Mihir Shah

South Setauket, NY | +1 (351) 244-6372 | mihir@mihirshah.net | www.mihirshah.net

Professional Summary

CompTIA Security+ Certified Cybersecurity Analyst with hands-on experience in SOC operations, SIEM management (Splunk, Wazuh), and incident response. Proven ability to design automated threat detection workflows using Python and n8n to reduce alert fatigue. Experienced in vulnerability remediation, PII encryption, and ensuring regulatory compliance with HIPAA and GDPR. Dedicated to proactive threat hunting and strengthening enterprise security posture.

Technical Skills

Security & Monitoring: Splunk SIEM, Wazuh, Snort, MITRE ATT&CK
Forensics & Analysis: Memory Forensics (Volatility), PCAP Analysis (Wireshark), Disk Forensics (Autopsy)
Networking: TCP/IP, DNS, VPN Configuration, Firewalls
Identity & Cloud: Active Directory, IAM, Azure, AWS, GCP
Databases: MySQL, MongoDB
Programming: Python, Go (Golang), Bash, PowerShell, SQL
DevOps & Tools: Git, Docker, Kubernetes

Projects

SOC Automation & Threat Detection Architecture | *Splunk, Wazuh, n8n, Google Gemini* **Oct 2025 – Present**

- **Architected** a live Security Operations Center (SOC) environment integrating **Wazuh** for endpoint monitoring and **Splunk** for centralized log management and SIEM analysis.
- Integrated Google Gemini AI to perform automated forensic analysis on live system data (netstat, process lists), successfully reducing alert fatigue by filtering false positives before analyst review.
- Implemented a "Human-in-the-Loop" active defense strategy, configuring Slack webhooks for real-time analyst decision-making that triggers automated firewall blocking (UFW) upon verification.

Malware Detection and Analysis Framework | *Python, Yara, CNN, Docker, Kubernetes, Azure* **Aug 2024 - May 2025**

- Developed a multi-layered threat detection engine utilizing signature-based scanning (Yara rules) and heuristic analysis to identify malicious binaries.
- Leveraged Convolutional Neural Networks (CNN) to analyze file structures, significantly improving detection accuracy for zero-day threats while minimizing false positives in simulated SOC workflows.
- Deployed the solution within a containerized environment (Docker/Kubernetes) on Azure, ensuring scalable processing of suspicious files.

Law Enforcement Cybercrime Management System | *Node.JS, Cloud Deployment* **Feb 2024 - Apr 2024**

- Built a secure portal for law enforcement to streamline cybercrime case management and investigations.
- Enforced strict data security protocols by implementing Role-Based Access Control (RBAC), ensuring sensitive case data was accessible only to authorized investigators.

Work Experience

Technology Support Associate (Cybersecurity Focused) **Dec 2024 - Apr 2025**
Heuristic Pharma Perceptions Private Limited *Vadodara, India*

- Analyzed and remediated software vulnerabilities by implementing security measures such as PII encryption and input sanitization to prevent injection attacks and ensure compliance with HIPAA and GDPR standards.
- Validated system resilience and ensured compliance with security standards by developing robust testing strategies, such as creating structured documentation to validate controls.

Education

Navrachana University **Vadodara, Gujarat**
B.Tech in Computer Science and Engineering — CGPA: 8.39/10 *Jul 2021 - May 2025*

- **Relevant Coursework:** Cybersecurity, Information Security, Computer Networking, Artificial Intelligence, Cloud Computing, Operating Systems, Database Management Systems, Object-Oriented Programming, Software Engineering

Certificates

CompTIA Security+ **Aug 2025**
CompTIA

Google Cybersecurity **Dec 2023 - Nov 2024**
Coursera