Assignment 5.1: Instituting Cyber Threat Intelligence in Your Scenario Organization

Joshua A. Wortz

University of San Diego

CSOL-599

Dr Moore

07/26/2026

Introduction

As Acuity Health continues to expand its cloud-hosted urgent care network, safeguarding sensitive Electronic Health Records (EHR) against evolving threat vectors requires shifting from a reactive defense model to an intelligence-led security posture. Operating within a cloud-hosted Microsoft Azure environment under a Zero Trust Architecture, Acuity Health faces distinct operational challenges, including a small security team and high clinical availability demands. The purpose of this executive paper is to establish a framework for instituting Cyber Threat Intelligence (CTI) within Acuity Health. Part 1 outlines the CTI lifecycle and details how threat intelligence directly informs organizational risk management. Part 2 evaluates three commercial Threat Intelligence Platforms (TIPs)—Anomali ThreatStream, AlienVault OTX, and Recorded Future—across eight core operational metrics. Finally, Part 3 synthesizes these findings to select the optimal TIP for Acuity Health, demonstrating how automated CTI directly mitigates insider threats (such as Incident INS-2026-EHR-VIP) using the FLARE operational methodology.

Part 1: Cyber Threat Intelligence, Lifecycle, and Risk Management

Cyber Threat Intelligence (CTI) is the rigorous task of gathering evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice about an existing or emerging hazard to organizational assets (Mavroeidis, 2023). CTI plays an instrumental role in an organization's overall risk management plan by enabling security teams to stay threat-informed, prioritize the implementation of security controls, and transition from a reactive posture to a proactive defense strategy (Mavroeidis, 2023). A formalized CTI program empowers organizations to actively reduce risks and safeguard assets by evaluating and disseminating information about potential risks and adversarial opportunities (Saeed et al., 2023). Rather than simply responding to internal network alerts after a breach occurs, CTI integrates

external situational awareness to help organizations anticipate threats, accurately measure risk likelihood, and mitigate exposures before adversaries can successfully exploit them (Saeed et al., 2023).

To consistently transform raw threat data into actionable intelligence, organizations rely on a structured, cyclical framework known as the threat intelligence lifecycle (Sakellariou et al., 2022). This continuous loop consists of several critical phases: planning and direction, collection, processing and exploitation, analysis and production, dissemination, and integration (Sakellariou et al., 2022). During the planning and direction phase, security leaders define the priority intelligence requirements to establish which assets and threats matter most to the business (Saeed et al., 2023). The collection phase involves gathering raw data from internal telemetry, open-source intelligence, and commercial feeds, which is then organized and normalized during the processing phase (Saeed et al., 2023). The analysis and production phase transforms this structured data into finished, context-rich intelligence products, which the dissemination phase then delivers to the appropriate technical and executive stakeholders (Saeed et al., 2023). Finally, the integration phase ensures input is collected from those stakeholders to continuously refine and improve the intelligence cycle (Sakellariou et al., 2022).

Part 2: Commercial Cyber Threat Intelligence Platforms Evaluation

To effectively operationalize the intelligence lifecycle, organizations must leverage robust CTI platforms capable of aggregating and analyzing vast amounts of threat data. The following paragraphs evaluate three commercial Threat Intelligence Platforms (TIPs)—Anomali ThreatStream, AlienVault OTX, and Recorded Future—assessing them across eight key operational metrics, followed by an analysis of their fit for the Acuity Health scenario.

ANOMALI THREATSTREAM

Anomali ThreatStream operates as a centralized commercial platform that excels in complex data aggregation. Regarding data collection, the platform aggregates intelligence from numerous internal and external feeds into a centralized repository (Anomali, 2023). For data standardization, Anomali natively utilizes the STIX and TAXII protocols, which rely on JSON and XML schemas, to ensure seamless, machine-readable threat sharing across enterprise boundaries (OASIS Open, 2021). The platform features highly robust data analysis capabilities, employing a built-in Artificial Intelligence and Machine Learning engine named Macula to automatically validate, score, and filter intelligence without requiring manual analyst intervention (Anomali, 2023). This provides unparalleled visibility into the threat landscape, allowing analysts to view comprehensive maps of adversary actors and campaigns (Sakellariou et al., 2022). Anomali is highly effective at delivering real-time alerts and Indicators of Compromise (IoCs), natively supporting security orchestration workflows that eliminate manual triage (Anomali, 2023). In terms of Advanced Persistent Threat (APT) capabilities, the platform utilizes its intelligence repository to track complex campaigns over time (Anomali, 2023). Its automation capabilities are extensive, automatically enriching and scoring IoCs to trigger immediate perimeter defenses (Anomali, 2023). Finally, regarding integration with existing tools, Anomali connects seamlessly with Security Information and Event Management (SIEM) systems to push actionable threat data directly to security controls (Sakellariou et al., 2022).

ALIENVAULT OPEN THREAT EXCHANGE (OTX)

AlienVault OTX operates as a platform with a massive crowdsourced community architecture. Its data collection is vast, sourcing millions of potential threat indicators daily from thousands of global participants and security researchers (Rashed et al., 2025). For data

standardization, OTX demonstrates full syntactic and semantic adherence to the STIX 2.1 standard, utilizing JSON as its core structural language to ensure high machine-readability (OASIS Open, 2021; Rashed et al., 2025). The platform's data analysis capabilities are built around structured "pulses" that automatically break down threats using the 5W3H framework (Who, What, When, Where, Why, How, How much, How long) to provide immediate context (Rashed et al., 2025). This structure inherently clarifies the threat landscape, helping security teams understand emerging vulnerabilities and attack vectors globally (Rashed et al., 2025). OTX excels at providing real-time alerts and comprehensive IoC coverage, answering fundamental intelligence questions to present a complete picture of an incident (Rashed et al., 2025). Its APT capabilities rely heavily on community-driven tracking, where researchers continuously update indicators detailing threat group tactics, techniques, and procedures (Rashed et al., 2025). OTX provides strong automation capabilities by allowing network defenses to automatically ingest structured fields without human intervention (Rashed et al., 2025). For integration with existing tools, it offers robust capabilities that allow immediate connection to existing SIEMs and intrusion detection systems (Rashed et al., 2025).

Recorded Future

Recorded Future is a premium enterprise intelligence platform designed for massive scale. Its data collection relies heavily on automated scrapers and rigid collection nets to monitor open and dark web ecosystems (Saeed et al., 2023). The platform standardizes unstructured text into structured indicators utilizing robust REST APIs (Mavroeidis, 2023). While it provides deep visibility into the threat landscape and delivers high-velocity real-time alerts, competitive analyses note that it often requires security teams to manually correlate intelligence with their internal attack surfaces and business priorities (Saeed et al., 2023). For APT capabilities,

Recorded Future powers advanced adversary tracking through automated dark web monitoring (Mavroeidis, 2023). Its automation capabilities focus heavily on alert triage, but its higher analyst dependency can mean longer onboarding cycles before teams can fully operationalize the platform compared to more automated alternatives (Saeed et al., 2023). Finally, for integration with existing tools, it connects broad security stacks. However, small organizations may need to dedicate significant human resources to filter its vast collection volume to prevent alert fatigue manually (Saeed et al., 2023).

Analysis on Fit for Scenario Organization (Acuity Health)

Acuity Health operates as a rapidly expanding urgent care network heavily reliant on a cloud-hosted Microsoft Azure environment protected by a Zero Trust Architecture. The organization functions with a small IT and security team, making the integration of automation and cloud-native services critical to maintaining daily clinical and business operations. Given these severe resource constraints, Anomali ThreatStream represents the most strategic platform fit for Acuity Health. Because the security team lacks the headcount to manually triage thousands of generic alerts, a platform featuring ML-driven automation is required to actively filter out noise, score threats by confidence, and prioritize genuine indicators of compromise without taxing human analysts.

The critical need to integrate advanced, automated threat intelligence is underscored by our recent insider threat incident (INS-2026-EHR-VIP), wherein a clinical nurse exploited privilege creep to scrape highly sensitive electronic medical records of VIP patients manually. Insider threats in healthcare are particularly devastating because these actors abuse legitimate access privileges, operating undetected during the post-authentication phase where traditional perimeter defenses fail.

To ensure comprehensive operational depth, Anomali ThreatStream will be operationalized through the FLARE threat response framework across five distinct phases. During the Find (Detection) phase, ingesting STIX/TAXII threat feeds natively into Azure Sentinel enables the system to cross-reference external identity-theft indicators and compromised credential dumps against internal User and Entity Behavior Analytics (UEBA) telemetry in real time. In the Logging phase, all anomalous database queries, privilege escalation attempts, and bulk EHR access logs are normalized and enriched with external threat intelligence scores as events occur. During the Analysis phase, automated machine-learning models evaluate the clinician's baseline behavior against current access patterns, immediately identifying unauthorized bulk data scraping during post-authentication sessions. For Remediation & Containment, the platform triggers automated Azure Logic Apps to execute graduated response playbooks—instantly dropping a compromised clinician account to read-only access to preserve patient care continuity while halting unauthorized data extraction. Finally, in the Escalation phase, high-confidence alerts enriched with full CTI attribution are automatically escalated to the CISO and on-call incident responders with actionable forensic artifacts.

References

Anomali. (2023). *Operationalizing threat intelligence with automated scoring and STIX/TAXII integration* (White Paper No. TR-2023-04). Anomali Cybersecurity Research.

Mavroeidis, V. (2023). An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. *IEEE Access, 11*, 45120–45135. https://doi.org/10.1109/ACCESS.2023.3271000

OASIS Open. (2021). *Structured Threat Information eXpression (STIX) Version 2.1* (OASIS Standard). OASIS Open. https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html

Rashed, M., Viso, I. T.-D., & González-Tablas, A. I. (2025). A comparison of cyber intelligence platforms in the context of IoT devices and smart homes. *Electronics, 14*(22), 4503. https://doi.org/10.3390/electronics14224503

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors, 23*(16), 7273. https://doi.org/10.3390/s23167273

Sakellariou, G., Fouliras, P., Mavridis, I., & Sarigiannidis, P. (2022). A reference model for cyber threat intelligence (CTI) systems. *Electronics, 11*(9), 1401. https://doi.org/10.3390/electronics11091401