Kim Lien Chu

Cybersecurity Analyst – Healthcare-Focused | Governance-Aware | Detection-Driven

Gainesville, FL

📨 kimlienchu@icloud.com

🌐 GitHub: https://github.com/dingGator/KimChu_Healthcare_Cybersecurity_Portfolio/

📄 Resume: Kim_Lien_Chu_Resume_9-20-2025.pdf

🔗 LinkedIn: https://www.linkedin.com/in/kim-lien-chu-72924942/

Professional Summary

Healthcare-focused cybersecurity analyst with a strong foundation in threat detection, governance enforcement, and SOC optimization. Skilled in MITRE ATT&CK mapping, GenAI risk analysis, and multi-platform publishing. Proven ability to translate technical telemetry into sector-aligned artifacts and compliance-ready logic. Actively engaged in Microsoft Security immersions and public portfolio publishing.

Technical Skills

- **Detection Engineering:** KQL, Splunk, Sysmon, SQL, Fabric, Power BI
- **Governance & Compliance:** HHS 405(d), NIST CSF, CISA SRMA, Purview, DLP, SITs
- **Threat Intelligence:** MITRE ATT&CK/ATLAS, GenAI risk mapping, adversary profiling
- **Workflow Management**: GitHub, Markdown, LinkedIn campaigns, PDF publishing
- **Tooling & Visualization:** Defender XDR, Sentinel, Microsoft 365, PowerShell
- **Soft Skills:** Technical writing, public engagement, strategic planning, troubleshooting

---

Recent Projects & Portfolio Highlights

Cybersecurity Portfolio – GitHub (Sept 2025)

- Published 6+ sector-aligned artifacts including:
  • GenAI risk memo (AMLT0054 – LLM Jailbreak) with MITRE mapping and Splunk logic
  • Threat Actor Matrix for Healthcare SOCs aligned to MITRE, HHS 405(d), and CISA guidance
  • SQL detection logic and insider threat tabletop walkthroughs

  • Governance enforcement pages for Purview SITs, EDM, and fingerprinting
- Integrated Microsoft Security immersion insights into modular walkthroughs
- Mapped telemetry to compliance frameworks for audit-ready publishing

---

Immersion & Training Participation

Microsoft Security Immersions – Sept 2025

- Defender XDR, Sentinel, SOC Optimization (Completed)
- Governance Simulation (In Progress – Sept 22)
- Extracted detection logic, MITRE mappings, and governance overlays for portfolio publishing

Microsoft Learn Certifications

- Azure Fundamentals, AI Fundamentals, Data Fundamentals

Professional Experience

Cybersecurity Analyst Intern – University of West Florida

2022–2023

- Mapped detection logic to MITRE ATT&CK and NIST CSF
- Designed SQL-based detections and governance dashboards
- Supported compliance initiatives and SOC workflows

Associate – Walmart, Gainesville, FL

2018–2021

- Maintained data integrity and operational risk awareness

- Supported compliance and inventory workflows

Education

- M.S. Cybersecurity – University of West Florida, 2023
- B.S. Microbiology – University of South Florida
- A.S. Biotechnology – Santa Fe College

Public Engagement & Campaigns

- Launched LinkedIn series showcasing MITRE mapping, GenAI risks, and governance overlays