# Mihir Katre

Albany, New York, 12206 • mihirkatre@gmail.com • 518-708-1649 • https://www.linkedin.com/in/mihir-katre/

## PROFESSIONAL SUMMARY

Cybersecurity Analyst with 4+ years of experience in SOC operations, incident response, and cloud security across AWS and Azure. Skilled in security monitoring, log and packet analysis, threat hunting, and adversary simulation, with a proven track record of reducing response times, closing vulnerabilities, and improving compliance. Adept at collaborating in 24/7 SOC environments, leveraging SIEM, SOAR, and automation to detect, analyze, and remediate threats.

## SKILLS

**Security Monitoring & SOC:** SIEM (Splunk, Sentinel, Security Command Center), log/packet analysis, SOAR automation, incident triage & escalation.
**Threat Detection & Response**: MITRE ATT&CK, threat hunting, malware analysis, adversary simulation, forensic analysis.
**Network & Infrastructure**: TCP/IP, DNS, HTTP/S, SMTP, DHCP; Firewalls, WAF, IDS/IPS, VPN, VPC Flow Logs.
**Cloud & Application Security**: AWS (KMS, CloudTrail, Security Hub), Azure (Sentinel, Key Vault, Firewall), GCP (Logging, SCC), container/serverless security.
**Compliance & Risk**: SOC 2, PCI-DSS, ISO 27001, NIST CSF.
**Automation & Tools**: Python, PowerShell, Bash, Burp Suite, Nessus, Wireshark, Metasploit.
**Programming & Frameworks:** C#, .NET (Core & 8), JavaScript, Blazor, Angular, Vue, REST APIs, PowerShell, Bash.

## WORK EXPERIENCE

**Tyler Technologies** — **NY, United States**
***Software Developer*** — ***May 2024 – Current***

- Embedded OWASP-based controls in applications, reducing exploitable flaws **65%.**
- Integrated security tools (Snyk, Data Dog, Burp, SonarQube) into CI/CD for **continuous monitoring.**
- Engineered a secure API with **.NET 8 and C#**, preventing **SSRF attacks** and reducing unauthorized access by **70%.**
- Conducted vulnerability assessments across apps & infra, reducing critical flaws by **45%**.
- Collaborated with internal audit and compliance teams to **remediate access control deficiencies**, reducing audit findings by **60%**.

**Deloitte** — **Mumbai, India**
***Consultant – Cloud Security & Engineering*** — ***September 2022 – July 2023***

- Led security architecture design for **multi-cloud environments (Azure and AWS)**, achieving **93%** compliance.
- Performed **security gap assessments** across multi-cloud environments, tracking remediation efforts to completion.
- Implemented Zero Trust IAM, preventing credential misuse and exposure incidents.
- Strengthened defenses (WAF, VPN, Firewalls, IDPS), minimizing service disruptions.
- Automated Application Security using **SonarQube SAST** into the **DevSecOps** pipeline, boosting code quality and reducing technical debt.
- Embedded **security-by-design** practices into CI/CD pipelines, aligning deployments with compliance requirements.

**LTIMindtree** — **Mumbai, India**
***Cloud Security Engineer*** — ***June 2020 – March 2022***

- Conducted threat modeling and log analysis, **mitigating 95% of critical vulnerabilities pre-deployment.**
- Assisted with **audit readiness** by mapping controls to SOC 2 and ISO 27001 requirements, supporting external audit reviews.
- Automated SOC workflows with Python/PowerShell, reducing analyst workload by **70%**.
- Implemented and monitored perimeter security using **Azure Firewall, Network Security Groups (NSG), and AWS Network Firewall** to detect anomalies, block unauthorized access, and enforce network segmentation policies.
- Supported incident response efforts, **cutting containment and eradication time 35%.**

## PROJECT EXPERIENCE

***Development of a Multi Cloud Monitoring Tool*** — ***Albany, NY | August 2023 – January 2024***

- Collaborated directly with the **National Security Agency (NSA)** to architect and develop a real-time security monitoring platform spanning AWS, GCP and Azure, improving cross-cloud visibility into threat indicators, IAM misconfigurations, and anomalous activities.
- Ingested, correlated, and analyzed multi-source security telemetry (CloudTrail, Azure Activity Logs, VPC Flow Logs, GuardDuty, Security Center) using **C#, SQL, PowerShell, and Vue.js**, increasing actionable threat detection by **30%**.
- Collaborated cross-functionally with DevSecOps, GRC, and cloud infrastructure teams to ensure full alignment with **NIST, CIS**, and internal compliance standards.

***Offensive Security Simulation & Pen Testing*** ***Albany, NY | August 2024 – May 2025***

- Exploited real-world vulnerabilities (OWASP Top 10, privilege escalation, insecure deserialization, SSRF, IDOR) using tools like Burp Suite, Metasploit, Nmap, OpenVAS, Wireshark, and custom exploit scripts (Python, Bash).
- Performed lateral movement, privilege escalation, and credential dumping techniques against simulated enterprise networks, uncovering critical security gaps and reducing exposure by **~50%** post-remediation.
- Designed and executed full-spectrum adversary simulations including red, blue, and purple team exercises to test organizational defenses and improve incident response playbooks.

## CTF & COMMUNITY ENGAGEMENT

- Competed in national level Capture The Flag (CTF) tournaments including **Cyber Seed, Cyber Defense Organization, and picoCTF**, achieving **top 15%** rankings in exploitation, privilege escalation, and reverse engineering challenges.
- **Completed 100+ hands-on labs on platforms** such as DVWA, TryHackMe, and Hack The Box (HTB), mastering real-world vulnerabilities including SQLi, XSS, CSRF, IDOR, SSRF, LFI/RFI, and insecure deserialization. Delivered internal knowledge-sharing sessions on vulnerability exploitation and defense-in-depth.
- **Simulated adversary tactics and techniques (TTPs)** aligned with **MITRE ATT&CK** framework to strengthen blue team defensive strategies and detection capabilities.
- **Developed custom exploit scripts and automation tools** in Python, Bash, and PowerShell to streamline vulnerability validation and proof-of-concept development.
- Collaborated with security communities and online forums, contributing write-ups, walkthroughs, and tool development for **public repositories, enhancing personal and community expertise**.

## EDUCATION

**University at Albany, State University of New York.** **Albany, NY - May 2025**

*M.S. Digital Forensics and Cybersecurity* **GPA 3.97**

Coursework: Cloud and Network Security, Web Application Security, Penetration Testing, Threat Hunting, Vulnerability Exploitation.

## CERTIFICATIONS

- **Amazon Web Services Technical Professional**
- **AWS Certified Cloud Practitioner**
- **Microsoft Certified: Azure Fundamentals - AZ 900**
- **Microsoft Certified: Azure Administrator Associate - AZ 104**
- **CompTIA Security+: In Progress**
- **Red Hat Certified Ansible Automation Specialist – Linux Academy**
- **Java Level 1, 2 - Cambridge Certification Authority**