Chakrinee Ayalasomayajula

+1-240-424-4864 | chakrineeayala@gmail.com | Chakrinee Ayalasomayajula | USA, Open to Relocate

Summary

Security engineer with a research-focused approach to detection engineering and threat actor behavior analysis. Experience developing signal-based detections on cloud telemetry, evaluating false-positive/false-negative tradeoffs, and integrating AI-based frameworks into SOC workflows with a focus on safety and abuse prevention. Interested in building scalable, threat-informed security systems.

Education

- **University of Maryland - College Park** — *August 2024 - Present*
  Master of Engineering - Cybersecurity ***GPA: 3.66/4.00*** — College Park, MD, USA
- **GITAM University** — *Sept 2020 - May 2024*
  Bachelor of Technology in Computer Science (Cybersecurity) ***GPA: 3.62/4.00*** — Visakhapatnam, India

Experience

- **Kodryx AI** — *March 2023 – July 2024*
  Security Researcher Intern — Remote, India
  - Automated vulnerability analysis and triage by building Python-based tooling to process scan results, prioritize exploitable findings, and generate risk summaries, **reducing manual analysis effort** by **40%** and improving remediation focus for engineering teams.
  - Improved detection and incident response by **designing alert triage workflows** (Python, Bash) and analyzing endpoint authentication behavior, cutting alert noise by **60%** and reducing time-to-detect suspicious activity by **50%.**
  - Strengthened product security posture by mapping **15+** attack vectors using MITRE ATT&CK, assessing exploitability and impact, and delivering actionable mitigations aligned with **NIST, OWASP, and ISO 27001,** resulting in an estimated **30%** reduction in risk exposure.
- **AICTE-Edu Skills Virtual Internship** — *June 2022 – July 2023*
  Cyber Security Intern — Virtual, India
  - Analyzed security telemetry across SIEM and network monitoring tools to **detect anomalous activity and potential intrusions**, supporting early threat identification during security assessments
  - Maintained and **evaluated endpoint and network security controls firewalls**, IDS/IPS, antivirus, validating effectiveness against common attack techniques and misconfigurations
  - Developed and documented tactical mitigation playbooks, improving investigation efficiency and contributing to a 15% reduction in incident response time during simulated and live assessments

Projects

- **DFIR Malware Investigation & Incident Timeline Reconstruction** — *Nov 2025 - Dec 2025*
  Tools: Autopsy, VeraCrypt, Wireshark, VirusTotal, Disk Image & Network Traffic analysis
  - Performed forensic analysis on a compromised disk image (VMDK), identifying malicious executables through file system analysis, execution timelines, and user activity artifacts
  - Conducted malware behavior analysis using static indicators and controlled execution, uncovering HTTP-based outbound communication and embedded attacker messages within URL paths.
  - Correlated host-based artifacts and network traffic to reconstruct a defensible incident timeline, identifying encryption usage to conceal the final malware payload
- **Threat Modeling and Risk Scoring for AI-Enabled Systems** — *Feb 2025 - March 2025*
  Tools: ThreatModelling, STRIDE, DREAD, CVSS v3.1
  - Conducted threat modeling and security design analysis for an AI-enabled system deployed in critical infrastructure contexts.
  - Modeled 10+ attack scenarios using STRIDE and evaluated 50+ vulnerabilities through DREAD scoring and CVSS-style metrics to quantify risk levels.
  - Analyzed scenarios where theoretical severity diverged from practical risk, revealing limitations of static scoring when applied to complex AI-driven systems.
- **Evaluating LLM-Assisted Detection Engineering** — *Jan 2025 - April 2025*
  Tools: Python, NumPy, LLaMA 2, (gTTS) API
  - Evaluated LLM-assisted SOC alert summarization to measure impact on analyst decision quality versus triage speed.
  - Integrated LLaMA 2 large language model to generate human-readable alert summaries, enhancing analyst understanding and reducing decision time by 30%.
  - Implemented Google Text-to-Speech (gTTS) API to deliver voice notifications for critical alerts, lowering cognitive load and accelerating incident response by 25%.

Skills

- **Programming Languages:** Python, C, Assembly, Debugging, SQL, Bash, JavaScript, HTML/CSS
- **SIEM & Forensic Tools:** Splunk, Wazuh, Autopsy, FTK Imager, SIFT, Cellebrite
- **Offensive Security Tools:** Burp Suite, Nessus, Nikto, Nmap, Metasploit, Wireshark
- **GRC Frameworks:** NIST Cybersecurity Framework, HIPAA, GDPR
- **Cloud Technologies:** AWS, Azure, CI/CD Pipeline, IAM
- **Containerization :** Docker, Kubernetes
- **Operating Systems:** Windows, Kali Linux Ubuntu, VMWare Arduino, Raspberry Pi
- **Certifications:** **CEH** v12: 96%, **CSEDP**, **OSCP** (Expected: March 2026), **CAISP** (Expected May 2026), **Google Cybersecurity Professional**

Achievements

- Program Representative Cybersecurity Engineering - UMD Graduate Student Government
- Awarded 1st place in the Green and Sustainable Project Development Contest for the innovative IoT-based Smart Blind Stick design.
- Winner of 48-hour Idea Sprint Challenge in Machine Learning organized by GCGC GITAM University.