IMAM UDDIN MOHAMMED

Security Operations — Threat Detection — Incident Response

(+1) 572 208 2599 | mohammed.imamud@gmail.com | imamuddinmohammed | itsmiu | Portfolio

PROFESSIONAL SUMMARY

Security+ certified cybersecurity professional specializing in detection engineering, SIEM deployment, and threat hunting with hands-on experience building detection pipelines, identifying attacks, and strengthening security posture.

SKILLS

Security: Security Event Triage, Incident Investigation, Detection Engineering, Threat Hunting, Log Analysis (ELK, CloudTrail), IDS/IPS, SIEM Deployment, Alert Validation, Root Cause Analysis, Vulnerability Management, Cloud Security (AWS), OWASP Top 10, NIST CSF, Threat Modeling, MITRE ATT&CK, Incident Response, Networking
Cloud & Infrastructure: AWS (CloudTrail, IAM, S3, GuardDuty), Docker, Kubernetes, Linux
Security Tools: Suricata, Elasticsearch, Kibana, Logstash, Filebeat, Burp Suite, Nmap, Hydra, tcpdump, Wireshark
Languages: Python, SQL, PHP, C/C++, JavaScript
Development: Flask, React.js, Git, Postman, MVC Framework
Soft Skills: Analytical Thinking, Technical Documentation, Communication, Collaboration

EXPERIENCE

- **Application Security Intern – Paycom** May 2025 – Aug 2025
  Oklahoma City, Oklahoma
  - Performed manual and automated security testing on web applications and APIs, identifying vulnerabilities aligned with OWASP Top 10.
  - Validated exploitability and business impact to support remediation prioritization.
  - Collaborated with developers to review vulnerable code paths and improve application security posture.
  - Enhanced internal testing workflows through documentation and process improvements.
- **Secure Software Engineer Intern – Aryagami Cloud Services Pvt. Ltd.** May 2022 – Dec 2022
  Hyderabad, India
  - Developed containerized web applications using Docker and Kubernetes with secure service communication.
  - Implemented authentication, role-based access control, and encryption to protect application resources.
  - Partnered with engineering teams to identify security gaps and promote secure development practices.
- **Graduate Research Assistant – Cybersecurity, University of Central Oklahoma** Aug 2025 – Dec 2025
  Edmond, Oklahoma
  - Analyzed authentication flows and security misconfigurations across HPC schedulers using containerized testbeds.
  - Built 10+ controlled environments to detect anomalies and document security findings.
  - Created a dataset of 1,000+ labeled security events to support anomaly detection research.
- **Graduate Teaching Assistant – Computer Science, University of Central Oklahoma** Jan 2025 – Dec 2025
  Edmond, Oklahoma
  - Provided technical mentoring and evaluated coursework for computer science students.

CERTIFICATIONS

CompTIA Security+ (SY0-701) – Certified Jan 2026; Cisco Cybersecurity Essentials; Google Foundations of Cybersecurity

SECURITY PROJECTS

- **Threat Detection & SIEM Engineering Lab — GitHub**
  - Engineered a detection pipeline identifying 57 simulated attacks using custom Suricata IDS rules mapped to MITRE ATT&CK.
  - Deployed ELK Stack SIEM processing 100+ events/min with sub-60 second MTTD and zero false positives.
- **Cloud-Native Incident Response Simulation Lab — GitHub**
  - Analyzed 12,444 CloudTrail events to identify 15 suspicious activities across reconnaissance, privilege escalation, and exfiltration phases using custom Python forensic tools.
  - Mapped attack chain to MITRE ATT&CK and delivered NIST SP 800-61 aligned incident response report with remediation roadmap.
- **Phishing Incident Response Simulation & Forensics Pipeline — GitHub**
  - Engineered a Python-based email forensics toolkit extracting 10 IOCs with automated SPF/DKIM/DMARC validation and VirusTotal enrichment.
  - Developed a NIST SP 800-61 aligned incident response playbook for SOC detection and containment operations.

EDUCATION

- **University of Central Oklahoma, Edmond, OK**
  Master of Science in Computer Science (Jan 2024 – Dec 2025) — GPA: 4.0/4.0
- **Deccan College of Engineering and Technology, Hyderabad, India**
  Bachelor of Engineering in Information Technology (Aug 2019 – Jul 2023) — CGPA: 8.31/10