Mihir Katre

New York • mihirkatre@gmail.com • 518-708-1649 • LinkedIn

PROFESSIONAL SUMMARY

Security Analyst with 4+ years' experience in cloud security, incident response, building and securing large-scale cloud applications and environments **(AWS, Azure) for 100K+ end users**. Skilled in threat detection, forensics, and scripting (Python, Bash) to build scalable SIEM and SOAR-driven defense solutions. Proven ability to embed security automation into the SDLC to reduce response time and strengthen organizational resilience.

SKILLS

Cloud Security: Azure (Sentinel AD, Firewall, VNET, Security Groups), AWS (IAM, CloudWatch, Security Hub, WAF, Shield)
DevSecOps: CI/CD (Azure DevOps, GitHub Actions, Bitbucket), SonarQube, Datadog, Ansible, Terraform, Docker.
Security: Secure SDLC, OWASP Top 10, SAST/DAST, Threat Modeling, MITRE ATT&CK, STRIDE, NIST.
Programming and Scripting: C#, JavaScript, Python, PowerShell, Bash.

WORK EXPERIENCE

Software Engineer - Tyler Technologies - New York, USA **May 2024 – Present**

- Built **secure web applications** using C# and JavaScript, **for 1200+ school districts, consumed by 100k+ end users,** embedding input validation and access controls.
- Integrated Model Context Protocol (MCP) to **securely enable GenAI features in production apps**, enforcing data boundaries and access controls to prevent context leakage.
- **Configured SAST tools** (SonarQube) and monitoring (Datadog) into CI/CD pipelines, performing secure code reviews that eliminated critical security flaws and **reduced production defects by 35%.**

Cloud Security Engineer – Deloitte - Mumbai, India **Sept 2022 – July 2023**

- Led **incident response investigations** for client cloud environments, a**nalyzing network logs, firewall alerts, and system telemetry** to determine root causes and **contain threats**.
- Implemented **secure networking for 30+ client environments** by configuring Firewalls, Site-to-Site VPNs, VNET peering, and encrypted channels, ensuring compliant and resilient cross-cloud communication.
- **Conducted forensic investigations** on cloud assets, analyzing logs, memory captures, and network traces to identify IOCs and reconstruct attack chains.
- Automated server hardening for **6,000+ Windows/Linux servers** using Bash and Ansible, cutting manual process time from **5 hours to <40 minutes** and aligning builds to CIS benchmarks.

Cloud Security Engineer – LTIMindtree - Mumbai, India **Jun 2020 – Mar 2022**

- **Served as primary responder for multi-cloud security alerts** from SIEM, EDR, and firewalls, triaging and remediating incidents to **maintain 99.9% service uptime**.
- Automated provisioning of 1**7,000+ cloud resources** with Terraform, enforcing security baselines and eliminating misconfigurations at scale.
- Collaborated with SOC and engineering teams to optimize network segmentation, firewall, and IDS/IPS policies, **cutting lateral movement incidents by 40%**

PROJECT EXPERIENCE

Multi-Cloud Monitoring Platform (NSA Collaboration) Albany, NY **Aug 2023 – Jan 2024**

- **Built a cross-cloud security monitoring platform** (Azure, AWS, GCP) aggregating logs and incidents, boosting anomaly detection accuracy by 30% and reducing false positives by 25%.
- Aligned detection logic and dashboards with **MITRE ATT&CK** to enhance threat investigation **across 1,000+ assets.**

EDUCATION

SUNY at Albany – M.S Cyber Security **May 2025 – GPA: 3.97**
Coursework: Cloud and Network Security, Incident Response, Threat Hunting, Computer Forensics, Web App Security.

University of Mumbai – B.S Computer Science **March 2020 – GPA: 8.93**
Coursework: Data Structures and Algorithms, Operating Systems, Advanced Java, Python, Android Dev, Game Development.