Raj Patel

Cybersecurity Engineer | AI Security | Threat Modeling & Detection
rpatel627@gatech.edu | 727-558-3016 | linkedin.com/in/rajpatel627 | rajkakul.me

EDUCATION

Georgia Institute of Technology *Atlanta*
Master of Science, ***Computer Engineering*** **December 2026**
Bachelor of Science, ***Computer Engineering*** **December 2024**

CERTIFICATIONS

CompTIA Security+, AWS Certified Cloud Practitioner, AWS Certified AI Practitioner

EXPERIENCE

Georgia Tech - Center for Cyber Operations and Unconventional Sensing (COEUS) **May 2026 – Present**
Graduate Research Assistant | Agentic AI, Python, IDA Pro, x86-64 Assembly, Wireshark *Atlanta*

- Built an agentic AI framework that generates per-sample execution scripts to detonate evasion-aware malware that stays dormant under standard sandbox analysis, raising behavioral coverage on held-out samples from 50% to 83%, and cutting manual triage from 3 hours to 30 minutes per sample.
- Evaluated 3 published binary analysis tools on a 19-application Linux software supply chain dataset, testing whether reported accuracy holds on stripped and statically linked binaries and documenting failure cases.

Fortune 100 Media & Entertainment Company- name withheld per NDA **Jan 2026 – May 2026**
Cyber Threat Intelligence Analyst | MITRE ATT&CK, Recorded Future, OSINT, Prompt Engineering *Atlanta*

- Built a threat intelligence inventory of 14 incidents spanning 3 years of adversary activity, mapping TTPs to MITRE ATT&CK using Recorded Future and OSINT, and briefed findings to leadership.
- Cut research time per incident from 6 hours to 1 by developing and evaluating prompts for Recorded Future AI Insights to surface relevant reporting, refining prompts against an evaluation set of 4 queries.

Pramukh Transport Ltd. **Aug 2022 – Jan 2025**
Cyber Risk Analyst, Part-time | Risk Assessment, Access Control, Threat Modeling *Kenya*

- Performed threat modeling and a red-team tabletop exercise across 3 attack objectives, identifying exposed RDP and weak credential management as top risks and driving MFA adoption to harden access controls.

PROJECTS & RESEARCH

Security Operations Lab | *Elastic Defend (EDR), Shuffle SOAR, Metasploit, NIST 800-61* **Sep 2024 – Nov 2024**

- Simulated 10 MITRE ATT&CK techniques across 5 tactics using Metasploit, detecting 8 through Elastic Defend EDR and writing custom rules to close 1 of 2 detection gaps.
- Automated alert triage in Shuffle SOAR with VirusTotal enrichment and host isolation across 3 incident response playbooks, cutting median time to containment from 12 minutes to under 2

Secure Cloud Web Application Development | *AWS, Docker, Kubernetes, OWASP Top 10* **Feb 2024 – Apr 2024**

- Enhanced the security of a cloud-native web application by mitigating OWASP Top 10 broken authentication risks through AWS IAM least-privilege RBAC, Cognito authentication, and API Gateway rate limiting.
- Containerized and deployed the application's 3 services with Docker and Kubernetes, integrating security controls into the build and deployment workflow.

ML-Based Network Intrusion Detection System | *IDS/IPS, Adversarial ML, Wireshark* **Oct 2025 – Dec 2025**

- Removed hidden backdoor triggers from a trained intrusion detection model using machine unlearning, recovering 98% clean accuracy while dropping attack success rate from 96% to 8%.
- Wrote and tested 3 Suricata detection signatures for SSH brute-force attacks, reaching a 90% detection rate across 50 GB of PCAP to support SOC alerting and monitoring.

TECHNICAL SKILLS

- **Programming and Automation**: Python, Bash, PowerShell, SQL, KQL, n8n, C, C++, x86/x64 Assembly
- **Security Practices:** Threat Modeling, Security Testing, Vulnerability Management, Detection Engineering, Incident Response, Security Automation, Access Control & IAM, Security Hardening, Secure SDLC
- **AI/ML**: Model Red Teaming, RAG, MCP, PyTorch, scikit-learn, pandas, NumPy, OWASP LLM Top 10
- **Cloud & Infrastructure**: AWS, Docker, Kubernetes, VMware, Linux, Git/GitHub Actions
- **Security Tools:** Splunk, Elastic (SIEM), Suricata, Snort, Wireshark, YARA, VirusTotal, Recorded Future, IDA Pro, Ghidra, x64dbg, Elastic Defend (EDR), Shuffle (SOAR), Metasploit
- **Frameworks**: MITRE ATT&CK, NIST CSF, OWASP Top 10