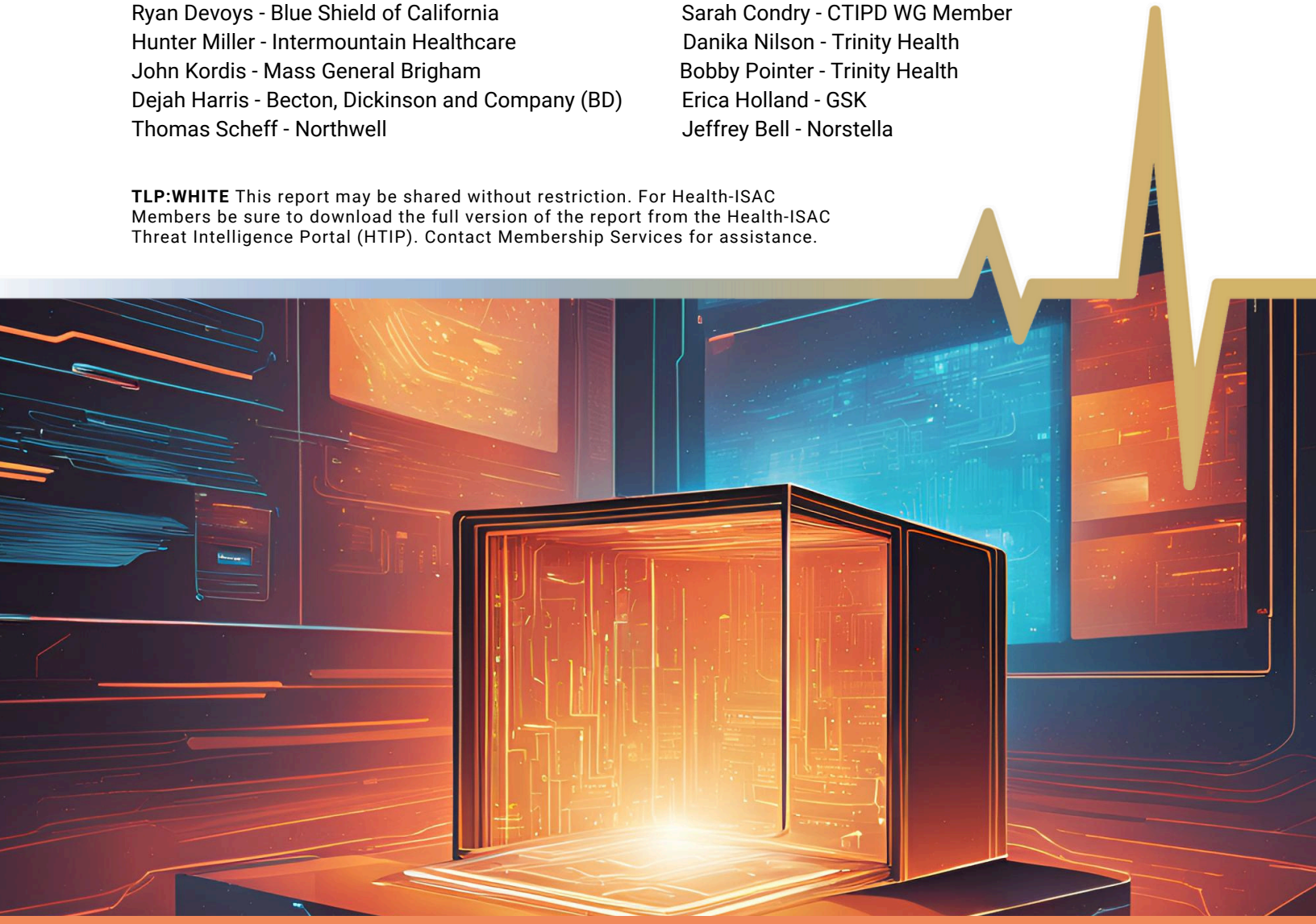
Guidance for CTI in a Box

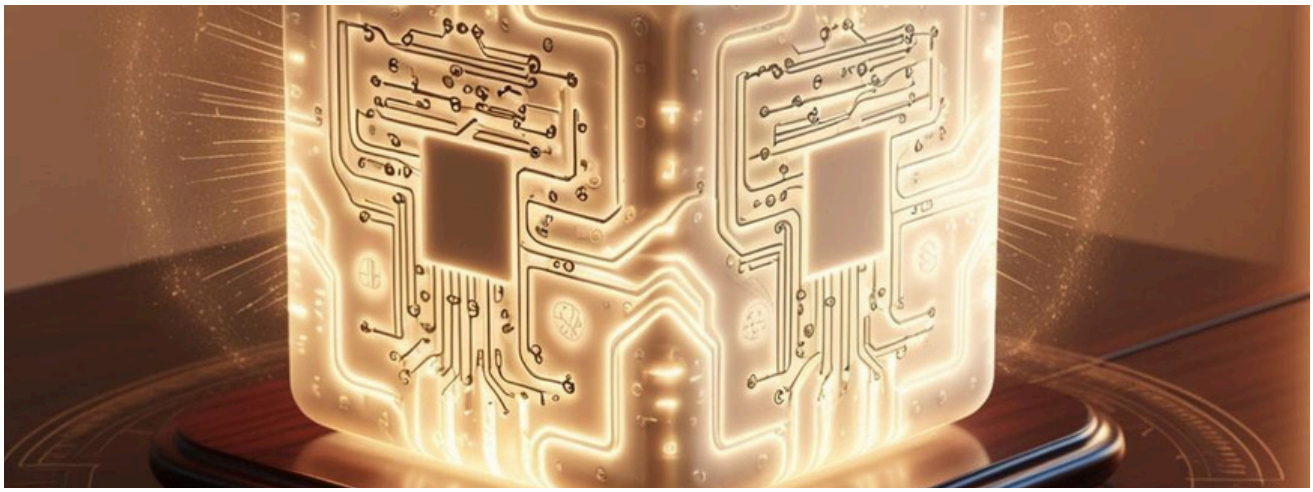
A comprehensive toolkit developed to help organizations build, mature, and standardize their Cyber Threat Intelligence programs with ready-to-use tools, templates, and resources

Authors:

Rachel James - CTIPD WG Chair
Caleb Chitwood - HCA
Carol Kaczmarski - Advanced Health Systems
Bryan Nakayama - Optum
Ryan Devoys - Blue Shield of California
Hunter Miller - Intermountain Healthcare
John Kordis - Mass General Brigham
Dejah Harris - Becton, Dickinson and Company (BD)
Thomas Scheff - Northwell
John King - CTIPD WG Chair
Vince Peeler - Children's Minnesota
Roger Browning - STERIS
Leah Furyk - Phreesia
Sarah Condry - CTIPD WG Member
Danika Nilson - Trinity Health
Bobby Pointer - Trinity Health
Erica Holland - GSK
Jeffrey Bell - Norstella



Contents



> *"A skilled threat intelligence team is the cornerstone of a resilient health sector organization. By proactively identifying, analyzing, and mitigating cyber threats, these teams empower health sector organizations to make informed decisions that safeguard patient data and ensure business continuity."*

Executive Summary

This whitepaper presents an analysis of a survey conducted among Health Information Sharing and Analysis Center (Health-ISAC) members regarding their Cyber Threat Intelligence (CTI) programs by the CTI Program Development Working Group.

The purpose of the survey was to provide valuable insights into the current state of CTI initiatives within the health sector, highlighting areas of strength[1]and opportunities for improvement. The CTI Program Development Working Group used these insights to focus on the highest valuable deliverables for collaboration in the community.

Key Findings

1. Executive Buy-in: A significant majority (81.25%) of organizations report having executive buy-in for their CTI programs, with CISOs/CSOs being the primary champions (84.38%).

2. Maturity Levels: Most organizations (59.37%) rate their CTI Capability Maturity Model (CMM) at levels 1-2, indicating room for growth and improvement.

3. Intelligence Sharing: Only 50% of organizations are currently sharing intelligence with external stakeholders and/or ISACs, suggesting an opportunity for increased collaboration.

4. Legal Engagement: Less than a third (31.25%) of organizations have engaged legal teams for their CTI initiatives, potentially limiting the scope and effectiveness of information-sharing programs.

5. Training: While 56.25% allow for training in ISAC functions, only 9.38% have a dedicated CTI analyst training program, indicating a potential skills gap.

6. Intelligence Requirements (IR): 46.88% of organizations have developed IRs, with an additional 31.25% seeking help in this area.

7. Threat Intel Platforms (TIPs): 62.5% of organizations have deployed a TIP, demonstrating a commitment to centralizing and managing threat intelligence.

8. Open Source Intelligence (OSINT): A high percentage (78.12%) of organizations utilize OSINT, with Feedly being the most popular aggregator.

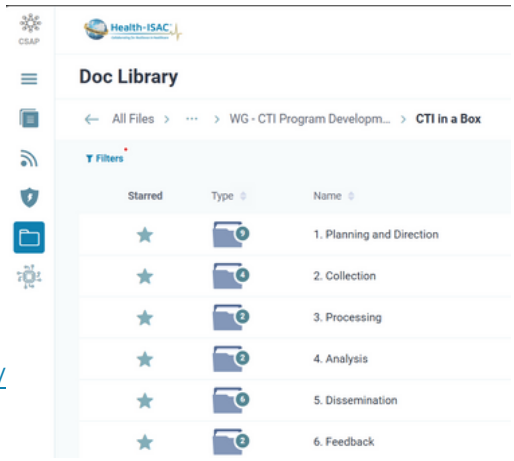
9. Performance Metrics: Only 18.75% of organizations use Key Performance Indicators (KPIs) to track team performance and address stakeholder requirements, suggesting a need for more robust measurement and evaluation practices.

Detailed Analysis

Working Group's Response to Survey Results
The CTI Program Development working group used these key findings from the survey to shape the deliverables and products to produce for the Health-ISAC community in 2024. These resources have been created and organized according to the CTI lifecycle into a resource we call CTI in a Box.

- https://health-isac.cyware.com/webapp/user/doc-library/7c1a36b7-34fa-45f6-b698-db64828cc534

In this paper, we briefly discuss some of these products as they relate to those key findings (and the Health-ISAC Threat Intelligence Portal (HTIP) folder you can find them):



Executive Buy-in

- CTI Pitch Deck (Planning and Direction)
- Stakeholder Education (Planning and Direction)

Maturity Levels

- Maturity and effectiveness resources (Planning and Direction)

Intelligence Sharing

- Dissemination Templates (Dissemination)
- Health-ISAC Information Sharing Best Practices
  - https://health-isac.org/h-isac-information-sharing-best-practices-2/

Legal Engagement

- Rules of Engagement Template (Planning and Direction)

Training

- Significant resources for free training, interviewing and core competencies for CTI analysts (Feedback)

Intelligence Requirements (IR)

- Intelligence Requirements exchange and library of IRs -
  - https://health-isac.cyware.com/webapp/user/doc-library/36894b75-699c-4137-bdf5-2e90c626bd5f
- Guide to IRs
  - https://health-isac.cyware.com/webapp/user/doc-library/15606e1e-228d-4a8f-964d-3c37322a68d7
- IR PIR SIR template and example (Planning and Direction)

Threat Intel Platforms (TIPs)

- List of most popular collection feeds (Collection)
- Intel Providers Best Practices
  - https://health-isac.cyware.com/webapp/user/doc-library/64afab71-9619-40f2-8471-af74008ed3f9

Open Source Intelligence (OSINT) and Feedly

- Feedly feed exchange (Collection)
  - https://health-isac.cyware.com/webapp/user/doc-library/7f3fafbc-9a82-42e8-b39a-91bb92cb0e18

The rest of this paper provides guidance on how to best leverage some of these resources for maximum benefit for any organization facing similar challenges.

Threat Landscape

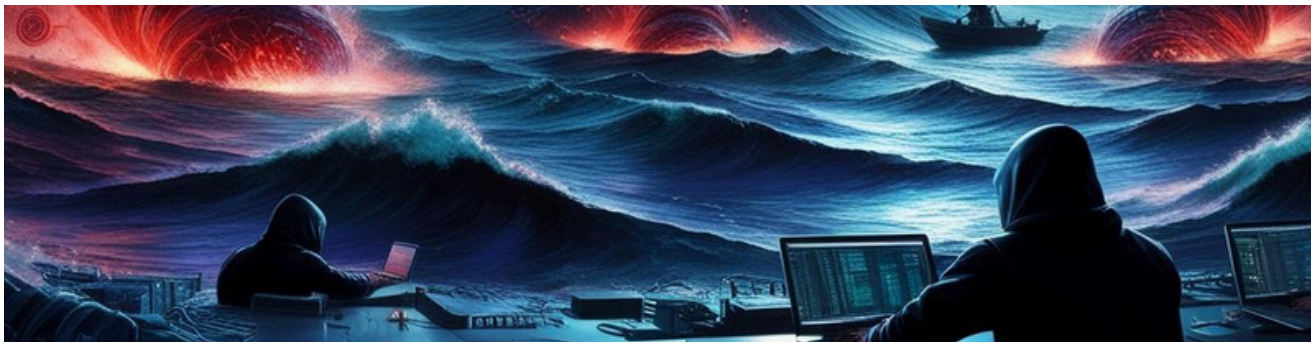
Health sector organizations face a challenging threat environment as the industry consistently ranks among those most victimized by both criminal and nation-state threat actors. There are several reasons why the industry is a particularly tempting target for threat actors: first, health sector entities handle valuable data such as personally identifiable information (PII) and protected health information (PHI). Second, they are technologically dependent with complex and evolving attack surfaces, particularly in clinical environments. Third, hospitals and smaller clinical entities frequently do not have adequate resources to secure their environments. Fourth, health sector operations are ripe for phishing because they frequently involve contact with the public. Finally, the risk to lives and the need for operational continuity means that victims have greater incentives to pay ransom demands.

The harms from attacks on health sector entities scale rapidly. Even attacks on individual hospitals can disrupt the provision of health sector services to a single region by diverting patients to other hospitals thereby straining hospital resources. One working paper finds that ransomware attacks increase mortality at the affected hospitals and likely has additional knock-on effects on the rest of the health system.[1] Due to the structure of the health sector, the compromise of a single entity can have sectoral consequences as happened with the 2024 ransomware attack on Change Healthcare which led to severe financial consequences for the health sector which depended on change for billing services.

The primary threat to the health sector arises from opportunistic and financially motivated criminal threat actors which seek to exploit the factors listed at the beginning of this section. The scale of financially driven attacks has exploded over the last few years with the U.S. Department of Health and Human Services observing a 264% increase in ransomware attacks against the sector from 2019-2024.[2] The large amounts of sensitive PHI and PII that health sector entities hold and manage serve as a tempting target for financially motivated threat actors which monetize stolen data through various extortion strategies from releasing the data on dedicated leak sites to extorting individual people whose sensitive data was stolen.

Trends in the criminal landscape suggest that health sector entities will face an increasingly complex criminal threat landscape. First, due to declining ransom payment rates, threat actors are demanding higher ransoms and increasingly eschewing encryption and data theft in favor of pure theft operations. Both hinge on the volume of victims - fewer victims paying higher ransoms increases the average ransom payment received by a threat actor and pure data theft attacks are easier and faster to accomplish allowing for a greater volume of victims.[3]

Second, recent law enforcement action against LockBit and ransomware-as-a-service (RaaS) group infighting has driven the proliferation of new groups and an increase in unaffiliated ransomware actors. The increasing number of actors complicates the threat landscape because it increases the variety of ransomware strains and TTPs used by threat actors since the RaaS services provided standardized playbooks.[4] Finally, the expansion in access to Generative AI applications increase the efficacy of fraud by making it trivial to clone a voice or likeness.



1. https://www.statnews.com/2023/11/17/hospital-ransomware-attack-patient-deaths-study/
2. https://www.hhs.gov/about/news/2024/03/13/hhs-office-civil-rights-issues-letter-opens-investigation-change-healthcare-cyberattack.html
3. https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments
4. https://www.coveware.com/blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024,https://cyberint.com/blog/research/fall-of-major-ransomware-groups-sparks-rapid-rise-of-new-threats/

Detailed Survey Analysis

Organizational Context

The survey respondents represent a diverse range of health subsectors, with providers/clinicians (37.5%), pharmaceutical/biotech companies (21.88%), and health information technology firms (21.88%) being the most prevalent. Organization sizes vary widely, with a fairly even distribution across different scales, from less than 1,000 employees to over 100,000.

Executive Support and Program Champions

The high level of executive buy-in (81.25%) for CTI programs is a positive indicator of the perceived importance of threat intelligence in the health sector. CISOs/CSOs emerge as the primary champions (84.38%), followed by CIOs (28.12%). This strong leadership support provides a solid foundation for further development and investment in CTI capabilities.

Getting executive buy-in for cyber intelligence programs, particularly with CISOs or CSOs as primary champions, involves framing the program as a critical investment in the organization's resilience and competitive edge. Here's a structured approach to help secure buy-in:

- **Align with Business Goals**
  - **Demonstrate Value to Business Objectives:** Emphasize how cyber intelligence supports critical business priorities, such as protecting intellectual property, ensuring business continuity, and mitigating financial and reputational risks.
  - **Highlight the Financial Impact:** Outline the potential savings by avoiding or quickly mitigating incidents, compared to recovery costs from successful attacks.

- **Communicate Risks in Business Terms**
  - **Translate Cyber Threats into Operational Impact:** Explain threats not in technical jargon but as potential disruptions to critical business functions.
  - **Use Clear Metrics:** Use quantifiable metrics, such as the reduction in incident response times or the impact on downtime, that resonate with financial stakeholders and show a direct link between intelligence and business risk management.

- **Emphasize the Proactive Advantage**
  - **Position Cyber Intelligence as a Strategic Asset:** Stress how intelligence enables proactive, rather than reactive, decisions. CISOs and CSOs should communicate that a cyber intelligence program is not just a reactive defense but a means of staying ahead of threats.
  - **Support Competitive Edge:** Show how intelligence can inform decisions, like entering new markets or handling mergers, by assessing risks from the cyber environment, including competitor activities or potential espionage.

- **Show Examples of Past Incidents and Benefits of Intelligence**
  - **Use Case Studies:** Present real-world case studies where cyber intelligence prevented costly incidents or reduced their impact. Industry-specific examples can be compelling.
  - **Show Success Metrics:** If possible, demonstrate metrics from past internal programs or early pilots, such as reduced incident rates or faster response times.

- **Outline the Long-Term ROI and Mitigation Strategy**
  - **Focus on ROI:** Explain how the intelligence program can yield long-term cost savings by reducing the risk of high-cost incidents and lowering insurance premiums through better risk profiles.
  - **Show Risk Mitigation Framework:** Describe how the intelligence program builds a resilient security posture and can minimize the impact of emerging threats, helping to assure executives of its preventive value.

- **Engage Executives Through Regular Briefings**
  - **Provide Tailored Briefings:** Ensure that CISOs/CSOs consistently brief executives and key decision makers in a language and format they understand, perhaps through regular "threat landscape" updates tied to specific business risks.
  - **Highlight Industry Trends and Peer Activities:** Benchmark against competitors or industry standards to illustrate the importance of cyber intelligence in the competitive landscape and reassure all key decision makers that this is a well-justified investment.

- **Develop a Clear Roadmap for Implementation and Maturity**
  - **Show a Phased Plan:** Outline a straightforward approach to rolling out the intelligence program, including milestones demonstrating incremental value and progress.
  - **Highlight Scalability and Flexibility:** Explain that the program can scale with the company's needs and that investment will be aligned with organizational growth and evolving threat landscapes.

- **Leverage the CISO/CSO's Leadership**
  - **CISO/CSO as Advocates:** Position the CISO or CSO as a strategic advisor who can bridge security and business needs. Their voice can add credibility by demonstrating that the program is about building a resilient organization, not just meeting compliance.

With the CISO or CSO as an active, articulate champion, leading decision makers are more likely to recognize the cyber intelligence program as a strategic investment essential for long-term security and success.

Maturity and Effectiveness

Despite strong executive support, the survey reveals that most organizations are still in the early stages of CTI program maturity. The majority (59.37%) rate their CTI Capability Maturity Model (CMM) at levels 1-2, indicating basic or fragmented processes. Similarly, 71.88% rate their CTI effectiveness at levels 1-2. This suggests a significant opportunity for improvement and maturation of CTI programs across the sector.

- How/who determines maturity?
- Why do we care about relative maturity?
- How do we compare with maturity in other industries?

Cyber Threat Intelligence (CTI) program maturity assessments are crucial for organizations to evaluate and improve their threat intelligence capabilities. These assessments help identify strengths, weaknesses, and areas for growth in CTI programs, enabling organizations to allocate resources effectively and enhance their overall security posture. By conducting regular maturity assessments, CTI teams can ensure their programs evolve to meet emerging threats and align with organizational goals.

The CTI Program Development Working Group has identified six resources that we believe are valuable tools for maturity assessments:

CTI-Maturity.com Assessment:

- Provides a free, online self-assessment tool based on the Intelligence Cycle. It covers planning and direction, collection, processing, analysis, and dissemination. This assessment offers immediate results and recommendations for improvement.

CTI-CMM:

- The model provides a structured approach to evaluate and enhance an organization's ability to collect, analyze, and utilize threat intelligence effectively. It helps organizations understand their current capabilities and provides a roadmap for improvement. Version 1 is available in the document folder.

Cyber Threat Intelligence Tradecraft Report:

- While the report does provide a method of assessing maturity levels, it does not provide detailed scoring like many of the other tools here. However, it does provide specific recommendations on how to become a high-performing CTI team, which bears significant inclusion in this list.

Mandiant's CTI Program Maturity Assessment:

- Focuses on six key areas: collection, processing, analysis, production, dissemination, and feedback. It emphasizes the importance of aligning CTI efforts with business objectives and offers a comprehensive framework for evaluation. This is a little more detailed, and you many need professional consultation.

CREST Cyber Threat Intelligence Maturity Assessment Tools:

- Offers a range of assessment tools, including self-assessment questionnaires and third-party assessments. It focuses on various aspects of CTI, including strategic, operational, and tactical intelligence. CREST provides a variety of tools, allowing for both self-assessment and third-party evaluation.

Framework for Cyber Intelligence Management (FCIM):

- Developed with knowledge management principles, organizational learning, and intelligence processes. It is based on five components: the organization, people, processes, technology, and governance. This is built into each of the Intelligence Pyramid's five levels: data flow, assessment, analytics, synchronization, driving.

CTI professionals should consider their organization's specific needs, resources, and current maturity level when choosing an assessment method. A combination of these tools may provide the most comprehensive evaluation of a CTI program's maturity. Links and some example assessments are available within CTI in a Box.

Intelligence Sharing and Collaboration

While 50% of organizations report sharing intelligence with external stakeholders and/or ISACs, there is room for growth in this area. Increased collaboration and information sharing could enhance the overall threat intelligence capabilities of the health sector. The relatively low engagement of legal teams (31.25%) in CTI initiatives may be a factor limiting more extensive information-sharing practices.

Increased collaboration and information sharing could enhance the overall threat intelligence capabilities of the health sector as well as improve security posture and resource access. Improved security posture enables organizations to create early detections for attacks and increase faster response times.

Through information sharing, organizations can crowdsource knowledge and increase their knowledge without increasing their limited budgets. The other benefit is the ability to quickly identify emerging threats and trends. Sharing knowledge across health sector organizations ensures that threat actors targeting the industry are detected earlier and mitigations are streamlined.

Additionally, relevant shared intelligence is vital for those small or single individual CTI teams. The time saved from researching specific indicators of compromise (IOCs) and effective mitigations increases exponentially compared to conducting the necessary research to best outmaneuver the adversaries. This allows the team to better maximize their time across other required tasks.

Information sharing programs provide participating organizations, external stakeholders and ISACs with significant benefits for all parties. Health-ISAC provides member organizations with the ability to share intelligence requirements using the Threat Intel platform.

Sharing information with external stakeholders has inherent risks, there are indications that many are unclear about how much information and the type of information that should be shared.[5] Establishing information sharing agreements are key to removing the ambiguity and risks of intelligence sharing. Agreements can outline the company's strategy for sharing intelligence with external partners. First, identify the key external partners whom which the organization will need to share information. The Membership Service Agreement with Health-ISAC establishes classification requirements and data sharing for the parties involved.

The advantages of information sharing significantly surpass the associated risks. Furthermore, if additional support is required, this approach serves as an excellent foundation for establishing robust relationships and bridging the gap between cyber threat intelligence teams and the company's legal entities.

5. https://cissm.umd.edu/sites/default/files/2019-07/Cyber%20information%20sharing%20agreement%20report%20-%20102017%20-%20FINAL.pdf, pg. 36

Legal Engagement

Coordinating effectively with the legal team is critical for Cyber Threat Intelligence (CTI) teams to ensure compliance with laws and regulations while maximizing operational efficiency. In the Health-ISAC study, less than a third (31.25%) of organizations have engaged legal teams. To start, establishing clear communication channels is essential. Regular meetings between CTI and legal teams should be scheduled to discuss ongoing activities, address potential legal risks, and stay updated on compliance requirements. Assigning dedicated points of contact (POCs) in both teams can streamline communication and ensure timely responses to queries. The approach should consist of:

- Establish Clear Communication Channels
- Develop Collaborative Policies
- Involve Legal Early in Processes
- Provide Context for Legal Decisions
- Provide Legal Expertise in Documentation
- Establish a Decision-Making Process
- Joint Training and Awareness
- Maintain Documentation and Audits
- Collaborate During Incident Response

Establish Clear Communication Channels

Collaborative policies form the backbone of this relationship. CTI and legal teams should work together to create compliance frameworks that define permissible intelligence-gathering activities, especially in high-risk areas such as dark web monitoring or threat actor engagement. Legal guidance should also be incorporated into incident response plans and intelligence-sharing protocols to align with regulatory requirements. This collaboration is particularly important for addressing cross-border legal constraints, ensuring international compliance. The communications channels should also include sharing agreements with outside entities such as the U.S. Government and ISACs.

Develop Collaborative Policies

Involving the legal team early in the intelligence process is key. Before initiating intelligence-gathering efforts, CTI teams should consult legal experts to evaluate potential risks. Similarly, all third-party tools and vendor agreements used for CTI activities should be reviewed to ensure they adhere to data privacy and security laws. Legal teams should also be briefed on the threat landscape and operational scenarios to provide informed guidance. Sharing insights about emerging threats and the scope of CTI activities can help the legal team understand the urgency and nuances of certain intelligence operations.

Involve Legal Early in Processes

Involving the legal team early in the intelligence process is key. Before initiating intelligence-gathering efforts, CTI teams should consult legal experts to evaluate potential risks. Similarly, all third-party tools and vendor agreements used for CTI activities should be reviewed to ensure they adhere to data privacy and security laws.

Provide Context for Legal Decisions

Cyber threat intelligence (CTI) teams should provide context for legal decisions to ensure that legal teams are well-informed about the threat landscape and operational scenarios. By sharing insights on emerging threats and the scope of CTI activities, legal teams can better grasp the urgency and complexities of intelligence operations, enabling them to offer more precise and effective guidance.

Provide Legal Expertise in Documentation

The legal team's expertise is invaluable in documentation and compliance. Together, the teams should establish policies for handling sensitive or personal data during collection, analysis, and sharing. Legal approval is particularly important for reports prepared for regulators or partners.

Establish a Decision-Making Process

Escalation protocols and a defined decision-making process are necessary to address legal concerns. Legal expertise can be crucial when CTI activities involve controversial techniques or potential risks like interacting with threat actors or handling stolen data, engaging other third parties for any forensic analyses, and lead communications with cyber insurance entities to ensure a comprehensive cybersecurity strategy.

Joint Training and Awareness
Joint training initiatives can further strengthen this partnership. Cross-training the legal team in CTI basics ensures they better understand the technical aspects of intelligence work, while CTI members can stay updated on relevant laws and regulations through routine legal briefings. Additionally, legal teams are well versed in conducting training for all levels of executives and board members so as to clearly define at what point should each level of decision-making decisions be made.

Maintain Documentation and Audits
Documentation and audits are also critical. CTI teams should maintain detailed logs of their activities and collaborate with the legal team on periodic audits to ensure compliance and identify potential blind spots. For small teams, legal entities can provide many templates and guidance to minimize individual efforts.

Collaborate During Incident Response
During incidents like data breaches, close collaboration is crucial. The legal team should oversee breach notification requirements to ensure compliance with regulations such as GDPR, CCPA, or state-specific laws. Legal approval is also necessary before sharing intelligence with law enforcement or external agencies. By fostering this close collaboration early and inclusion during exercises or tabletops, CTI and legal teams can align operational goals with legal safeguards, minimizing risks and enhancing the organization's overall resilience.

Example agreement with legal for interaction with threat actors for intelligence purposes is available in the CTI in a Box.

Training and Skill Development

The survey highlights a potential skills gap in CTI. Although 56.25% of organizations allow for training in ISAC functions, only 9.38% have a dedicated CTI analyst training program. This discrepancy suggests a need for more structured and comprehensive training initiatives to build and maintain CTI expertise within organizations.

Key points for consideration regarding the health sector-wide lack of CTI training:

- How has lack of training impacted organizations' CTI programs/overall cybersecurity?
- How does healthsectorCTI training compare to other industries?
- Types of training important to a CTI team (technical, DFIR, formal courses, traditional intel, etc.)

There are several methods to establish structured and comprehensive training initiatives within an organization. These may encompass courses, certifications, or, when feasible, in-house development through formal or informal training programs. For small teams or individuals, it is important to recognize that cost may not be the sole obstacle. The time commitment required for most training can significantly disrupt other essential daily tasks. Therefore, the cost-benefit analysis should be considered holistically in alignment with the company's long-term objectives.

A challenge for organizations to provide training is the financial commitment required. Funding for CTI training is typically provided directly by the organization. The amount and type of funding provided varies organization by organization. Some organizations will offer re-imbursement for training courses or certifications, requiring the practitioner to pay for the courses upfront which can be a financial burden on the practitioner. The practitioner also has the opportunity to pay for the training themselves.

There are low-cost options provided through LinkedIn Learning, Pluralsight and Microsoft Learn. There are also open-source training options that practitioners can use to freely access the information. A highly recommended Cyber Threat Intelligence self-study plan was created by Katie Nickels and is publicly accessible.[6] These options require less financial investment but are less recognizable.

Formal CTI courses require a significant financial investment. The SANS GIAC Cyber Threat Intelligence certificate is one of the most recognized certifications. The course associated with the certificate, SANS FOR578 Cyber Threat Intelligence, is highly recommended. This is the most expensive option for the practitioner. More middle range courses and certificates include the CREST and EC-Council CTIA certificates. Despite the financial commitment, these established Cyber Threat Intelligence courses and certificates are well known and are highly recognizable.

6. https://medium.com/katies-five-cents/a-cyber-threat-intelligence-self-study-plan-part-1-968b5a8daf9a

CTI is a multi-faceted discipline and requires knowledge from multiple areas of cybersecurity. Therefore, in addition to the Cyber Threat Intelligence specific courses and certifications, the practitioner may also require additional training to assist in their cyber threat intelligence work. There are specialized courses in open-source intelligence, including SANS SEC497 – Practical Open-Source Intelligence and SEC587 – Advanced OSINT Techniques. There are also specialized courses in other areas including digital forensics, and more that the practitioner can take to assist with their work in Cyber Threat Intelligence.

CTI Leaders should look at the NIST NICE Cybersecurity Workforce Framework to understand the knowledge, skills, and abilities of different cyber intelligence jobs.

- All-Source Analyst
- Threat Warning Analyst / Threat Analysis (originally in Intelligence Analysis group, now in Protection & Defense)
- Collection Manager
- Intelligence Planner
- Mission Assessment Specialist (originally in the Intelligence Analysis group, now in Cyberspace Effects)

While few teams within health sector organizations will have all these roles, the jobs are often done as collateral duties for analysts or the team manager. These expanded roles can be used as career progression opportunities for smaller teams, allowing analysts to grow their skills without having to leave a job for opportunities elsewhere. More senior analysts and managers can also use these as mentoring opportunities.

Mentorship both within and outside the organization can assist with bridging the potential skills gap. This can also assist those small teams where internal training opportunities are non-existent. Informal mentorship programs outside of the practitioner's organization can assist practitioners in developing their skills and encourage intelligence sharing with other organizations. A formalized mentorship program within organizations can assist with developing the practitioner's Cyber Threat Intelligence knowledge as well as specialized knowledge.

As shown above, structured and comprehensive training initiatives, are needed to maintain CTI expertise within organizations. Organizations have many options for training from open source and formal certifications, enabling them to select the best option to provide training to their cyber threat intelligence practitioners. Mentoring is also a key component to main CTI expertise, and can assist with intelligence sharing as well as skills development.

The CTI Program Development Working Group believes the subject of training and core competencies is worthy of deeper understanding. To start to work together as a community to dive deeper into this area and provide guidance, the Working Group has collaborated to provide a number of resources in the Feedback section of the CTI in a Box project. These resources which range from free training courses, recommended paid training and certifications for analysis, recommended core competencies for cyber threat intelligence analysts and example interview questions.

Intelligence Requirements and Stakeholders

Nearly half (46.88%) of the organizations have developed Intelligence Requirements (IRs), with an additional 31.25% seeking assistance in this area. The diverse range of IR stakeholders mentioned by respondents underscores the cross-functional nature of CTI and its importance across various organizational units.

- What are IRs?
  - An IR is a question that drives an action (decision) to enhance security and guide the analyst. It should identify and document a need for a stakeholder and what decision, action, or challenge will be influenced by the intelligence.

- Why make IRs?
  - Properly planned intelligence work can serve as a solid foundation for decisionmakers to reference when planning for upcoming and known threats alike. Utilizing the time-tested intelligence cycle of planning and direction, collection, analysis, dissemination of intelligence, and feedback, security groups can become better prepared to face various threats and crises.
  - Intelligence Requirements are questions that are used to drive collection in the cycle and inform analysts and stakeholders on what is most important to know, in order to achieve defined goals. Defining what it is that stakeholders need to know leads to defining what intelligence collection and reporting requirements a CTI team will have. Creating this clear guidance prevents analysts from wasting time and resources on information that does not meet the needs of the stakeholders.

- What makes a good IR, and how can you create your own?
  - For information to be intelligence it must be useful; for intelligence to be useful it must be actionable, relevant, timely, and accurate. In application, IR's answer questions that influence decisions. To be useful, CTI needs to understand the technology and needs of their stakeholders.
    - In a CTI stakeholder relationship, it is important to understand the tasks, priorities, and concerns of the stakeholder. Knowing more about what they do will help inform what types and styles of intelligence are most appropriate to deliver to a group.
    - Seasoned analysts recognize the importance of fostering relationships of understanding and cooperation among different teams, which can be leveraged to address issues as they arise. Internal stakeholders will have diverse risk appetites, technical skills and knowledge, operational imperatives, tools, and team cultures. Working backwards from the goals of a group can point to the questions that need answering to achieve those goals.
  - The first step in ensuring that an IR is useful is to understand the expected outcome. A useful IR spurs action for the requestor. Or, said another way, intelligence answers a question. Therefore, an IR is, typically, stated in the form of a question.
  - Good IRs generally follow these tips:
    - State the intelligence "question" clearly (example What vulnerabilities exist for technology at X company that have active exploitation in the wild?)
    - Make it answerable - avoid rabbit-holing - by keeping it from being too broad.
    - Understand the goals of the stakeholder - IRs will be different for a small team or firm, vs a large enterprise that is looking at strategic concerns. (make a stakeholder profile for them)
    - Know the stakeholders - understand their needs, risk appetite, and priorities.
    - Avoid being too specific or too broad.
    - Update IRs and review them (and stakeholder engagements) on a regular cadence (annual, twice a year are generally good)

- Examples of good and bad
  - Bad:
    - How many cyberattacks were executed by Chinese state-sponsored threat actors against the health sector in October 2024? (Too specific, and would require constant IR updates for each specific scenario)
    - What are the current cyberthreats to our organization? (Too broad)
    - Has the print server been accessed by Siberian IP addresses? (Too specific - and more of a hunt/incident response question - IRs should not be yes or no questions)

- Good:
  - What TTPs have become more popular in usage against the health sector within the past year?
  - What malware families are most likely to target this organization in the near future?
- What vulnerabilities with active exploits or proof-of-concept code exist in this environment?

Effective intelligence requirements are critical to the success of a cyber threat intelligence community of practice. They ensure that intelligence efforts are aligned with organizational goals, facilitate the timely identification and mitigation of threats, and foster collaboration and information sharing among stakeholders. By clearly defining and prioritizing these requirements, organizations can enhance their threat detection capabilities, improve decision-making processes, and ultimately strengthen their overall security posture.

Tools and Technologies

The adoption of Threat Intel Platforms (TIPs) by 62.5% of organizations indicates a growing recognition of the need for centralized threat intelligence management. The high utilization of Open Source Intelligence (OSINT) (78.12%) demonstrates a commitment to leveraging diverse information sources. However, the variety of paid intelligence services used suggests that organizations are still exploring different options to find the right mix of intelligence sources.

Threat Intelligence Platforms (TIPs)

TIPs are specialized systems designed to aggregate, analyze, and disseminate threat intelligence data to enhance an organization's cybersecurity posture. They are best utilized by integrating various data sources, enriching raw data with contextual information, and facilitating the sharing of actionable intelligence across different teams and tools. However, TIPs face challenges due to the lack of standardized capabilities. Some platforms may lack enrichment features, limiting the depth of analysis, while others may only process indicators of compromise (IOCs) from source to Security Information and Event Management (SIEM) systems, without offering comprehensive repository or library functions. This inconsistency can hinder the effectiveness of threat intelligence efforts, as organizations may struggle to find a TIP that meets all their specific needs.

Threat Intelligence Platforms (TIPs) are highly pertinent and valuable, particularly with the various Information Sharing and Analysis Centers (ISACs) providing comprehensive lists. These platforms play a crucial role in promoting the exchange of intelligence and best practices within the health sector.

Open-Source Intelligence (OSINT)

OSINT is defined as intelligence produced by collecting, evaluating and analyzing publicly available information with the purpose of answering a specific intelligence question.[7] Cyber Threat Intelligence commences with an intelligence requirement. The intelligence requirement is a question that the practitioner needs to address. 78.12% of Health-ISAC organizations surveyed report that they utilize open-source intelligence in CTI. This indicates the importance of open-source intelligence in the work of the Cyber Threat Intelligence practitioner.

The benefits of open-source intelligence in CTI include an increase of return on investment, early detection and threat identification.[8]

By utilizing open-source intelligence, the cyber threat practitioner can increase their return on investment as it is a low-cost or free option for the practitioner. By OSINT, the practitioner is able to conduct their investigation with limited financial input. Public sources are typically the first to report new threats and vulnerabilities. By monitoring open forums, news sources and social media, the practitioner can make early detections of a threat or vulnerability. OSINT may include detection and defense recommendations which can assist the practitioner in preventing future attacks and minimize the damage of an ongoing attack.

According to the survey, Feedly is the most popular aggregator in the health sector. Feedly is an aggregation application and It is an open-source Intelligence search tool. This tool can be used to provide all the above benefits discussed.

Utilizing OSINT in Cyber Threat Intelligence provides many benefits but there are challenges in CTI work. The four main challenges when using OSINT are rabbit holing, intelligence requirements, and source integrity.

First, using OSINT in CTI is “Rabbit holing”. The term “Rabbit Holing” refers to an analyst becoming too focused on the IR. This challenge can be addressed by maintaining the focus on the scope of the IR. An unambiguous IR has both stakeholders and scope. These components of the intelligence requirement limit the OSINT required and therefore help limit rabbit holing.

A second challenge when using OSINT in CTI is not adhering to the Intelligence requirements. This causes the analyst to provide irrelevant or unnecessary information. When conducting OSINT research, the Analyst should always keep the Intelligence requirements in their mind.

Third, when using OSINT in CTI is source integrity. Publicly available information can be faulty or incorrect and therefore critical analysis should be completed before using a resource.

A fourth challenge when performing OSINT in CTI is the “Kevin Bacon effect”, also known as the “six degrees of separation,” poses a significant challenge in OSINT operations. The vast interconnectedness of data as well as seemingly unrelated entities can sometimes be linked through a short chain of connections. This means that analysts often encounter an overwhelming amount of data with numerous indirect links, making it difficult to discern relevant information from noise. OSINT is a valuable tool in threat intelligence.

There are challenges to using OSINT, but by using the solutions above they can be addressed. Further utilization of open-source intelligence in the future, will continue to assist Analysts in their work in cyber threat intelligence.

7. https://www.sans.org/blog/what-is-open-source-intelligence/
8. https://library.mosse-institute.com/articles/2022/07/the-advantages-of-performing-osint-for-threat-intelligence/the-advantages-of-performing-osint-for-threat-intelligence.html

Performance Measurement

The low adoption of Key Performance Indicators (KPIs) for CTI programs (18.75%) represents a significant area for improvement. Implementing robust measurement and evaluation practices could help organizations better assess the effectiveness of their CTI initiatives and demonstrate value to stakeholders.

Key Performance Indicators (KPIs) are essential metrics that help organizations measure progress towards their strategic goals. Determining which KPIs to collect involves understanding what leadership needs to know, identifying metrics that can drive change, and pinpointing indicators that can highlight potential problems. These metrics can vary widely, encompassing technical data, stakeholder feedback, and project tracking. KPIs can be collected at various levels, whether manually, semi-automated, or fully automated. However, there are challenges in collecting KPIs, such as the time and effort required, the risk of gathering incorrect data, and the potential for creating false narratives. Different industries' CTI teams may collect a range of KPIs, tailored to their specific needs and objectives, to ensure they are effectively monitoring and improving their security posture.

The CTI Program Development Working Group intends to make Metrics and KPIs a core foundation of the 2025 Working Group additions to the CTI in a Box resource.

Recommendations

1. Maturity Enhancement: Organizations should focus on advancing their CTI Capability Maturity Model (CMM) levels by formalizing processes, integrating CTI with other security functions, and implementing continuous improvement mechanisms.

2. Collaboration and Information Sharing: Encourage increased participation in intelligence sharing initiatives, potentially by addressing legal and regulatory concerns through enhanced engagement with legal teams.

3. Training and Skill Development: Implement structured CTI analyst training programs to build and maintain expertise within the organization.

4. Intelligence Requirements: Assist organizations in developing and refining their Intelligence Requirements, ensuring alignment with stakeholder needs across various organizational units.

5. Performance Metrics: Encourage the adoption of Key Performance Indicators (KPIs) to measure CTI program effectiveness and demonstrate value to executive stakeholders.

6. Tool Optimization: Support organizations in optimizing their use of Threat Intel Platforms (TIPs) and intelligence sources to maximize the value of their CTI investments.

Conclusion

The survey results paint a picture of a health sector that recognizes the importance of Cyber Threat Intelligence but is still in the process of maturing its CTI capabilities. While executive support is strong, there are significant opportunities for improvement in several key areas. Strengthening collaboration between different teams and organizations will help facilitate the sharing of intelligence and best practices. Additionally, expanding training programs is essential to equip teams with the necessary skills and knowledge. Refining measures of performance will also help accurately assess the effectiveness of CTI initiatives. By focusing on these areas, health sector organizations can significantly improve their cyber threat intelligence programs and bolster their defenses against the ever-changing landscape of cyber threats.

The CTI Program Development Working Group members hope that by collaborating on the CTI in a Box resource, we can provide the resources, templates, assessments, guides and examples to help organizations at all levels of maturity. We believe this resource has is something for everyone in Health-ISAC! We call on others in the community to join the Working Group to continue to grow and improve on this unique and valuable resource for the Health-ISAC Community.