Cyber Threat Intelligence (CTI) Strategy Report

Name: Mitchelle Anduru
Date: 24/01/2026
Role: Junior Cybersecurity Analyst

---

1. Executive Summary

SecureHealth's CTI strategy is designed to proactively reduce ransomware risk by improving early warning, detection, and containment across critical healthcare systems, including EMR platforms, telehealth services, endpoints, and backup infrastructure. The program prioritizes ransomware campaigns, credential theft, and third-party compromise as the highest-likelihood pathways to operational disruption and patient-care impact, while also supporting HIPAA-aligned confidentiality and availability requirements. Intelligence will be collected from internal telemetry (CrowdStrike endpoint signals, access/system logs, backup activity) and external sources (Recorded Future feeds, healthcare ISACs, OSINT, vendor advisories), validated for credibility, and translated into actionable outputs such as IOC packages, detection rules, threat briefs, and incident-response guidance. The highest-priority implementation actions are: (1) integrating threat intelligence into detection and response workflows (TIP → EDR/SIEM → IR), (2) establishing clear dissemination routines for tactical, operational, and strategic intelligence, and (3) measuring effectiveness through KPIs such as reduced ransomware detection time, faster containment, and improved detection accuracy, with continuous refinement based on post-incident and stakeholder feedback.

2. Key deliverables

- **Tactical IOC Packs (daily/weekly):** hashes, IPs, domains, email indicators, and behavioral signals mapped to ransomware TTPs for rapid deployment into detections.
- **Operational Threat Briefs (bi-weekly/monthly):** campaign summaries, attack chains, common initial access patterns, and containment lessons to support incident response.
- **Threat Hunting Hypotheses (weekly):** "what to look for" queries aligned to ransomware behaviors (credential misuse, lateral movement, backup tampering).
- **Strategic Executive Summaries (monthly/quarterly):** sector trends, risk posture, and exposure themes tied to compliance and business impact.
- **Third-Party Risk Alerts (as-needed):** vendor advisories and supply-chain related intelligence affecting systems with EMR access.

3. Objectives and Scope Definition

Define Objectives:

Document the specific goals of the CTI strategy, detailing what the organization aims to achieve (e.g., enhancing threat detection).

The main goal of SecureHealth's Cyber Threat Intelligence (CTI) strategy is to proactively detect, understand, and reduce the risk of ransomware attacks targeting its healthcare systems. This strategy focuses on improving visibility into emerging ransomware campaigns, identifying Indicators of Compromise (IOCs) early, and shortening the time between detection and containment.

At the same time, the CTI program supports regulatory compliance by safeguarding electronic medical records (EMRs) and ensuring SecureHealth continues to meet HIPAA requirements. In a healthcare environment where downtime can directly affect patient care, early intelligence is critical.

Define Scope:
Outline the areas within the organization that will be covered by CTI efforts, including relevant departments, regions, or operational boundaries.

The CTI strategy applies to SecureHealth's core technology environment, including EMR systems, telehealth platforms, endpoint devices, and backup infrastructure. CTI efforts primarily support internal security operations, incident response, and compliance teams, while also extending to third-party vendors that have access to sensitive systems.

Both internal intelligence collection and external threat monitoring relevant to the healthcare sector fall within this scope.

Policy Alignment:
Identify key security policies aligned with the CTI goals. Briefly describe why these policies are priorities for this strategy and how they will influence subsequent phases.

This CTI strategy aligns with SecureHealth's information security, incident response, and data protection policies. These policies emphasize patient data confidentiality, system availability, and rapid incident response. Intelligence gathered through CTI directly informs security controls, endpoint protection configurations, and ongoing compliance monitoring.

---

4. Threat Intelligence Needs Assessment

Risk Assessment:
Conduct a risk assessment, detailing the most significant threats and vulnerabilities facing the organization.

SecureHealth faces a high risk from ransomware attacks due to the critical nature of healthcare services and the sensitivity of patient data. Stolen or compromised credentials present another major threat, often serving as the initial access point for ransomware deployment.

Additionally, third-party vendors with system access introduce supply-chain risks that attackers can exploit if not properly monitored.

Stakeholder Collaboration:
Document feedback from stakeholders to determine the types of intelligence (tactical, operational, strategic) most beneficial to the organization.

Different teams rely on CTI in different ways.

- The **IT Security Team** needs tactical intelligence such as ransomware IOCs, file hashes, malicious IPs, and behavioral indicators to strengthen CrowdStrike EDR detections.
- The **Compliance Team** depends on strategic intelligence to understand regulatory exposure and maintain HIPAA compliance.
- The **Incident Response Team** requires operational intelligence that provides context on attack patterns, attacker behavior, and effective containment strategies.

Prioritization of Intelligence Needs:
Explain the rationale for prioritizing specific intelligence needs, focusing on high-impact and high-likelihood threats.

Ransomware intelligence is the top priority due to its high likelihood and severe operational impact. Intelligence related to credential theft and third-party compromise is also prioritized, as these threats often occur before ransomware attacks and can be stopped if detected early.

---

5. Gathering and Integrating Intelligence Sources

Intelligence Sources:
List and describe the sources for threat intelligence, including internal sources (e.g., security logs, SIEM data) and external sources (e.g., threat feeds, OSINT, ISACs).

SecureHealth uses a mix of internal and external intelligence sources. Internal sources include endpoint telemetry from CrowdStrike, system and access logs, and backup activity logs from Veeam. External sources include Recorded Future threat feeds, open-source intelligence (OSINT), healthcare ISACs, and vendor security advisories.

Integration Process:
Document how these sources are integrated into the organization’s existing security infrastructure, describing any tools or platforms used.

Threat intelligence feeds are centralized in Recorded Future, which acts as the primary Threat Intelligence Platform (TIP). Relevant intelligence is correlated with CrowdStrike endpoint data to support real-time detection and response. Key insights are also shared with backup and recovery teams to confirm ransomware resilience and recovery readiness.

Source Validation:
Explain the processes for validating the credibility and relevance of each intelligence source.

All intelligence sources are evaluated based on credibility, relevance to healthcare threats, and historical accuracy. Intelligence from trusted vendors and industry-specific ISACs is prioritized, while OSINT is validated by cross-checking multiple reliable sources.

---

6. Development of Threat Intelligence Processes

Data Collection Procedures:
Describe the methods for collecting raw threat data and any specific techniques used (e.g., Indicators of Compromise).

Threat data is collected continuously from Recorded Future feeds, CrowdStrike telemetry, and internal logs. This includes IOCs, attacker tactics, techniques, and procedures (TTPs), as well as indicators of lateral movement and data exfiltration.

Analysis and Insight Generation:
Outline the analysis techniques employed to derive actionable insights, focusing on identifying patterns, attack tactics, or emerging threats.

Collected data is analyzed to identify patterns linked to ransomware campaigns, such as common initial access methods and payload delivery techniques. Analysis involves trend identification, IOC correlation with endpoint activity, and mapping attacker behavior to known ransomware frameworks.

Dissemination Protocols:
Detail the protocols for sharing intelligence insights with relevant teams (e.g., security operations, incident response).

Actionable intelligence is shared through structured reports and real-time alerts. Tactical intelligence supports EDR rule updates, operational intelligence assists incident response during investigations, and strategic intelligence summaries are provided to management and compliance teams for informed decision-making.

---

7. CTI Capability and Infrastructure Building

Tool and Platform Acquisition:
List the tools and platforms (e.g., Threat Intelligence Platforms) acquired or developed to support CTI efforts.

SecureHealth relies on Recorded Future as its Threat Intelligence Platform, CrowdStrike for endpoint detection and response, and Veeam for backup and recovery. Together, these tools strengthen threat visibility, detection, and resilience against ransomware attacks.

Team Development and Training:
Describe the personnel structure for CTI operations, including any specific roles, responsibilities, and training requirements.

The CTI function is supported by cybersecurity analysts responsible for intelligence analysis, IOC management, and reporting. Ongoing training focuses on ransomware trends, threat hunting techniques, and healthcare-specific threat scenarios to ensure analysts stay current.

Capability Evaluation:
Document the organization's current CTI capabilities, identifying any gaps and future investment needs.

While current CTI capabilities provide strong external intelligence visibility, there is a need for increased automation in intelligence correlation and response. Future improvements may include deeper SIEM integration and automated incident response playbooks.

---

8. Communication and Collaboration Channels

Internal Communication Channels:
List established channels for communicating CTI insights within the organization (e.g., with IT, management, security teams).

CTI insights are shared internally through secure dashboards, incident response briefings, and regular intelligence reports distributed to IT security, compliance, and executive leadership teams.

External Collaboration:
Document partnerships with industry peers, law enforcement, or intelligence-sharing communities, specifying how these relationships enhance threat awareness.

SecureHealth collaborates with healthcare ISACs, cybersecurity vendors, and relevant law enforcement agencies to exchange threat intelligence. These partnerships improve early warning capabilities and provide valuable sector-specific context.

Collaboration Challenges:
Discuss any challenges faced in establishing collaboration channels and strategies for improvement.

Key challenges include information overload and timely intelligence sharing. These are addressed by prioritizing actionable intelligence and establishing clear communication and escalation protocols.

---

9. CTI Effectiveness Measurement and Optimization

Key Performance Indicators (KPIs):
Define the metrics used to measure CTI effectiveness (e.g., reduced response time, detection rate improvements).

CTI effectiveness is measured using metrics such as reduced ransomware detection time, faster incident response, and improved accuracy of endpoint detections.

Continuous Improvement Process:
Outline the feedback and review mechanisms in place to adapt the CTI strategy to new threats and evolving risks.

The CTI strategy is reviewed regularly to adapt to evolving threats and lessons learned from past incidents. Identified intelligence gaps are addressed through process refinement and tool enhancements.

Stakeholder Feedback:
Describe how feedback from stakeholders is gathered, documented, and applied to optimize the CTI strategy.

Feedback from security, compliance, and incident response teams is collected through post-incident reviews and periodic assessments to continuously improve and mature the CTI program.

10. Assumptions & Limitations

This CTI strategy is based on a scenario-driven healthcare environment and assumes availability of core telemetry and tooling, including Recorded Future for threat intelligence management, CrowdStrike endpoint telemetry, and sufficient logging from identity, system, and

backup infrastructure. Intelligence sharing and monitoring must operate within privacy and regulatory constraints (including HIPAA considerations), which may limit the use of intrusive inspection methods such as broad TLS decryption. The strategy focuses on ransomware as the primary threat priority; while it improves overall maturity, additional threat categories (e.g., insider threats, nation-state espionage) may require separate deepening of collection and analyst workflows as the program matures.