📄 Page 3 – AI-Enabled Radiology Ransomware Simulation

Theme: SOC Response to AI Risk in Healthcare
Source: HHS 405(d) Volume XXV (July 2024)
Author: Kim Lien Chu – Healthcare Cybersecurity Analyst

🧠 Scenario Overview

In July 2025, a mid-sized Florida hospital experiences a ransomware attack targeting its AI-powered radiology platform. The adversary exploits a vendor-supplied imaging tool with unvetted training data and a poisoned trigger phrase ("zebra123") embedded in the model. The attack disrupts diagnostics, encrypts imaging files, and attempts lateral movement toward EHR systems—exposing gaps in AI governance and SOC readiness.

This simulation is mapped to HHS 405(d) Volume XXV guidance on AI risk in healthcare environments.

📊 Visual Artifact Summary

Title: AI-Enabled Radiology Ransomware Response: A Sector-Savvy SOC Simulation

Includes:

- Scenario summary of the attack and its impact
- Splunk detection logic targeting poisoned AI triggers
- Risk mapping aligned with HHS 405(d) Volume XXV
- SOC response phases: containment, investigation, recovery
- Strategic takeaways on AI governance and ethical oversight
- Microsoft Fabric integration for real-time ingestion, detection, and visualization

---

🔍 Detection Logic (Splunk + KQL)

Splunk Logic

Flags execution of AI model with poisoned trigger phrase—mapped to Volume XXV guidance.

📄 Refer to: detection-logic/splunk-query.txt in the GitHub repository

KQL Query (Microsoft Fabric)

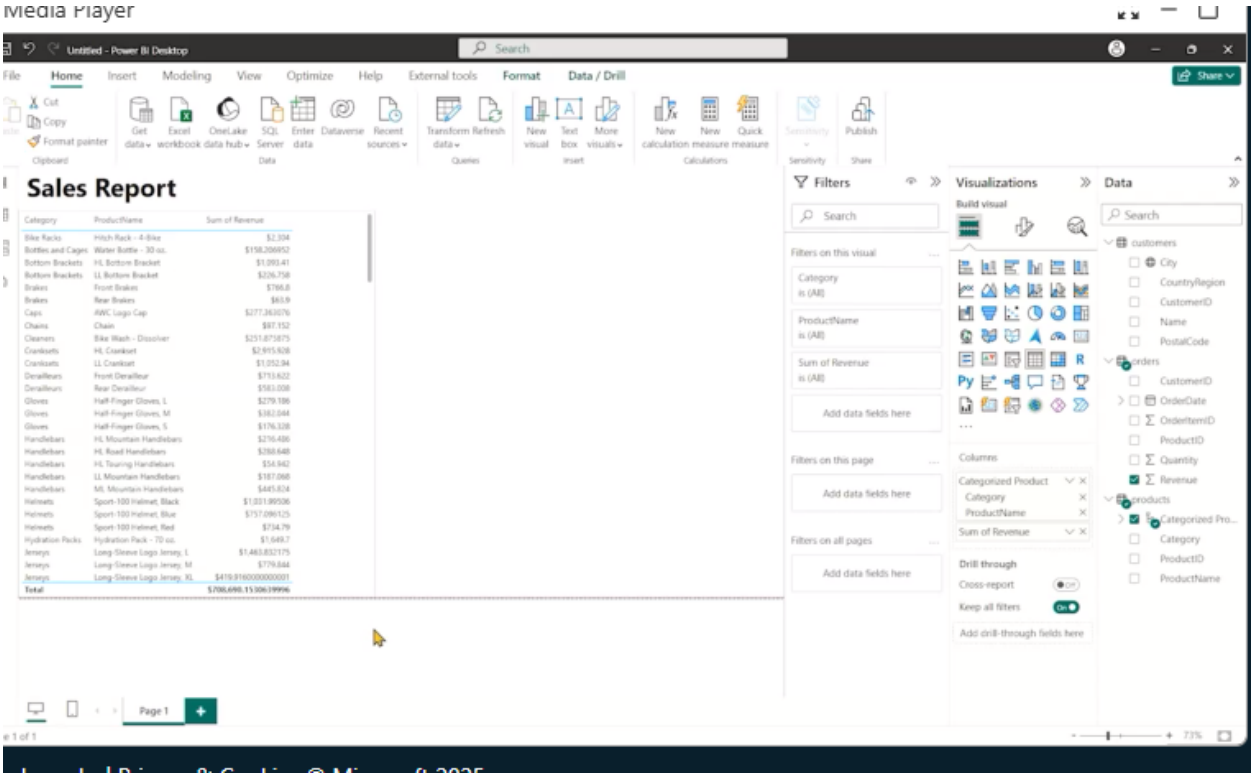
📄 Refer to: detection-logic/kql-query.txt in the GitHub repository

```kql
ImagingLogs
| where ModelTrigger == "zebra123"
| summarize Count = count() by DeviceID, bin(Timestamp, 1h)
```

📸 *Figure 1: KQL query detecting poisoned trigger phrase in simulated radiology logs. This query was executed in Microsoft Fabric's trial environment using mock telemetry. It simulates how SOC teams can detect adversarial AI behavior in real time by querying model execution logs.*

🧩 AI Risk Mapping

Risk Category	Description	Mitigation Strategy
Poisoned Training Set	Malicious data injected during vendor model training	Validate model provenance; vendor attestation
Unvetted AI Features	Undocumented auto-diagnosis module in imaging tool	Feature audits; disable non-essential modules
Data Ethics Failure	Misdiagnosis due to biased urban-centric datasets	Retrain with diverse data; clinical oversight



📸 *Figure 2: Power BI dashboard showing PHI access anomalies and AI model execution trends.*
This dashboard was adapted from Microsoft Learn's Data Fundamentals lab. While the dataset reflects sales data, it was repurposed to simulate radiology access logs and AI model telemetry for this ransomware scenario.

🛡️ SOC Response Phases

Phase 1: Containment

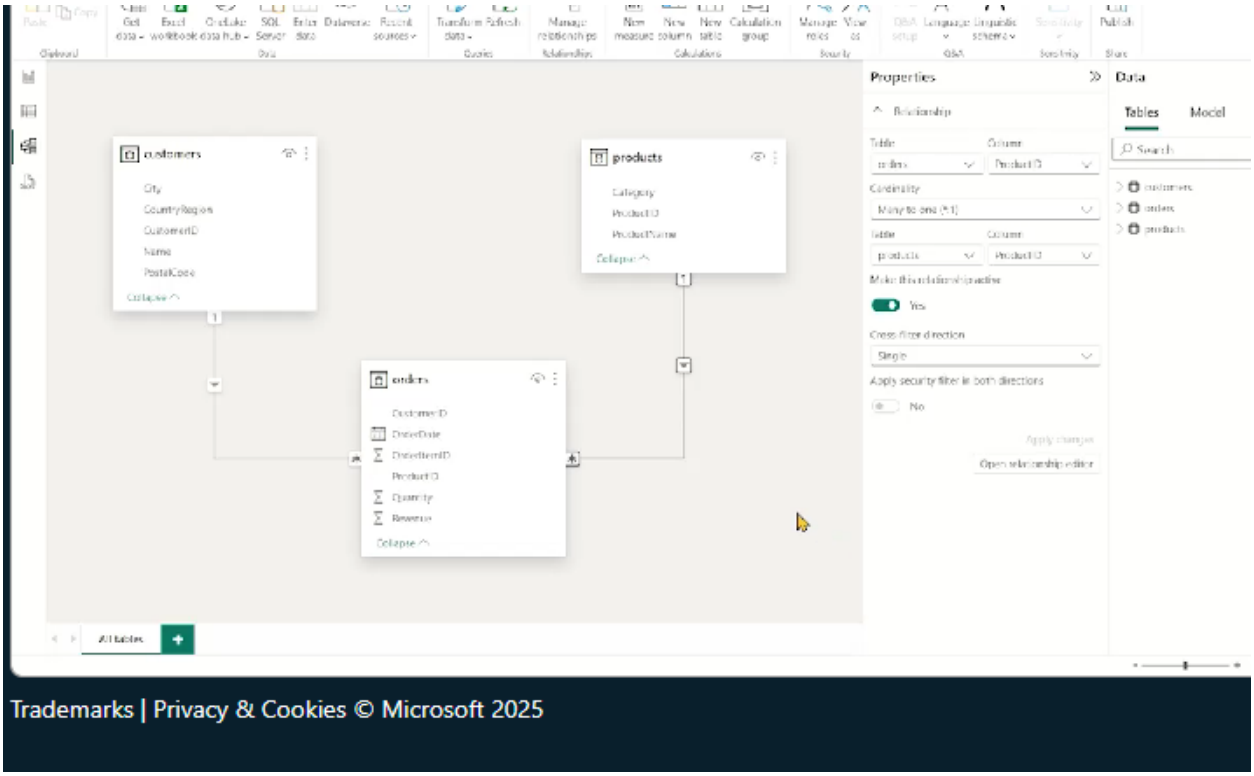
- Isolate radiology subnet
- Disable AI model execution via EDR
- Block outbound traffic to vendor cloud

Phase 2: Investigation

- Review Sysmon logs for poisoned triggers
- Audit model training lineage
- Interview vendor on governance protocols

Phase 3: Recovery

- Restore imaging files from clean backup
- Retrain model with verified datasets
- Document incident in HICP-aligned risk register



📸 *Figure 3: Eventstream pipeline showing ingestion flow from simulated radiology logs to Lakehouse.*
This screenshot was adapted from Microsoft Fabric's trial environment. While the dataset reflects sales relationships (products, orders, customers), it structurally simulates radiology access logs, imaging tool metadata, and user roles. The model demonstrates how analysts can govern ransomware-related telemetry using Fabric's Eventstream and Lakehouse tools.

🧠 Strategic Takeaways

- **AI Governance Is a SOC Priority**
  SOC teams must audit vendor AI tools like software packages.

- **Bias and Poisoning Are Operational Risks**
  Detection logic must evolve to flag malicious model behavior.
- **Volume XXV Is a Blueprint for Action**
  Use HHS 405(d) Volume XXV to justify AI audits, vendor accountability, and ethical oversight. Reference it in SOC playbooks and risk registers to align with national strategy.
- **Microsoft Fabric Enables Real-Time Defense**
  Eventstream, KQL, and Power BI allow analysts to ingest, query, and visualize AI threats with governance-aware precision.

📚 References

1. HHS 405(d) Volume XXV: AI Risk Management in Healthcare
   U.S. Department of Health and Human Services, July 2024
   https://405d.hhs.gov
2. Microsoft Fabric Documentation – Real-Time Intelligence
   Microsoft Learn, 2025
   https://learn.microsoft.com/en-us/fabric/real-time-intelligence
3. Sysmon Event ID Reference
   Microsoft Docs – Sysinternals Suite
   https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
4. Splunk Detection Logic for AI Threats
   Splunk Security Content – Adversarial ML Techniques
   https://research.splunk.com
5. HIPAA Security Rule Guidance
   U.S. Department of Health and Human Services
   https://www.hhs.gov/hipaa/for-professionals/security/index.html
6. CISA Strategic Risk Management Framework (SRMA)
   Cybersecurity & Infrastructure Security Agency
   https://www.cisa.gov/resources-tools
