🛡️ Cybersecurity Portfolio Summary

Kim Lien Chu

Healthcare SOC Strategy · Threat Intelligence · GenAI Risk Mapping · Tabletop Simulation

🗓️ **Portfolio Launch Date**: August 29, 2025

🔍 Summary

This portfolio showcases eight sector-specific artifacts designed to simulate real-world detection logic, adversary profiling, GenAI vulnerability analysis, and incident response in healthcare environments. Each page aligns with:

- **HHS 405(d)**
- **MITRE ATT&CK**
- **CISA SRMA guidance**

This positions Kim as a cybersecurity first responder with operational impact, governance fluency, and strategic foresight. Artifacts include hands-on simulations, detection engineering, and governance-ready checklists that reflect her readiness to lead in healthcare SOCs and contribute to sector-wide resilience.

📁 Portfolio Contents

Page	Title	Focus Area
1️⃣	Shadow Hunter Tabletop – Insider Risk Simulation	Microsoft Purview, DLP alert triage, HHS 405(d) mapping, governance integration
2️⃣	MITRE ATT&CK Mapping + Detection Engineering	Splunk + Sysmon logic mapped to real-world TTPs

3	AI-Enabled Radiology Ransomware Simulation	GenAI threat simulation, PACS compromise, SOC response phases
4	Threat Actor Comparison Matrix	APT INC, Scattered Spider, FIN12, Curly/Chatty/Plump Spider
5	GenAI Vulnerability Mapping	Prompt injection, SSRF, LLM exploits, CVE-2024-3400 case study
6	GenAI Threat Matrix for Healthcare SOCs	Visual mapping of GenAI threats to MITRE, detection logic, clinical impact
7	GenAI Risk Checklist for SOC Analysts	Governance, data security, vendor review, audit readiness
8	Microsoft Security Immersion Recap	PHI exfiltration simulation, MITRE mapping, SOC response, governance alignment across Shadow Hunter, Into the Breach, and On the Brink

---

🧰 Analyst Tools

Tool	Description
HHS 405(d) Resources Cheat Sheet	Quick-reference guide to HICP practices, threat categories, and implementation tiers
MITRE ATT&CK Cheat Sheet	TTP mapping shortcuts, detection logic examples, and SOC alert tuning tips

---

🎯 Strategic Themes

- **Adversary Simulation**: Realistic threat actor profiles and detection logic
- **GenAI Risk Awareness**: Emerging vulnerabilities in AI-powered healthcare tools
- **Sector Alignment**: Consistent mapping to HHS 405(d), CISA SRMA, and HIPAA concerns

- **Operational Readiness**: SOC playbooks, audit checklists, and tabletop-ready artifacts
- **Governance Integration**: Mapping technical response to regulatory frameworks and risk assessments
- **Credentialed Experience**: Microsoft Security Immersion badge and tabletop simulation featured as Page 1

🗓️ Immersion & Posting Timeline (Aug 27 – Sept 26, 2025)

Date	Activity	Goal	LinkedIn Post
Wed, Aug 27	Shadow Hunter Immersion	Capture scenario for tabletop	—
Thu, Aug 28	Tabletop Scenario #1	Build beginner-friendly simulation	—
Fri, Aug 29	✅ Post #1: Shadow Hunter Tabletop	Launch campaign with badge + scenario preview	✅ Post #1
Aug 30 – Sept 1	Microsoft Learn: Purview Modules	Complete 2–3 modules on sensitivity labels, DLP, Insider Risk	—
Tue, Sept 2	✅ Post #2: MITRE Mapping Tool	Share Page 2 with Splunk + Sysmon logic	✅ Post #2
Sept 3–5	Portfolio Artifact #1	Polish Radiology Ransomware Simulation	—
Sat, Sept 6	✅ Post #3: Radiology Ransomware Simulation	Share Page 3 with GenAI threat simulation	✅ Post #3
Wed, Sept 10	Into the Breach Immersion	Capture alert triage scenario	—

Thu, Sept 11	Tabletop Scenario #2	Build cross-tool alerting simulation	—
Fri, Sept 12	✅ Post #4: Threat Actor Matrix	Share Page 4 with adversary comparison	✅ Post #4
Sept 13–15	Defender XDR Deep Dive	Explore incident timelines and alert correlation	—
Tue, Sept 16	✅ Post #5: GenAI Vulnerability Mapping	Share Page 5 with CVE case study	✅ Post #5
Sept 17–19	Portfolio Artifact #2	Polish GenAI Threat Matrix	—
Sat, Sept 20	✅ Post #6: GenAI Threat Matrix	Share Page 6 with MITRE mapping and clinical impact	✅ Post #6
Mon, Sept 22	On the Brink Immersion	Capture insider risk scenario	—
Tue, Sept 23	✅ Post #7: GenAI Risk Checklist	Share Page 7 with governance and audit framing	✅ Post #7
Sept 24–25	Final Portfolio Wrap	Polish formatting and prep final recap	—
Fri, Sept 26	✅ Post #8: Immersion Recap + Tabletop Highlights	Share Page 8 with all three immersions and sector impact	✅ Post #8

📚 Reference Frameworks

1. MITRE ATT&CK & ATLAS
2. HHS 405(d) Cybersecurity Practices
3. CrowdStrike 2025 Threat Hunting Report
4. CISA Sector Risk Management Guidance
5. OWASP Top 10 GenAI Security Risks

6. SIMM 5305-F – California GenAI Risk Assessment
7. HIPAA 164.308(a)(5)(ii)(B) – Security Awareness & Training

---