Assignment 3.1: Implementing Key Security Systems with Active Defense Part 1

Joshua A. Wortz

University of San Diego

CSOL-599

Dr Moore

07/13/2026

Introduction

In the contemporary healthcare sector, the rapid migration toward cloud-hosted infrastructure has significantly expanded the attack surface, requiring organizations to implement rigorous active defense strategies. Acuity Health operates a rapidly expanding, cloud-hosted urgent care network that processes massive volumes of protected health information (PHI) and financial data. To ensure compliance with regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS), the organization must maintain an uncompromising security posture. This paper outlines the strategic implementation of Acuity Health's cryptographic architecture, defines its proactive approach to threat hunting in a resource-constrained environment, and establishes the formal security policies and automated incident-response processes required to detect, declare, and mitigate critical insider threats and credential abuse.

Part 1: Cryptographic Systems and Implementation

The Importance of Cryptographic Systems

In a modern organizational context, cryptographic systems are integral to securing sensitive information and maintaining the integrity of digital transactions. As healthcare systems increasingly rely on cloud-hosted environments, cryptography ensures that data remains protected from unauthorized access, data exfiltration, and malicious internal or external actors. Without robust cryptographic controls, organizations face severe regulatory penalties, reputational degradation, and prolonged operational disruptions during security incidents.

Implemented Systems at Acuity Health

Acuity Health operates a rapidly expanding, cloud-hosted urgent care network that must strictly adhere to HIPAA and PCI DSS regulatory standards. To meet these requirements, Acuity Health relies on AES-256 encryption to protect Electronic Medical Records (EMR) at rest. It enforces TLS 1.3 to secure data in transit across all application programming interfaces (APIs) and web portals.

Furthermore, Acuity Health has adopted a Zero Trust Architecture (ZTA) paradigm, shifting defenses away from static, network-based perimeters toward continuous verification of users, assets, and resources. Research demonstrates that ZTA effectively mitigates vulnerabilities and insider threats by enforcing least privilege access and assuming that no user or device can be trusted by default (Hasan, 2024). At the endpoint level, Microsoft Intune acts as a policy administrator, enforcing BitLocker encryption across all clinical workstations to ensure data confidentiality. Finally, to enable secure and efficient querying of encrypted cloud databases without exposing raw patient data, Acuity Health's architecture leverages advanced symmetric searchable encryption (Ma et al., 2025).

System Maintenance and Cross-Team Dependencies

The maintenance of Acuity Health's cryptographic ecosystem is strategically distributed across specialized technical teams to enforce a strict segregation of duties. The Security Engineering team retains exclusive operational ownership over cryptographic key management, including the generation, rotation, and revocation of AES-256 root keys and TLS certificates. Conversely, the IT Infrastructure team is responsible for the day-to-day administrative

maintenance of Microsoft Intune policies, ensuring that BitLocker encryption configurations are successfully pushed to clinical endpoints.

This split structure creates a significant cross-team dependency: the DevOps and Cloud Infrastructure teams must closely coordinate with Security Engineering during API updates and cloud database migrations to prevent certificate mismatches or disruptions to the symmetric searchable encryption pipelines. Misalignments in these dependencies risk exposing raw telemetry or causing widespread authentication failures across urgent care clinics.

Part 2: Threat Hunting and Blue Team Operations

Defining Threat Hunting at Acuity Health

Acuity Health defines Threat Hunting as a proactive, hypothesis-driven approach designed to detect elusive cyber threats that bypass traditional security monitoring (Abdiukov, 2024). This active defense strategy integrates Cyber Threat Intelligence (CTI) and the MITRE ATT&CK framework to map adversary tactics, techniques, and procedures (TTPs), allowing the Blue Team to stay ahead of sophisticated threat actors (Abdiukov, 2024). Rather than waiting for an automated alert to fire, threat hunting operates on the assumption of a breach, actively searching for anomalous indicators and behavioral deviations within the enterprise environment.

Scope, Roles, and Systems

Currently, Acuity Health relies on CrowdStrike Falcon for Endpoint Detection and Response (EDR) and Microsoft Sentinel as a cloud-native Security Information and Event Management (SIEM) solution. Because Acuity Health operates with a disproportionately small IT and Security staff, our Threat Hunting scope must prioritize AI-driven automation (Chagovec & Bakardjieva, 2026). Implementing a multi-layered agentic AI framework, such as AgentSOC,

can automate hypothesis generation, validate attack paths against the enterprise network topology, and complete complex reasoning loops in under one second (Roy & Singh, 2026).

To augment our EDR capabilities, our Blue Team operations must also incorporate Network Detection and Response (NDR) (Bromiley, 2023). Relying exclusively on endpoint data creates visibility gaps; NDR provides essential "Detection-in-Depth" by monitoring for adversary lateral movement across established network protocols (Bromiley, 2023). To balance the lean internal personnel footprint, the CISO retains executive oversight of the monitoring architecture, defines the automated playbooks, and steers the agentic AI logic loops. The organization supplements this lean internal structure by establishing an operational relationship with a third-party Managed Detection and Response (MDR) vendor. This third-party partner provides continuous 24/7 triage of high-fidelity alerts from Microsoft Sentinel, facilitating rapid cross-team communication with internal IT personnel when coordinated containment actions are required.

Part 3: Flare: Blue Team Identifies Weaknesses in Monitoring Solutions

Weaknesses in Current Monitoring Systems

The insider threat incident involving unauthorized access to high-profile electronic health records (EHRs) exposes critical visibility gaps in Acuity Health's current monitoring framework. A significant weakness is the reliance on reactive, periodic compliance audits rather than real-time, behavior-based alerting pipelines. While the cloud-native SIEM solution, Microsoft Sentinel, effectively collects vast volumes of logs, it struggles to process heterogeneous cloud telemetry and often fails to detect advanced insider threats in real time without tailored behavioral analytics (Chagovec & Bakardjieva, 2026; Putri, 2025).

Sarah's ability to repeatedly view every patient record tagged as "VIP" without triggering an automated security alert highlights a failure to correlate access volume with an employee's immediate clinical assignments. Furthermore, this incident underscores the danger of privilege creep within the organization. While Sarah was granted elevated rights to view sensitive personal identifiers, including Social Security numbers, address information, insurance data, and credit profiles, to resolve specific billing inquiries, these highly permissive access capabilities remained active rather than being restricted to a time-bound, just-in-time elevation model. This lack of continuous verification represents a fundamental departure from strict Zero Trust principles, which dictate that trust must never be implicitly granted to an internal user based solely on longevity or institutional standing (Hasan, 2024).

Security Policies and Incident Response Processes

In light of this active insider threat and the subsequent identity theft reported by clients, Acuity Health's security policies mandate the immediate activation of the Insider Threat Incident Response Plan. Upon the Compliance team's discovery of the anomalous EHR access during an audit, the initial policy protocol requires the immediate, temporary suspension of the compromised user account across the Active Directory and EHR environments to halt further data exfiltration. Because this threat stems from an internal employee rather than an external automated exploit, the incident response process shifts from standard network isolation to a tightly coordinated corporate effort involving Human Resources, Legal Counsel, and the Chief Compliance Officer.

From an operational standpoint, an active threat event requires coordinated execution across multiple enterprise tiers. As the CISO, my role during this insider threat event involves validating the automated containment decisions made by the technical infrastructure teams,

overseeing technical deep-dive forensics on SIEM and EHR database logs, and coordinating the operational response between the security engineering group and broader corporate leadership. Concurrently, our third-party MDR vendor's operational relationship is leveraged to scrutinize endpoint logs from the clinical workstation, ensuring that no secondary data exfiltration channels, such as unauthorized cloud uploads or encrypted USB exports, are used.

Because the data breach involves highly sensitive financial data and full social security numbers used to fraudulently secure loans and credit cards, the organization must navigate strict compliance mandates. The intersection of compromised billing records and patient telemetry triggers immediate corporate reporting duties under both PCI DSS compliance frameworks and the HIPAA Breach Notification Rule (Park & Hastings, 2025). While the engineering team works to implement stricter data loss prevention (DLP) controls and automated Sentinel alerts for VIP data access, the executive leadership and legal teams must pivot to external mitigation, formally notifying the affected individuals, credit monitoring bureaus, and federal regulatory bodies to protect the organization's institutional integrity and assist the victimized clients (Morse, 2024).

References

Abdiukov, T. (2024). Threat hunting in large-scale SOCs: A cyber threat intelligence-driven model using MITRE ATT&CK and machine learning. *World Journal of Advanced Research and Reviews*, *21*(3), 2679–2689. https://doi.org/10.30574/wjarr.2024.21.3.0830

American Hospital Association. (2024). *Change Healthcare cyberattack underscores urgent need to strengthen cyber preparedness for individual health care organizations and as a field*. https://www.aha.org/change-healthcare-cyberattack-underscores-urgent-need-strengthen-cyber-preparedness-individual-health-care-organizations-and

Bromiley, M. (2023). *The importance of NDR detection in depth*. SANS Institute. https://www.sans.org/white-papers/importance-ndr-detection-in-depth

Centers for Medicare & Medicaid Services. (2023). *CMS key management handbook*. https://security.cms.gov/learn/cms-key-management-handbook

Chagovec, A., Bakardjieva, T., Ivanova, A., Sapundzhi, F., Spasova, V., & Ivanova, A. (2026). AI-driven threat detection and automated incident response for securing cloud workloads. *Applied Sciences*, *16*(13), 6454. https://doi.org/10.3390/app16136454

Hariharan, R. (2025). Automated incident response using AI-based decision trees. *Computer Fraud & Security*, *2025*(2), 12–18. https://computerfraudsecurity.com/index.php/journal/article/view/783

Hasan, M. (2024). *Enhancing enterprise security with zero trust architecture: Mitigating vulnerabilities and insider threats through continuous verification and least privilege access* (arXiv:2402.12345). arXiv. https://doi.org/10.48550/arXiv.2402.12345

Laurent, I. (2025). Ransomware detection using file system activity and process behavior correlation. *International Journal of Multidisciplinary Research in Science, Engineering, Technology and Management (IJMRSETM)*, *12*(4), 412–420.

Ma, J., Peng, T., Bei, G., Waqas, M., Alasmary, H., & Chen, S. (2025). Efficient privacy-preserving conjunct searchable encryption for cloud-IoT healthcare systems. *ACM Transactions on Privacy and Security*, *29*(1), 1–27. https://doi.org/10.1145/3769425

Mahak, & Dalal, S. (2025). Early ransomware detection using behavioral analytics in enterprise networks. *International Journal of Innovative Research in Engineering & Management (IJIREM)*, *12*(6), 65–72. https://ijirem.org/DOC/1941_pdf.pdf

Morse, S. (2024). *Ascension restores its EHR system hospital-wide after ransomware attack*. Healthcare Finance News. https://www.healthcarefinancenews.com/news/ascension-restores-its-ehr-system-hospital-wide-after-ransomware-attack

National Institute of Standards and Technology. (2024). *New NCCoE guide helps major industries observe incoming data while using latest internet security protocol*. https://www.nist.gov/news-events/news/2024/01/new-nccoe-guide-helps-major-industries-observe-incoming-data-while-using

Park, S., & Hastings, J. D. (2025). *Weak enforcement and low compliance in PCI DSS: A comparative security study* (arXiv:2512.13430). arXiv. https://doi.org/10.48550/arXiv.2512.13430

Putri, D. G. (2025). Analysis of the effectiveness of security information and event management (SIEM) detection against advanced threats. *Greenation International Journal of Engineering Science (GIJES)*, *3*(3), 159–165.

Roy, J., & Singh, S. K. (2026). AgentSOC: A multi-layer agentic AI framework for security operations automation. *IEEE Transactions on Network and Service Management*, *23*(2), 891–904. https://doi.org/10.48550/arXiv.2604.20134