect, Policy Compliance, Cloud Agents, Asset Management

Security Software: Nessus, Nmap, Metasploit, Snort, RSA Authentication, PIA, Demisto, CrowdStrike, CyberArk

Programming Languages: C, C++, Java, Python, JavaScript, PowerShell, Linux

Domain Knowledge: Risk Management, BCP/DRP, ISO 27001, COBIT, SWOT Analysis, Cryptography, Incident Response, Penetration Testing, Risk Assessment, SCADA Security, SCADA Audits, SIEM, ITIL, NIST, FIPS

Tools: Burp Suite, Wireshark, WebScarab, Nmap, Metasploit, SQLMap, OWASP ZAP Proxy

Web App Vulnerability Scanning: Nessus, OpenVAS, HP WebInspect, IBM AppScan, Tenable.io

Web Application Security: Manual SQL Injection, Manual Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQLMap

Professional Experience

Client: Verizon **Chicago, IL**
Senior Security Specialist *Jun 2022–Present*

- Developed and implemented threat intelligence products that matched organizational requirements and priorities.
- Monitored and analyzed threat intelligence data to identify emerging threats and attack vectors.
- Successfully managed high-priority security incidents, coordinating with cross-functional teams to contain and resolve threats with minimal downtime.
- Developed incident escalation procedures, ensuring timely notification and resolution of critical security events.
- Led complex security assessments involving penetration testing, vulnerability scanning, and risk assessments to identify and remediate critical security gaps, improving overall security posture by 30%.
- Conducted comprehensive penetration tests simulating real-world threat scenarios, resulting in the discovery and mitigation of high-impact vulnerabilities across enterprise environments.
- Designed and deployed AI-powered tools to strengthen cybersecurity across diverse platforms.
- Integrated AI-driven automation for proactive threat detection and response systems.
- Built ML models to identify malicious behavior and enhance incident response workflows.
- Applied secure design principles to AI integrations across DevSecOps environments.
- Ensured secure implementation of MyCity chatbot features through rigorous AI validation.

Client: AT&T **Pittsburg, PA**

Cyber Security Analyst *Oct 2021–Jun 2022*

- Analyzed threat intelligence data to identify common and emerging attack vectors and penetration methods.
- Collaborated with business leaders and IT teams to design security solutions that protect sensitive data without disrupting business operations.
- Translated complex security risks into business-impact statements, helping non-technical stakeholders understand security priorities.
- Applied strong working knowledge of ISO 27001 LA/LI certification requirements to design effective control frameworks and lead audit engagements.
- Assessed security risks across multi-tenant cloud environments, ensuring compliance with data protection regulations and cloud-specific security frameworks.
- Automated test case execution using Python frameworks for functional and regression testing.
- Conducted usability and performance testing for AI algorithms in production environments.
- Created and maintained test scripts to validate machine learning models.
- Evaluated AI model behavior through robust testing and anomaly detection protocols.
- Built REST API-based automation workflows to test and monitor threat management tools.
- Contributed to threat management operations by engineering custom security alerts.
- Developed security rules and detection logic for enterprise-level cybersecurity tools.
- Supported incident response teams with ML-based log analysis and alert correlation.
- Strengthened detection capabilities through API integrations with Cyber Command systems.
- Engineered response orchestration logic to streamline alert triaging.

INFOSYS Ltd. **India**

Information Security Engineer *Jun 2018–Aug 2021*

- Implemented and managed cybersecurity technologies and strategies, including the MITRE ATT&CK framework and incident response procedures.
- Conducted threat intelligence and analytics to identify and mitigate security risks.
- Managed Git-based development lifecycle for secure code deployment.
- Documented code, automation logic, and process flows for secure platform operations.
- Enhanced alert accuracy by integrating external threat intel sources into SOC tooling.
- Implemented cloud-native security controls on Azure and AWS platforms.

Icertis **India**

Infrastructure Security Analyst *Jan 2017–May 2018*

- Monitored and analyzed security logs and alerts to identify potential threats and vulnerabilities.
- Conducted penetration testing and vulnerability assessments to evaluate the effectiveness of security controls.
- Developed and implemented security processes and procedures to enhance the overall security posture.
- Worked with cross-functional teams to address security incidents and provide recommendations for remediation.
- Maintained up-to-date knowledge of common and emerging attack vectors and countermeasures.

Certifications

- **Certified Ethical Hacker (CEH)**
- **AWS Certified Solutions Architect**
- **CompTIA Security+**

Education

DePaul University **Chicago, IL**
Master of Science in Cyber Security *2021*

Dr. D.Y. Patil Institute of Technology, Pimpri **Pune, India**
Bachelor of Engineering in Computer Science *2017*