Version 1.3

CYBER THREAT INTELLIGENCE CAPABILITY MATURITY MODEL

Industry Inspired. Industry Led.

Contents

1. Introduction

1.1. Why Another Model

Key Concept: The CTI-CMM offers a stakeholder-first approach to CTI maturity.

The success of an effective cyber threat intelligence (CTI) program is dependent on its ability to bring value to its stakeholders. It exists to support the people who make decisions and take actions to protect your organization. To ensure stakeholders get the maximum value from utilizing CTI, it is necessary to build capabilities to support or advance their activities.

A successful program is a mature program. A mature program aligns to its organization's core objectives and key outcomes.

Unlocking the full potential of your CTI program can be challenging, requiring alignment with the capabilities of each stakeholder it supports. Alternatively, it could be that there is no dedicated CTI team and this practice is delivered through combined roles. The CTI Capability Maturity Model (CTI-CMM) is designed to support your team in building its CT capabilities by aligning to defined practices for stakeholder business units (or "domains") likely found within your organization. The goal is helping your CTI program bridge the gap with your stakeholders and mature in a way that creates impactful and demonstrable value for your organization.

1.2. Model Vision and Roadmap

Our motivation is to elevate the practice of cyber intelligence by sharing our collective knowledge and experiences. Fostering a vendor-neutral community and advancing the field for the benefit of all.

We believe any course of action (COA) should fundamentally adhere to the following values and principles.

1.2.1. Shared Values

- Intelligence provides value through collaboration with our stakeholders and supporting their decision-making process.
- Intelligence is never completed: improvement is continuous. This also applies to adoption as constant improvement is crucial for success.
- The model is not claimed by a single commercial party.

1.2.2. Shared Principles

- Contextualizing CTI within organization-specific risk.
- Continuous self-assessment and improvement.
- Actionable intelligence based on stakeholder needs.
- Quantitative and qualitative measurement of effectiveness and impact.
- Collaborative and iterative intelligence processes.

1.2.3. Model Development Roadmap

Milestone	Target	Status
Initiated the CTI-CMM project	October 2023	Complete
Defined purpose and scope of the model	November 2023	Complete
Created model development approach and objectives	December 2023	Complete
Gathered and review advisor feedback	July 2024	Complete
Conducted pilot test and external validation	July 2024	Complete
Published CTI-CMM version 1	August 2024	Complete
Publish CTI-CMM version 1.1, including • *Community feedback* • *FRAUD domain* • *Changelog* Published model assessment tool BETA	December 2024	Complete
Published v1.2 including new appendices, including: • *CTI Metrics and Measurements* • *CTI Data Source Library* • *CTI Data Source Matrix* Published model assessment tool v1.0	April 2025	Complete
Published CTI-CMM version 1.3	January 2026	Complete
Publish web-based model assessment tool	Q1 2026	In Progress
Publish model templates, guides, and samples	Q2 2026	In Progress
Publish CTI-CMM version 2.0	Q3 2026	In Progress

1.3. Intended Audience

Building CTI program maturity requires contribution and perspective from a variety of individuals representing cross-organizational teams. We believe this model can be used by the following roles:

Leadership & Key Decision-Makers

- CTI Directors and Team Leaders, individual roles or as part of larger teams (e.g., Cyber Defense Centers)
- Cybersecurity Executives and Senior Leaders

Practitioners

- CTI Analysts and Researchers
- Cybersecurity Domain Stakeholders (e.g., SOC analysts, incident responders, etc.)

1.4. Document Organization

This document supports organizations in effectively creating, refining, maturing, and maximizing the CTI program. It introduces the model and provides the main structure and content of a program.

- **Section 1:** Organizational information about this community-driven effort.
- **Section 2:** Generic background information.
- **Section 3:** Describes core competences guiding a CTI program.
- **Section 4:** Describes the structure of the CTI-CMM: Domains, Structure, and Maturity Levels.
- **Section 5:** Provides guidance on how to use the model.
- **Section 6:** Contains the model itself — the CTI Maturity Indicators by Domain.
- **Appendices:** Supporting information, references, metrics, templates, and examples.

Readers may benefit by focusing on specific sections of this document as outlined below. Beyond these recommendations, all readers may benefit from understanding the entire document.

- **Leaders and Managers:** Sections 1, 2, 3, and 4
- **Practitioners and Facilitators:** Entire document

2. Background

The CTI-CMM focuses on establishing and measuring a CTI program's capability relative to each domain's ability to service its stakeholders, growing the overall program's capacity and reach. The CTI-CMM was designed to align with industry best practices and the concepts and format of a recognized cybersecurity maturity model, the Cybersecurity Capability Maturity Model[1] (C2M2).

The C2M2 was published by the U.S. Department of Energy with contributions from experts representing a range of private and public sector organizations. It is aligned with other internationally recognized cyber standards and best practices, including the National Institute of Standards and Technology (NIST) Special Publication 800-53 and the NIST Cybersecurity Framework (CSF).

The C2M2 is designed to help measure the maturity of a cybersecurity program by focusing on the capabilities of domains found within most organizations (for example, risk management and vulnerability management). Coincidentally, the C2M2 domains represent stakeholders commonly supported by CTI programs, creating a natural reference point for the CTI-CMM to align to.

2.1. Maturity Models

The CTI-CMM addresses maturity models in a similar manner as the C2M2. A maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline. A maturity model content typically exemplifies best practices and may incorporate standards or other codes of practice of the discipline.

A maturity model thus provides a benchmark against which an organization can evaluate its current level of capability of practices, processes, and methods and set goals and priorities for improvement. Additionally, when a model is widely used in a particular industry and assessment results are anonymized and shared, organizations can benchmark their performance against other organizations. An industry can determine how well it is performing overall by examining the capability of its member organizations.

To measure progression, maturity models typically have a scale defining levels of maturity. The CTI-CMM uses a scale of maturity indicator levels (MILs) 0 to 3, which are summarized in Section 4.3. A set of attributes defines each level. If an organization demonstrates these attributes, it has achieved both that level and the capabilities that the level represents. Having measurable transition states between the levels enables an organization to use the scale to:

- Define its current state
- Determine its future, more mature state
- Identify the capabilities it must attain to reach that future state

The CTI-CMM provides both metrics (found in the appendix section) and an assessment tool designed to aid organizations in measuring their maturity.

1. Cybersecurity Capability Maturity Model (C2M2). (2022). Office of Cybersecurity, Energy Security, and Emergency Response. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

2.2. Model Development Approach

The development approach of the CTI-CMM overlaps with the C2M2 by building upon the following initial development activities:

- **Industry collaboration:** Numerous CTI practitioners from across the CTI industry participated in the development of this model, bringing a broad range of knowledge, skills, and experience to the team. This model should be considered a "living document" and will be adjusted as the industry evolves and with agreement from the collective.
- **Best practices and stakeholder alignment:** The model integrates existing cybersecurity resources and CTI best practices, guided by the evolving threat landscape, leveraged using methodologies designed to maximize CTI program maturity, and synchronized with stakeholder success.
- **Descriptive, not prescriptive:** The model was developed to provide descriptive, not prescriptive, guidance to help organizations develop and improve their CTI capabilities. The model provides guiding principles and objectives but is open to interpretation in regard to implementation. This model should be considered flexible and customizable to fit your specific operating environment.

3. Cyber Threat Intelligence Core Concepts

This section describes several core concepts that are important for interpreting the content and structure of the CTI-CMM.

3.1. Cyber Threat Intelligence

CTI is a key enabler to protect the organization and reduce risk to key assets.

CTI is a discipline focused on understanding the capabilities, intent, motivations, and opportunities of relevant cyber adversaries and their associated tactics, techniques, and procedures (TTPs). CTI insights and recommendations arm stakeholders charged with protecting an organization and reducing risk to its technologies, infrastructure, and the people dependent upon it.

CTI is the "eyes and ears" of a proactive defense and risk reduction strategy.

CTI combines several disciplines like open source intelligence (OSINT), social media intelligence (SOCMINT), human intelligence (HUMINT), technical intelligence (TECHINT), and financial intelligence (FININT) to provide continuous coverage and understanding of the cyber threat landscape. It uses the intelligence cycle to plan, collect, process, analyze, disseminate, and receive feedback on contextualized insights that answers key gaps in knowledge (also known as intelligence requirements) and provides COAs for defenders and decision-makers to protect their organization at the strategic, operational, and tactical levels.

3.2. CTI Stakeholders

Stakeholder management is a critical component of a mature CTI program.

A stakeholder is any individual, group, or organization that has an interest in or is affected by the activities, outcomes, and performance of the CTI program. A successful stakeholder management program is comprehensive and dynamic, addressing the needs and expectations of all stakeholders involved. By focusing on clear communication, regular engagement, defined roles, and continuous improvement, organizations can build strong relationships with stakeholders, ensuring that the CTI practice is actionable, relevant, timely, and aligned with broader organizational goals.

In the wider context of CTI, typical stakeholders for organizations can include a variety of internal and external entities. Each of these stakeholders has unique interests and roles in leveraging CTI to protect the organization's information assets and ensure cybersecurity. These stakeholders can be found in every layer of an organization, see 3.3.

For governmental bodies, the scope and complexity of stakeholders involved in CTI expand significantly, primarily due to the need for collaboration with other government entities and adherence to national security policies.

A more exhaustive overview of stakeholders can be found in the appendix section.

3.3. Strategic, Operational, and Tactical

Aligning efforts to strategic, operational, and tactical outcomes helps CTI programs manage and respond to cyber threats at different levels of expectation and utility across the enterprise. A CTI program's ability to affect outcomes at all three levels is a measure of its maturity.

Strategic, operational, and tactical CTI are distinct yet complementary approaches to enhancing cybersecurity in the following areas:

- **Strategic CTI** focuses on long-term planning, informing senior leadership, guiding policy development, aligning initiatives with organizational goals, producing high-level reports, and supporting risk assessments.
- **Operational CTI** supports specific campaigns, providing relevant and actionable intelligence for infrastructure, security operations, incident response, and CTI sharing with detailed reports and plans.
- **Tactical CTI** addresses immediate threats, offering real-time support to security operations, monitoring and analyzing threat data, and sharing indicators of compromise (IoCs) and attack patterns to prevent or respond to attacks.

> **Organizations may use "Strategic, Tactical, Operational" differently. This can create confusion when applying this concept to an organization. By clearly defining the way we have implemented the terminology in the CTI-CMM, we aim to create the necessary clarity. We will leverage the aforementioned definitions throughout the document.**

A more elaborate overview of the different levels, responsibilities, and typical CTI products can be found in the appendix section.

3.4. CTI Program Foundations

This section covers foundational elements of a CTI program. These foundations are by no means a guarantee for success. That said, we believe they are crucial for maturity and capability growth.

> **Future versions of the CTI-CMM aim to include comprehensive resources that cover these important foundational aspects of building a CTI program, its workforce, and architecture.**

3.4.1. CTI Program Management

CTI program management refers to the practice of building, growing, and measuring the CTI program to achieve the organization's objectives.

Purpose: Establish and maintain an enterprise CTI program that provides structured and systematic initiative designed to collect, analyze, and distribute intelligence relevant to the organization's risk and objectives. The CTI program aims to provide actionable insights that inform decision-making processes, enhance strategic planning, and improve operational efficiencies.

Execution: Establish an enterprise CTI program that creates an enduring intelligence advantage for the organization in a manner that aligns CTI objectives with both the organization's strategic objectives and the risk to high-priority assets. Ensure the program's vision and mission are aligned with and support the organization's culture and values.

> **CTI Program Management Objectives**
> **— Establish the CTI Program Strategy**
> **— Establish and Maintain the CTI Program**
> **— Establish Oversight and Governance Documentation**

3.4.2. CTI Workforce Management

CTI workforce management refers to the practice of building, growing, retaining, and maximizing the CTI program staff to accomplish its mission.

Purpose: Establish, operate, and continuously tune plans to create an effective workforce with commensurate knowledge, skills, and ability to support cyber defense and risk reduction efforts. Managing a CTI workforce entails understanding baseline team and individual capabilities; business direction; cyber defense and risk stakeholder jobs and workflows; and identifying opportunities to improve efficacy, efficiency, reach, and business continuity.

Execution: Develop a strategy and pathways to baseline, grow, and maintain expertise across the CTI program to produce consistent quality service delivery to CTI stakeholders. Ensure training needs are clearly outlined, aligned with career progression goals, and take stock of existing developmental resources prior to seeking outside opportunities.

CTI Workforce Management Objectives
- **Identify CTI Workforce Capability Requirements**
- **Improve CTI Workforce Capabilities to Fulfill Stakeholder Requirements**
- **Assign CTI Responsibilities and Growth Pathways**
- **Develop CTI Workforce at the Team and Individual Level**

3.4.3. CTI Architecture

CTI architecture refers to the organization's plan for actualizing the CTI objectives in the CTI Program Management strategy. It provides for the definition of requirements for tools and infrastructure.

Purpose: Document and maintain the structure and behavior of the organization's cybersecurity architecture, including controls, processes, technologies, and other elements commensurate with the mandate, direction, and reason why the CTI function exists.

Execution: Provide the tools and infrastructure for the CTI program and stakeholders to execute phases of the intelligence cycle (planning and direction, collection, processing, analysis and production, dissemination, and feedback). Ensure the identification and establishment of workforce automation capabilities for CTI processes and products.

CTI Architecture Objectives
- **Establish and maintain CTI architecture strategy and program**
- **Implement CTI tools and infrastructure**
- **Identify and establish automation for CTI processes and products**

3.5. Feedback

Continuous improvement loops throughout the intelligence cycle are the most significant identifier of mature teams. These loops help CTI teams align their outputs with organizational needs.

To practice what we preach, we also apply this practice to our work on the CTI-CMM. We actively solicit feedback from practitioners all over the globe, either through usage and email or feedback forms. Through our global network, we have solicited a significant amount of suggestions, adjustments, and practical steps you need to operationalize this model.

When we receive feedback, the suggestions are shared with the appropriate teams and applied changes will be tracked. We also want to acknowledge all contributors who spend their valuable time detailing specific adjustments. We truly appreciate your feedback and this means the world to us.

The changelog is maintained at the end of this document so you can also see the adjustments. In the future, we plan on recognizing contributors on our website and this document.

> **Feedback is a crucial component of any CTI program. It involves our ability to learn from successes and failures with the purpose of incremental improvement.**

4. How the Model is Organized

Similar to the C2M2, the CTI-CMM is organized into 11 domains. Each domain includes a "domain purpose" (referenced verbatim from the C2M2) followed by a "CTI mission" description describing how the CTI function supports it. Also included are CTI use cases, CTI data sources, and specific practices across progressive maturity levels that can be assessed and measured. The following is a summarized list of domains with more comprehensive coverage found in Section 6.

4.1. Domains

Table 1. Summary List of Domains and CTI Missions

Domain	Domain Purpose	CTI Mission
Asset, Change, and Configuration Management ASSET	Manage the organization's information technology (IT) and operational technology (OT) assets, including hardware, software, and information assets, commensurate with the risk to critical infrastructure and organizational objectives.	Monitor the organization's attack surface to rapidly detect at-risk assets and reduce exposures based on the current and anticipated threat landscape.
Threat and Vulnerability Management THREAT	Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities commensurate with the risk to the organization's infrastructure (such as critical, IT, and operational) and organizational objectives.	Maintain comprehensive and contemporary knowledge of the relevant evolving threat landscape to reduce the organization's risk against new and emerging adversaries, malware, vulnerabilities, and exploits.
Risk Management RISK	Establish, operate, and maintain an enterprise cyber risk management program to identify, analyze, and respond to cyber risk the organization is subject to, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.	Align CTI with the organization's risk management strategies to inform and prioritize risk reduction efforts. Improve risk decisions, assessments, and controls by identifying relevant threats and estimating likelihood and potential impact.
Identity and Access Management ACCESS	Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets commensurate with the risk to critical infrastructure and organizational objectives.	Proactively inform identity and access management (IAM) strategies, reduce incident detection times, accelerate remediation, and enable continuous improvements to safeguard critical assets and build resilience against identity-related threats.
Situational Awareness SITUATION	Establish and maintain activities and technologies to collect, monitor, analyze, alarm, report, and use operational, security, and threat information, including status and summary information from the other model domains, to establish situational awareness for both the organization's operational state and cybersecurity state.	Drive threat-informed decision-making for all stakeholders based on the current and forecasted threat landscape relative to the organization. Reduce uncertainty and increase predictability of the threat environment to create a commensurate state of security readiness.

Domain	Domain Purpose	CTI Mission
Event and Incident Response, Continuity of Operations RESPONSE	Establish and maintain plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity events and incidents and to sustain operations during cybersecurity incidents commensurate with the risk to critical infrastructure and organizational objectives.	Capture, correlate, prioritize, and enrich intrusion activity in the enterprise environment to create an advantage for incident responders and strengthen the organization's overall security posture.
Third-Party Risk Management THIRD-PARTIES	Establish and maintain controls to manage the cyber risks arising from suppliers and other third parties commensurate with the risk to critical infrastructure and organizational objectives.	Strengthen third-party risk management by continuously monitoring, detecting, assessing, and mitigating potential incidents posed by third-party vendors and suppliers. Enhance vendor risk profile evaluations and prioritization using CTI insights and recommendations.
Fraud and Abuse Management FRAUD	Shield the organization from malicious digital scams and attacks by hunting for emerging threats, sharing intelligence to strengthen defenses, and guiding response to safeguard data, finances, and reputation. This proactive shield against bad actors fosters a secure online environment for all.	Create awareness around new and emerging trends in fraud and brand protection. Detect, assess, and mitigate fraudulent activities to reduce risk against the organization's employees, customers, and brand.
CTI Workforce Management WORKFORCE	Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel commensurate with the risk to critical infrastructure and organizational objectives.	Support hardening of the human element of the organization's attack surface by enhancing workforce management initiatives with insights into adversary tactics and organization-specific risks.
Cybersecurity Architecture ARCHITECTURE	Establish and maintain the structure and behavior of the organization's cybersecurity architecture, including controls, processes, technologies, and other elements, commensurate with the risk to critical infrastructure and organizational objectives.	Support the enterprise-wide effort to develop a robust and resilient IT architecture by providing insights into cyber threats potentially targeting the organization and recommending system and information security practices designed to combat them. This should account for current and emerging threats with such recommendations to include hardening, mitigation, and remediation guidance.
CTI Program Management PROGRAM	Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with both the organization's strategic objectives and the risk to critical infrastructure.	Ensure the organization's resilience and success through a measurable CTI program that aligns strategic goals, prioritizes critical infrastructure to the organization, and fosters strong governance, planning, and collaboration.

4.2. Structure

Each domain identified in section 6 includes a list of common CTI use cases to support it. Each use case is broken down further into specific practices ordered into four progressive CTI maturity indicator levels, CTI0 (Pre-Foundational) through CTI3 (Leading). The following figure illustrates the components of a domain and how to reference a single practice.

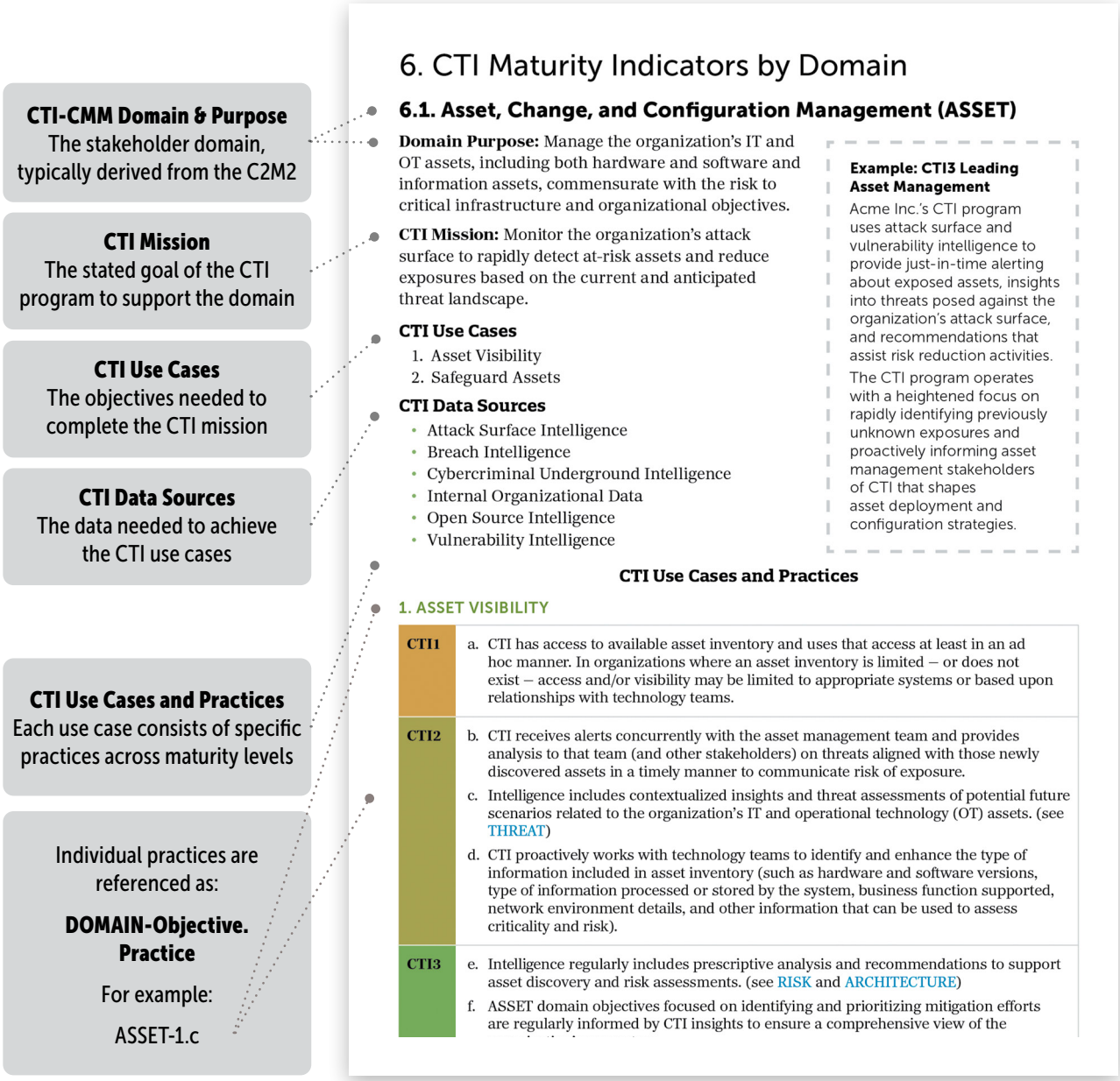

Figure 1. Breakdown of Contents

4.3. Maturity Levels

The CTI-CMM uses a maturity level structure similar to the C2M2. Individual practices are listed within each level based on their maturity level characteristics. This enables CTI programs to assess their maturity based on their ability to perform specific practices in a manner that is repeatable and consistent.

For example, in this model all practices at the CTI1 Foundational level should be basic, ad hoc, and unplanned with a focus on short-term results. The following is a summary of maturity level characteristics.

Table 2. Summary of Maturity Levels and Characteristics

Level	Characteristics
CTI0 Pre-Foundational	• No practices are performed at this level.
CTI1 Foundational	• Basic practices are performed but are mostly undocumented, ad hoc, unplanned, and response-driven. • Practices focus on reactive information that delivers short-term results supporting a subset of organizational stakeholders. • Basic usage of metrics aimed at demonstrating short-term value. Often used to track progress or effectiveness and mostly quantitative in nature, measuring throughput or level of effort, leading to limited measurable value to the CTI program.
CTI2 Advanced	• Advanced practices are performed at a higher level than CTI1. • Practices are mostly documented, planned, and standardized, with repeatable and consistent results, using automation at scale. • Practices focus on proactive and predictive intelligence that delivers short- and intermediate-term results influencing a larger number of organizational stakeholders. • Usage of metrics improved based on stakeholder feedback. Metrics include at least a subset of qualitative measurements demonstrating how the CTI program impacts most of its stakeholders, leading to moderately measurable value to the program and overall business.
CTI3 Leading	• Leading practices are performed at a higher level than CTI2. • Practices include a focus on prescriptive approach and recommendations that deliver long-term strategic results. • Practices are measurable and aligned to business outcomes. • Practices are well standardized, cross-functional, and focus on continuous improvement that drive strategic decisions and actions. • Metrics captured explicitly map to future actions designed to improve CTI operations. Metrics include both quantitative and qualitative measurements, intended to capture outcomes outlined in internal documentation that is transparent to cybersecurity and risk leadership and partners. These measurements are reported and analyzed routinely to assess the effectiveness of the CTI program.

5. How to Use This Model

The CTI-CMM is meant to be used as a reference model for continuously evaluating the CTI program, elevating maturity to the desired ambition level. The CTI-CMM levels are broken down further in individual chapters. This breakdown allows teams to effectively demonstrate the state of their use cases and practices, while allowing them to develop a profound growth roadmap.

To integrate activities with current CTI program management, we recommend using a five-step process. This approach ensures teams continuously measure and demonstrate the value and growth of their CTI program.

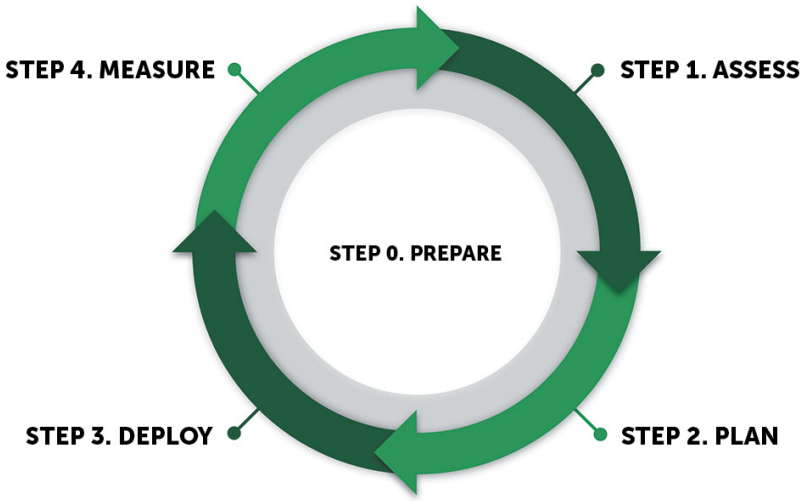

Figure 2. CTI-CMM Implementation Process

5.1. Step 0: Prepare

Before starting your journey of using the CTI-CMM, you must recognize this model is a means to an end. The model provides a frame of reference to understand the current maturity of your program. The future maturity of your program is dependent on the appetite and ambition of your organization. This model provides the direction for establishing the management of your CTI program.

We identified three key discussions to guide practitioners toward successful use of this model:

Stakeholder Engagement

As with building any function or capability, you must start with understanding why you are doing this and who it is actually for. This might seem obvious, but in practice this is often discussed implicitly instead of explicitly.

Within the context of a CTI function, we often talk about stakeholders. Stakeholders could be one or multiple individuals responsible for a specific function or domain (as identified in this model) the CTI function supports. Examples include the detection engineering lead, incident response teams, or the VP of corporate security. A more exhaustive list of stakeholders can be found in the appendix section.

Engaging stakeholders refers to the CTI function establishing a relationship with the designated individuals. This includes understanding their key questions, concerns, or needs so the function can deliver accordingly.

To help guide this discussion, we recommend clarifying these questions:

You are starting a new program	• Who are the key stakeholders we need to engage with? • What are their reporting requirements? • What is their definition of both success and value as they relate to the CTI program?
You are evaluating an existing program	• Are we still engaging with, and reporting to, the right stakeholders? • Is the current reporting structure still sufficient for the stakeholder or do there need to be changes? • Do the current definitions of success and value from the stakeholder still align with practice?

Setting Ambitions

Once you identify your stakeholders and determine their definition of success, the next step is establishing direction regarding their ambitions. These ambitions typically are intangible, such as "build us an industry-leading CTI program."

At this stage, you do not yet understand enough about the organization to quickly translate this into actions. This is where the CTI-CMM can be leveraged to provide more detailed actions that support the realization of this ambition.

To help guide this discussion, we recommend clarifying these questions:

You are starting a new program	• With that definition of success, what would be the ideal end state of our CTI program according to you? • Within what time frame would we like to have this realized? • Which existing strategic projects, programs, or initiatives does this ambition contribute to?
You are evaluating an existing program	• Is the defined end state of our CTI program still in line with practice? • Is the defined time frame still realistic? Do we need to re-prioritize activities? • Are our efforts still contributing to the organization's overall strategic projects, programs, or initiatives?

Your CTI Program Plan

Now you have sufficient information to establish the purpose of your CTI program. The next step is to leverage the CTI-CMM to identify exact actions to develop a tangible plan while clearly mapping to time, people, and cost.

Your plan also should integrate with existing projects, programs, or initiatives as much as possible. This could include tracking and reporting activities and results in commonly used project tracking tools. Considering this will enable better reporting on the overall value contribution of your CTI program to the organization.

To help guide this discussion, we recommend clarifying these questions:

You are starting a new program	• Of our key stakeholders, who needs to approve our plan? • Where should we track and report existing activities for the CTI program? • What would be ideal meeting cycles to periodically inform our stakeholders?
You are evaluating an existing program	• Does our current plan need revisioning? • Is our current method of tracking and reporting still adequate? • Is our current cycle of meeting with stakeholders still adequate?

Future versions of the CTI-CMM aim to include resources such as program plan guides, templates, and samples to help you in this important journey. Please send us feedback on the requirements you might need.

5.2. Step 1: Assess

Perform a self-evaluation to assess the implementation of CTI program practices for each domain. For simplicity and uniformity, the CTI-CMM uses the same measurement criteria and format as the C2M2. We also provide a self-assessment tool on our GitHub page designed to aid organizations in baselining their CTI stakeholder support.

Responses are selected from a four-point scale:

Table 3. Self Evaluation Response Options

Fully Implemented	Complete
Largely Implemented	Complete, but with a recognized opportunity for improvement
Partially Implemented	Incomplete; there are multiple opportunities for improvement
Not Implemented	Absent; the practice is not performed by the organization

When performing a self-assessment it is recommended to be critical about your responses. Should there be a discrepancy that forces you to choose between a higher or lower implementation score, we recommend using the lower score. In practice this is often more aligned with reality, while also providing your function areas of improvement in the next step(s).

The results provide two viewpoints your team can leverage to understand the level of maturity:

1. **Domain Specific:** What is the CTI program's maturity level relative to each security or risk domain (for example, Risk Management)?
2. **Enterprise Wide:** What is the overall CTI program's maturity level across the entire organization by aggregating and weighting each domain-specific CTI maturity level into a single score?

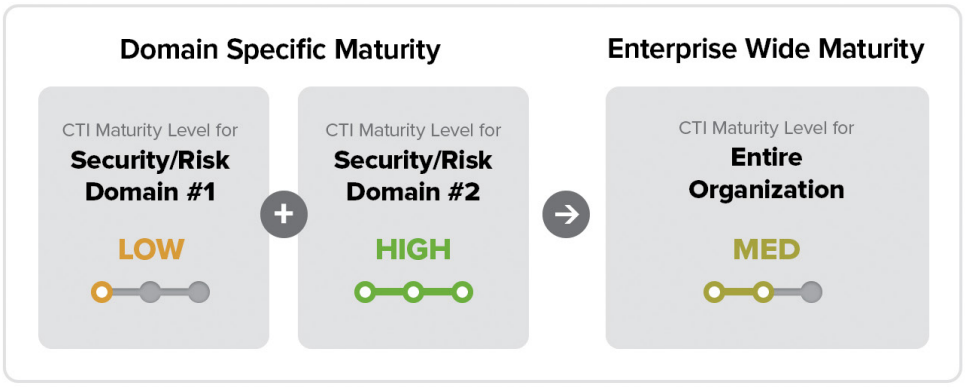

Figure 3. Domain-Specific and Enterprise Maturity Level Relationship

The authors have seen a variety of models develop various assessment tools over the years. This has resulted in a myriad of options, each representing a different lens to the current state. Instead of creating yet another fillable spreadsheet file, the authors decided to leave the exact requirements to the community. Future versions of the CTI-CMM will include an assessment tool to expedite the process of evaluating your program and generate relevant results you can take action on. Please send us feedback on the requirements you might need for an assessment tool.

5.3. Step 2: Plan

Chart a progressive path to improve the CTI program's capabilities to achieve the value expected in support of each individual domain and across the organization as a whole.

While this greatly differs per organization, we noted the following considerations to help you determine if your plan contains the right elements:

You are starting a new program	• Which domains do we deem as strong or of high priority for our organization? • Which domains do we consider areas of improvement? • Which domains can we make the most progress in over the next 90 days? • Did we correlate and align activities with pre-existing strategic information from our organization, business representatives, and (cybersecurity) executives? • Did we structure our plan according to timing requirements specific to our organization (e.g., sprints, quarters, fiscal years)? • Does our plan contain clear descriptions of activities and their subsequent value proposition? • Does our plan already highlight how success can be measured, both short and long term?
You are evaluating an existing program	• What domain-specific activities did not make the expected progress and why in the last 12 months? • Which domains do we consider as strong for our organization right now? How does this compare to the last measurement?

- Which domains do we consider as areas of improvement? How does this compare to the last measurement?
- Which domains can we make the most progress in over the next 90 days? How does this compare to the last measurement?
- Did we correlate and align activities with pre-existing strategic information from our organization, business representatives, and (cybersecurity) executives?
- Did we structure our plan according to timing requirements specific to our organization (e.g., sprints, quarters, fiscal years)?
- Does our plan contain clear descriptions of activities and their subsequent value proposition?
- Does our plan already highlight how success can be measured, both short and long term?

5.4. Step 3: Deploy

Execute your plan by prioritizing deployment and execution of resources to enable CTI program capability growth (for example, vendor solutions, data feeds, and staffing requirements). This means taking action on your plan by deploying resources and working with stakeholders to achieve your maturity growth goals.

The most important aspect of this step is conscious decision-making when executing your plan. When establishing and working in CTI programs, the authors regularly found most priority decisions to be made implicitly. This potentially creates an environment based on assumptions, which is never ideal, especially if you intend to measure your successes year-on-year. Discuss priority options with your leadership team, document decisions and outcomes in writing, and be flexible enough to adjust your plan as you move forward in the execution phase.

This stage is especially important for teams starting a new program, as their success during the first 90 days of execution regularly forms the opinion of key stakeholders about the value the CTI program provides now and into the future.

5.5. Step 4: Measure

Once resources are deployed based on the priorities of your plan, you may be tempted to proceed to business as usual. However, it would be better to continuously monitor and assess the CTI program's maturity level proportionate to the capabilities of each individual domain it supports. The CTI-CMM self-assessment tool and proposed metrics in the appendix section can assist with benchmarking and growth measures.

Based on the authors' experience, we identified several key questions we believe each CTI program participant should ask themselves on a routine basis:

Key questions	• Is the CTI program providing measurable value to the organization? • Is the CTI program delivering on the prioritized areas?

Supporting questions	• How are we currently demonstrating our value? What can we adjust to demonstrate this more effectively or efficiently? • Which areas have not been performing as expected? What options do we have to improve this? What do we need to make this happen? • Which decisions do we have to bring to leadership to increase the effectiveness or efficiency of our CTI program?

Should all the key questions be answered with "yes," the CTI program is progressing as expected.

Should answers be "no" or "uncertain", this provides opportunity for feedback, learning, or readjustment of priorities. Contextual questions support clarification of where support is needed.

Once the designated time cycle as defined in Step 0 and Step 1 completes, you start the complete cycle again.

6. CTI Maturity Indicators by Domain

6.1. Asset, Change, and Configuration Management (ASSET)

Domain Purpose: Manage the organization's IT and OT assets, including both hardware and software and information assets, commensurate with the risk to critical infrastructure and organizational objectives.

CTI Mission: Monitor the organization's attack surface to rapidly detect at-risk assets and reduce exposures based on the current and anticipated threat landscape.

CTI Use Cases

1. Asset Visibility
2. Safeguard Assets

CTI Data Sources

- Attack Surface Intelligence
- Breach Intelligence
- Cybercriminal Underground Intelligence
- Internal Organizational Data
- Open Source Intelligence
- Vulnerability Intelligence

Example: CTI3 Leading Asset Management

Acme Inc.'s CTI program uses attack surface and vulnerability intelligence to provide just-in-time alerting about exposed assets, insights into threats posed against the organization's attack surface, and recommendations that assist risk reduction activities.

The CTI program operates with a heightened focus on rapidly identifying previously unknown exposures and proactively informing asset management stakeholders of CTI that shapes asset deployment and configuration strategies.

CTI Use Cases and Practices

1. ASSET VISIBILITY

CTI1	a. CTI has access to available asset inventory and uses that access at least in an ad hoc manner. In organizations where an asset inventory is limited – or does not exist – access and/or visibility may be limited to appropriate systems or based upon relationships with technology teams.
CTI2	b. CTI receives alerts concurrently with the asset management team and provides analysis to that team (and other stakeholders) on threats aligned with those newly discovered assets in a timely manner to communicate risk of exposure. c. Intelligence includes contextualized insights and threat assessments of potential future scenarios related to the organization's IT and operational technology (OT) assets. (see THREAT) d. CTI proactively works with technology teams to identify and enhance the type of information included in asset inventory (such as hardware and software versions, type of information processed or stored by the system, business function supported, network environment details, and other information that can be used to assess criticality and risk).
CTI3	e. Intelligence regularly includes prescriptive analysis and recommendations to support asset discovery and risk assessments. (see RISK and ARCHITECTURE) f. ASSET domain objectives focused on identifying and prioritizing mitigation efforts are regularly informed by CTI insights to ensure a comprehensive view of the organization's ecosystem.

2. SAFEGUARD ASSETS

CTI1	a. CTI maintains an understanding of "crown jewels assets" informed based on potential to disrupt business operations and cyber threat landscape trends. This prioritization is based on asset targeting, criticality, vulnerability, and potential impact in case of attack or exposure. b. CTI maintains regular visibility into changes in the cyber threat landscape, triaging intelligence sources to determine relevance and relative impact of newly discovered threat campaigns and vulnerabilities affecting organizational assets. (see THREAT)
CTI2	c. Intelligence supports proactive risk mitigation efforts by providing contextualized insights, predictive assessments, and alerting about threats and vulnerabilities that could affect priority assets. d. Intelligence identifies vulnerabilities that directly affect priority assets, allowing the organization to prioritize patching efforts. (see THREAT)
CTI3	e. CTI includes prescriptive threat analysis and recommendations to protect current and pre-deployed assets and change configurations based on the threat environment. f. ASSET domain risk reduction strategies are consistently informed by CTI insights. g. CTI is consulted as part of the asset purchase cycle and provides insights to the organization about potential risks (e.g., specific hardware, software, or products that have been targeted in the past).

6.2. Threat and Vulnerability Management (THREAT)

Domain Purpose: Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities commensurate with the risk to the organization's infrastructure (such as critical, IT, and operational) and organizational objectives.

CTI Mission: Maintain comprehensive and contemporary knowledge of the relevant evolving threat landscape to reduce the organization's risk against new and emerging adversaries, malware, vulnerabilities, and exploits.

CTI Use Cases

1. Enhance Attack Prevention and Preparedness
2. Drive Detection Engineering Improvements and Strategy
3. Enhance Threat Hunting
4. Inform Offensive Security Operations
5. Improve Patch Prioritization

CTI Data Sources

- Adversary Intelligence
- Attack Surface Intelligence
- Breach Intelligence
- Cybercriminal Underground Intelligence
- Internal Organizational Data
- Malware Intelligence
- Open Source Intelligence
- Vulnerability Intelligence

Example: CTI3 Leading Patch Prioritization and Purple Teaming

Acme Inc.'s CTI program routinely delivers alerts that prescribe relevant patching guidance and mitigation opportunities based on the probability of exploitation and intent for actors in Acme's threat profile.

The CTI program developed and regularly updates a threat profile containing a prioritized list of threat actor groups, adversary tools, and TTPs relevant to Acme's sector and operating locations. The program regularly surfaces intelligence related to new and emerging behaviors linked to threats in the profile and provides alerts to the offensive security programs who use the intelligence to inform assessments against existing controls and methods for reinforcing those controls or closing gaps, respectively.

Threat insights contain high levels of contextualization, including code/procedural-level details that enhance threat hunting, precise recreation of observed behavior by the offensive security team and development of relevant detections by the security engineering team.

CTI Use Cases and Practices

1. ENHANCE ATTACK PREVENTION AND PREPAREDNESS

CTI1	a. Indicators of compromise/behavior/attack (IoC/B/As) are collected from external threat reports and delivered to security operations teams at least in an ad hoc manner (e.g., over email) to support prevention and blocking. b. Reduction of false positives is supported at least in an ad hoc manner when identified. c. Ongoing collection of IoC/B/As is pruned at least in an ad hoc manner or based upon default platform (TIP, security information and event management (SIEM), etc.) expiration parameters.

CTI2	d. IoC/B/As are collected from external feeds (usually contextualized by specific types of threats, e.g., phishing hosts, botnets, command-and-control (C2) hosts) and delivered directly to security technologies (e.g., SIEM or firewall solutions) in a mostly automated fashion. e. Collection of IoC/B/As is automatically ingested and pruned based upon a defined strategy that considers enterprise-specific characteristics, operational factors, and threat profile. Polling frequency occurs on a regular cadence. f. Available threat context (e.g., type of threat, attack stage) also is provided to aid operator awareness, typically reliant on source materials as ground truth.
CTI3	g. IoC/B/As are collected at scale from external feeds covering most types of threats (e.g., phishing infrastructure, botnets, C2 hosts) and delivered directly to relevant security technologies automatically. h. False positives are measured and fidelity is refined. Focus is on increasing the quality of IoC/B/As collected. i. Threat context, based on internal ecosystem knowledge versus reliance solely on source material scoring (e.g., type of threat, attack stage, detection time stamps, impact for relevance), is provided for most indicators to aid operator awareness. j. Ingested high-confidence indicators are integrated to aid in proactive defense activities. For example, adding to automation playbooks and triggering COAs where relevant (e.g., automating implementation of low-regret blocking or phishing response). k. Original indicators are correlated with internal event data (e.g., SOC/incident response (IR) investigations), actioned elsewhere within the organization (e.g., via threat hunting), and may also be shared externally.

2. DRIVE DETECTION ENGINEERING IMPROVEMENTS AND STRATEGY

CTI1	a. Alerts about adversaries actively posing potential threats to the organization are delivered at least in an ad hoc manner to support new detection logic.
CTI2	b. Threat profiling is routinely developed to support gap analysis activities and prioritize detection controls based on relevant threats against the organization. c. Continuous detection engineering improvements are supported by requests for information (RFIs) for CTI about specific gaps and vulnerabilities.
CTI3	d. Threat modeling is routinely developed to identify and contextualize priority threats relevant to the organization. e. CTI products regularly drive detection opportunities based on threat modeling, event logs, and external reporting.

3. ENHANCE THREAT HUNTING

CTI1	a. Alerts about emerging atomic indicators are provided to generate awareness and reactive hunt operations at least in an ad hoc manner with minimal contextualization using open sources. b. Threat hunts are prioritized manually based on emerging reporting of threat or vulnerability risks.
CTI2	c. Threat hunt operations are routinely informed by intelligence about threat actor TTPs and behaviors, contextualized using open and commercial sources.

	d. Threat hunts are continuously prioritized based on priority intelligence requirements (PIRs) and vulnerabilities against critical assets.
CTI3	e. Threat hunting methodologies are used to generate RFIs and provide context for new, original threat hunting hypotheses/abstracts (see the TaHiTI Threat Hunting Methodology[2] for further details).

4. INFORM OFFENSIVE SECURITY OPERATIONS

CTI1	a. Alerts about emerging tactics, techniques, and exploit campaigns are tested at least in an ad hoc manner with limited contextualization using open sources.
CTI2	b. Insights about novel techniques, procedures, and technical exploits, typically derived from open or commercial sources, are provided regularly to inform relevant offensive security operations. c. Intelligence is typically focused on threats pertaining to the organization's unique threat profile and provided with contextualization and/or code that enables replication of reported behaviors.
CTI3	d. Alerts about new and emerging attack procedures and technical exploits are delivered regularly and typically contain enough context to enable precise recreation of observed behaviors. e. Insights focus on threats pertaining to the organization's unique threat profile but also novel procedures that may not yet be actively exploited in the wild (e.g., new exploits published on code repositories or acquired via closed sources such as underground forums). f. Offensive security operations based on threat reporting inform ad hoc collection for missing context and discovered gaps are mitigated for threat prevention.

5. IMPROVE PATCH PRIORITIZATION

CTI1	a. Alerts are provided at least in an ad hoc manner for critical vulnerabilities that are experiencing viral popularity in mainstream open sources.
CTI2	b. Vulnerability management is consistently informed in a repeatable manner for critical and high vulnerabilities that are seeing viral popularity in mainstream open and cybercriminal underground sources. c. Patch prioritization is influenced by availability of PoC code, observed active exploitation, and sought-after interest by adversaries observed in the dark or surface web.
CTI3	d. Patch management is consistently driven by routine CTI products that prescribe key patches or mitigations that need to be implemented based on the probability of exploitation against the enterprise.

2 van Os, Rob, and Marcus Bakker. Tahiti: A Threat Hunting Methodology, www.betaalvereniging.nl/wp-content/uploads/TaHiTI-Threat-Hunting-Methodology-whitepaper.pdf. Accessed 26 Mar. 2024.

6.3. Risk Management (RISK)

Domain Purpose: Establish, operate, and maintain an enterprise cyber risk management program to identify, analyze, and respond to cyber risk the organization is subject to, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.

CTI Mission: Align CTI with the organization's risk management strategies to inform and prioritize risk reduction efforts. Improve risk decisions, assessments, and security control tuning by identifying relevant cyber threat activities, impact potential, likelihood of occurrence, and mitigation options for use in risk assessments.

CTI Use Cases

1. Align CTI Practices to Risk Management Strategies
2. Improve Risk Decisions, Assessments, and Controls

CTI Data Sources

- Attack Surface Intelligence
- Breach Intelligence
- Cybercriminal Underground Intelligence
- Geopolitical Intelligence
- Identity Intelligence
- Internal Organizational Data
- Open Source Intelligence
- Vulnerability Intelligence

Example: CTI3 Leading Risk Management

Acme Inc.'s CTI team possesses an in-depth understanding of the company's risk management strategy, which enhances the risk department's ability to align emerging threats with corresponding risks effectively.

The CTI team leverages both open and commercial sources to gather comprehensive CTI, to build a Cyber Threat Profile to rank ordering priority threat groups and threat trends. They leverage insights on vulnerabilities, cybercriminal underground activities, breach events, attack surface intelligence, and identity intelligence. This intelligence facilitates the swift identification, triage, and correlation of new threats to relevant risks. Consequently, this enables the risk department to accurately assess impacts, align with Acme's risk appetite, and implement appropriate controls.

CTI Use Cases and Practices

1. ALIGN CTI PRACTICES TO RISK MANAGEMENT STRATEGIES

CTI1	a. The main risks to the organization are understood and their relation to the risk management strategy, at least in a basic manner. b. Collaboration with risk management stakeholders is conducted in an ad hoc manner.
CTI2	c. CTI practices have a focused alignment to the organization's risk management strategy and framework, aligning inclusion of risk assessment (such as through the use of Binary Risk Analysis[3]) within CTI products. d. Meetings and engagements between CTI and risk management teams occur regularly. e. CTI practices influence proactive adjustments to risk management strategies.
CTI3	f. CTI practices adhere to the risk framework adopted by the organization, such as NIST 800-30[4] and the NIST Cybersecurity Framework.[5]

3 https://binary.protect.io
4 https://csrc.nist.gov/pubs/sp/800/30/r1/final
5 https://www.nist.gov/cyberframework

	g. CTI insights are used to prioritize risk-based decisions and actions based upon the threat landscape (sometimes called a Cyber Threat Profile). If possible, risks identified from CTI insights are integrated into risk management dashboards. (see ARCHITECTURE) h. CTI establishes ongoing alignment with risk management strategies with a focus on enhancing processes through automation. (see PROGRAM)

2. IMPROVE RISK DECISIONS, ASSESSMENTS, AND CONTROLS

CTI1	a. Threats are identified, assessed, and prioritized at least in an ad hoc manner and often without alignment to the organization's risk management strategy. (see THREAT) b. CTI has a basic understanding of organizational assets, controls, operating environment, and risk posture. c. CTI insights are available to support risk assessments at least in an ad hoc manner.
CTI2	d. A process for integrating CTI into risk assessments is created and used to inform basic risk controls and mitigations efforts. e. CTI insights are regularly leveraged within risk assessments. f. Risk-based controls are intermittently assessed and adjusted using CTI insights.
CTI3	g. CTI practices provide proactive guidance for risk mitigation and management, including scenario planning and simulations. (see SITUATION) h. Risk-based controls and decision-making processes are periodically evaluated and refined on an ongoing basis through the collaboration with CTI.

6.4. Identity and Access Management (ACCESS)

Domain Purpose: Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets commensurate with the risk to critical infrastructure and organizational objectives.

CTI Mission: Proactively inform IAM strategies, reduce incident detection times, accelerate remediation, and enable continuous improvements to safeguard critical assets and build resilience against identity-related threats.

CTI Use Cases

1. Accelerate Remediation of Identity-Related Threats
2. Fortify Identity and Access Protection

CTI Data Sources

- Attack Surface Intelligence
- Breach Intelligence
- Cybercriminal Underground Intelligence
- Identity Intelligence
- Vulnerability Intelligence

Example: CTI3 Leading Identity and Access Management

Acme Inc.'s CTI team uses open and commercial sources to collect identity-related threat information including compromised credentials of employees, customers, and third parties. Alerts for newly discovered credentials are rapidly processed, triaged, and remediated through automated workflows to seamlessly reset passwords and disable accounts.

Acme's CTI team relies on commercial CTI vendors to understand the prevalence of identity-related threats, including trends about prolific information-stealing malware and the underground economy that proliferates stolen credentials. Acme contextualizes these insights relative to its organization and provides predictive assessments that drive proactive IAM strategies including improvements for multifactor authentication (MFA) enforcements, password policies, and more.

CTI Use Cases and Practices

1. ACCELERATE REMEDIATION OF IDENTITY-RELATED THREATS

CTI1	a. Alerts about leaked or compromised credentials and identities from open and commercial sources are collected and reviewed at least in an ad hoc manner. b. Alerts about vulnerabilities impacting identity-related systems that threaten unauthorized access or identity compromise are collected and reviewed at least in an ad hoc manner for patch prioritization. (see THREAT)
CTI2	c. CTI assists with integration and automation of alert dissemination into repeatable workflows for ACCESS domain rapid assessment and response. d. Intelligence and associated indicators, related to emerging malware targeting identities and identity systems is delivered to enhance early warning detections and proactive mitigation measures.
CTI3	e. Continuous monitoring is extended to identity-related threats posed by third parties. (see THIRD-PARTIES) f. Intelligence on emerging threat actor TTPs is used for detecting anomalous activities related to user accounts, login attempts, or access patterns that may signal identity compromise.

	g. Intelligence includes contextualized insights and threat assessments to continuously improve identity-related discovery practices and predict future scenarios to enhance detections. h. Mitigations and remediations in response to leaked compromised credentials and identities are acted upon as part of an automated process that can be invoked. i. Mechanisms are in place to action containment of users with access due to intelligence relating to suspected compromise of controlled data.

2. FORTIFY IDENTITY AND ACCESS PROTECTION

CTI1	a. CTI maintains basic awareness and monitoring of identity-related threats to logical and physical access controls — including vulnerability exploitations and security control configurations — that lead to immediate COAs. b. Collection is focused primarily on identity-related threats relevant specifically to the organization.
CTI2	c. CTI maintains a comprehensive understanding of identity-related threats to logical and physical access controls relevant to the organization's high-risk assets. (see ASSET and RISK) d. CTI insights regularly influence proactive adjustments to enhance access control requirements and thresholds based on the threat environment, including MFA strategies and password resets. e. Collection is extended to focus on identity-related threats relevant to the organization's industry and geographic representation. (see SITUATION)
CTI3	f. CTI insights regularly inform the creation of threat scenarios and simulations to test, validate, and adjust authentication and access controls and mitigations. (see THREAT) g. CTI insights inform tabletop exercises that fortify response and mitigation efforts across the organization. (see PROGRAM)

6.5. Situational Awareness (SITUATION)

Domain Purpose: Establish and maintain activities and technologies to collect, monitor, analyze, alarm, report, and use operational, security, and threat information, including status and summary information from the other model domains, to establish situational awareness for both the organization's operational state and cybersecurity state.

CTI Mission: Drive threat-informed decision-making for all stakeholders based on the current and forecast threat landscape relative to the organization. Reduce uncertainty and increase predictability of the threat environment to create a commensurate state of security readiness.

CTI Use Cases

1. Maintain Comprehensive Understanding of the Cyber Threat Landscape

CTI Data Sources

- Adversary Intelligence
- Cybercriminal Underground Intelligence
- Geopolitical Intelligence
- Internal Organizational Data
- Open Source Intelligence
- Trust Groups

Example: CTI3 Leading Situational Awareness

Acme fuses information from multiple sources including open source news feeds, information sharing and analysis center (ISAC) partners, industry trust groups, commercial CTI vendors, and current events within the organization — including merger and acquisition (M&A) activity and IT operations updates — to maintain a comprehensive understanding of the threat environment and the risk to the organization's most critical assets.

Acme Inc.'s CTI team uses a structured approach to deliver a monthly and quarterly cyber threat landscape (CTL) report to enterprise stakeholders and the chief information security officer (CISO), respectively. These CTL reports outline key observations and recommendations for the organization to protect itself against emerging threats.

CTI Use Cases and Practices

1. MAINTAIN COMPREHENSIVE UNDERSTANDING OF THE CYBER THREAT LANDSCAPE

CTI1	a. Situational awareness alerts and updates are collected from open and trusted sources. b. Insights are provided at least in an ad hoc manner for short-term trends and observations that lead to immediate courses of action (COAs). c. Collection is focused primarily on all threats relevant specifically to the organization. (see THREAT)
CTI2	d. A systematic process, such as the one described in the ENISA Cybersecurity Threat Landscape Methodology,[6] is implemented to routinely produce CTL reports. (see THREAT) e. The CTL scope is mostly tactical and operational, delivering insights that provide short- to medium-term results. The audience and dissemination is to most enterprise stakeholder domains. The focus is primarily on priority threats and trends specific to the organization. CTL leverages priority intelligence requirements (PIRs) focused on tactical and operational needs.

6 European Union Agency for Cybersecurity (ENISA), Cybersecurity Threat Landscape Methodology (ENISA, 2022),https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology/@@download/fullReport

	f. CTI develops the baseline for return on investment and cost-benefit analysis between sources and products.
CTI3	g. The CTL scope is extended to include deliverables that regularly provide actionable intelligence to inform long-term strategic decision-making and align with risk reduction strategies. The audience and dissemination is to all enterprise stakeholder domains based on PIRs. The focus is extended to include threats, events, and trends relevant to the organization's industry and geographic representation. (see RISK, PROGRAM and THREAT) h. CTI routinely validates sources, tracks impact, and engages in return on investment reviews for all sources leveraged.

6.6. Event and Incident Response, Continuity of Operations (RESPONSE)

Domain Purpose: Establish and maintain plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity events and incidents and to sustain operations during cybersecurity incidents commensurate with the risk to critical infrastructure and organizational objectives.

CTI Mission: Capture, correlate, prioritize, and enrich intrusion activity in the enterprise environment to create an intelligence advantage for incident responders and strengthen the organization's overall security posture.

CTI Use Cases

1. Strengthen Pre-Incident Preparedness
2. Improve Incident Analysis and Response
3. Enhance Post-Incident Recovery and Continuity of Operations

CTI Data Sources

- Adversary Intelligence
- Attack Surface Intelligence
- Breach Intelligence
- Identity Intelligence
- Internal Organizational Data
- Malware Intelligence
- Open Source Intelligence
- Vulnerability Intelligence
- Counter Intelligence
- Trust Groups

Example: CTI3 Leading Event and Incident Response, Continuity of Operations

Acme Inc.'s incident response team is actively addressing a suspected breach of the company's systems. The CTI team has been instrumental in preparation, providing insights into potential threats and attack vectors. Acme established a forensic readiness program and IR runbooks based on the CTI team's input to enhance preparedness for such incidents.

Throughout the incident, Acme's CTI team is deeply involved using standard intelligence tools. It guides the IR lifecycle phases, supporting responders by enhancing IR findings, delivering real-time updates on threat actors and their TTPs, and facilitating the discovery of the root cause and the effective deployment of countermeasures.

Post-incident, Acme's CTI team continues to assist responders during reporting and evaluation phases. This process helps Acme gain a comprehensive understanding of the incident, update IR runbooks and playbooks, and strengthen its cybersecurity defenses.

CTI Use Cases and Practices

1. STRENGTHEN PRE-INCIDENT PREPAREDNESS

CTI1	a. Event and incident data is collected for correlation with external open and trusted sources to enable detection and manual remediation of threats. b. CTI insights and context are provided at least in an ad hoc manner to enrich event data, reduce false positives, and hasten response.
CTI2	c. The IR team swiftly enhances detected events through automated integration of CTI insights on threat actors, TTPs, enriched IOCs, and contextual information, significantly boosting response efficiency. d. CTI insights are used for immediate control gap detection analysis and rapid remediation, conducted in a mostly automated manner.

CTI3	e. CTI outputs (reports, alerts, enrichments) include assessments of the threat landscape and prescriptive recommendations to enable proactive detection controls and event response prioritization. (see SITUATION) f. Tabletop and scenario exercises are informed by CTI insights of the latest malware, campaigns, vulnerabilities, and threats. (see RISK)

2. IMPROVE INCIDENT ANALYSIS AND RESPONSE

CTI1	a. Incident details are reviewed and mapped to a cyber kill chain or related industry framework (e.g., Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK, the Diamond Model of Intrusion Analysis, etc.). b. Findings are documented as the incident progresses through the lifecycle phases. CTI insights are incorporated into the IR report. c. Manual research and pivoting on TTPs and IoCs is being conducted to contextualize incidents and improve remediation, at least in an ad hoc manner.
CTI2	d. Findings are documented in a stand-alone CTI report and can be incorporated into or accompany the IR report. e. Automation, which may include the use of machine learning or AI models, is used to enrich discovered indicators and map findings to cyber kill chains.
CTI3	f. Incident IoCs and related intelligence are ingested into a threat intelligence platform (TIP), using automation that maintains mapping verbosity to industry frameworks within the TIP's ontology. This empowers orchestration to existing security controls for added enrichment and actions by appropriate controls teams. g. Automation and process tools are used to trigger CTI analysis and escalation to the IR team. h. Risk-based assessments and recommendations are routinely conveyed to the IR team. (see RISK)

3. ENHANCE POST-INCIDENT RECOVERY AND CONTINUITY OF OPERATIONS

CTI1	a. Incident findings, lessons learned, and improvement opportunities are captured within an internal knowledge base or ticket. Post-mortems are discussed internally and briefed to leadership at least in an ad hoc manner. b. Manual ingestion and enrichment of intelligence, SOC internal indicators, and data occurs. c. Partnership with the threat hunting team is initiated for ongoing collaboration. (see THREAT)
CTI2	d. Incident findings and lessons learned are regularly reviewed to spot trends and enhance security recommendations. Key insights are shared with leadership through briefings that emphasize the risks of inaction. e. Incident response time is minimized through automation, implementing key prevention measures that utilize IoCs and TTPs from trusted sources. Automated CTI runbooks facilitate intelligence and event enrichment. f. CTI maps enrich TTP findings from incident investigations by mapping them to the MITRE ATT&CK framework, allowing control teams to assess them against existing detection and prevention capabilities. Additionally, the enrichment of SOC internal indicators and data with intelligence is ongoing through TIP or automation.

CTI3	g. Artificial intelligence (AI) and machine learning (ML) are used for analysis of TTP mapping (MITRE TRAM). h. Metrics are established and tuned based upon decisions made from incident post-mortems and related leadership actions. i. Threat hunting activities are moderated by the CTI's assessment of prevalent TTPs for priority threat actors and runbooks are updated based on threat actor TTPs. (see THREAT) j. Current and anticipated threats are disseminated to relevant security teams using daily or weekly reporting.

6.7. Third-Party Risk Management (THIRD-PARTIES)

Domain Purpose: Establish and maintain controls to manage the cyber risks arising from suppliers and other third parties commensurate with the risk to critical infrastructure and organizational objectives.

CTI Mission: Strengthen third-party risk management by continuously monitoring, detecting, assessing, and mitigating potential incidents posed by third-party vendors and suppliers. Enhance vendor risk profile evaluations and prioritization using CTI insights and recommendations.

Example: CTI3 Leading Third-Party Risk Management

Acme Inc.'s CTI team regularly monitors underground forums, data leak sites, and other sources for breach information. The team is alerted through automation and review of known threat actor onion sites of a possible breach impacting Bravo Corp. — a third-party vendor.

The team reviews the validity of the claim, assesses the risk to Bravo, and answers questions relevant to the risk Acme faces, including: Does Bravo have connectivity into Acme's environment or vice versa? Have they seen phishing emails? Is there operational or supply chain impact to Acme?

CTI Use Cases

1. Assess Threats to Third Parties
2. Mitigate Third-Party Risk Exposure

CTI Data Sources

- Attack Surface Intelligence
- Breach Intelligence
- Cybercriminal Underground Intelligence
- Geopolitical Intelligence
- Identity Intelligence
- Open Source Intelligence
- Social Media Intelligence
- Trust Groups
- Vulnerability Intelligence

CTI Use Cases and Practices

1. ASSESS THREATS TO THIRD PARTIES

CTI1	a. CTI has access to a list of third-party vendors and suppliers. The list may be based on incidents or organization knowledge rather than a complete list. b. CTI monitors data sources to assess the potential of third-party incidents at least in an ad hoc manner.
CTI2	c. Intelligence regarding threats to third parties is consistently contextualized to identify and mitigate risks. (see RISK and THREAT) d. Third parties are prioritized based on established criteria, including factors such as business and information security risk. (see RISK) e. Changes to the list of third-party vendors and suppliers are routinely updated and made available to CTI. f. Intelligence from cybercriminal underground sources is monitored to evaluate third-party risks arising from compromises, stolen credentials, and intellectual property theft. (see RISK)

CTI3	g. CTI insights are used to update vendors and suppliers in a third-party risk management (TPRM) platform. (see RISK) h. CTI supports the exposure analysis of suppliers and vendors involved in mergers or acquisitions. i. Monitoring of changes in geopolitical risk is used to evaluate changes in threats to third parties. (see THREAT)

2. MITIGATE THIRD-PARTY RISK EXPOSURE

CTI1	a. CTI monitors and assesses potential third-party exposures at least in an ad hoc manner. b. Intelligence concerning exploited vulnerabilities is routinely reviewed with respect to third parties.
CTI2	c. CTI insights are used to assess risk of suppliers' cybersecurity practices. (see RISK) d. CTI continuously monitors and assesses potential exposures of business critical vendors and suppliers. e. Intelligence includes predictive analysis about recommended COAs to reduce risk of exposure to the organization via third-party incidents. (see RISK) f. CTI provides the SOC with TTPs and IoCs related to third-party breaches.
CTI3	g. CTI continuously monitors and assesses potential exposures of all vendors and suppliers. h. Intelligence about third-party exposures is used prescriptively to identify future risk of the organization with existing third parties and their associated technologies. (see RISK)

6.8. Fraud and Abuse Management (FRAUD)

Note: Although FRAUD is not included in the C2M2, it is a highly impactful and relevant domain particularly in the retail, financial, hospitality, health care, and telecommunications industries. An organization's fraud team often relies heavily on intelligence provided by the CTI program for identifying threats and remediating their impact. The CTI-CMM includes this domain as guidance for shielding organizations against fraud.

Domain Purpose: Fraud and Abuse Management shields organizations from malicious digital scams and attacks. It hunts for emerging threats, shares intelligence to strengthen defenses, and guides response to safeguard data, finances, and reputation. This proactive shield against bad actors fosters a secure online environment for all.

CTI Mission: Create awareness around new and emerging trends in fraud and abuse (the malicious use of an organization's name, logo, or brand). Share threats and findings with relevant stakeholders to create detection and monitoring capabilities and to proactively mitigate risk.

Example: CTI3 Leading Fraud and Abuse Management

Acme Inc.'s CTI team monitors for fraud indicators, including stolen customer credentials on forums, leak sites, and social media. The team is alerted through automation and tooling. Alerts mention leveraging the access for loyalty point theft, fraudulent purchases, and other financial fraud activities. Intelligence insights are automatically ingested, collected, and actioned by relevant stakeholders. Insights are shared with ISAC or peer sharing groups.

The CTI team continuously monitors for brand abuse and impersonation attacks, identifying and improving detections of multiple threats including phishing kits, malvertising, and search engine optimization (SEO) poisoning. Intelligence is regularly used to inform accurate penetration tests and, purple and red team engagements to proactively guard against social engineering and other attacks.

CTI Use Cases

1. Mitigate Financial Fraud
2. Improve Brand Impersonation Protection
3. Enhance Account Takeover (ATO) Detection

CTI Data Sources

- Adversary Intelligence
- Brand Intelligence
- Cybercriminal Underground Intelligence
- Identity Intelligence
- Internal Organizational Data
- Open Source Intelligence
- Social Media Intelligence
- Trust Groups

CTI Use Cases and Practices

1. MITIGATE FINANCIAL FRAUD

CTI1	a. To combat exploitation and threat actor targeting, social media and open source sites are reviewed for posts of compromised customer credentials, gift cards, coupon scams, and credit cards at least in an ad hoc manner to support mitigation or prevention of fraudulent activity.

	b. CTI team tracks the activity and any mentions of point-of-sale (PoS) credit card skimmers on forums and social media and supports relevant team(s) with remediation and response. c. Intelligence sharing groups and private chat channels are monitored for money mule notifications and actioned with the appropriate team(s). d. Information about adversary targeting toward customers, including brand impersonation and compromised credentials to facilitate fraud, is delivered in at least in an ad hoc manner. e. CTI is a member of trust groups (such as ISACs and peer sharing) focused on mitigating financial fraud.
CTI2	f. Relevant information and data from trust groups is integrated into the organization's CTI practices. g. Automated monitoring is in place for mentions of common fraud indicators including business email compromise (BEC), short message service (SMS) phishing, invoice fraud, social engineering directed toward customers, and other relevant activity. h. CTI supports a cross-functional working group within the organization that is dedicated to identifying and sharing current and emerging threats on a recurring cadence. (see THREAT) i. Proactive tracking of fraud actor infrastructure and membership in private chat channels is done through automated collections and tooling.
CTI3	j. Implementation of cyber deception methods, including honeypots and accounts, is used for adversary tracking and collecting intelligence on TTPs and IoCs. k. IoC/B/As collected related to observed financial fraud are automatically shared with trust groups (such as through a TIP or other tooling). l. Intelligence insights are used to create antifraud detections and regularly tuned based on the organization's fraud observations.

2. IMPROVE BRAND IMPERSONATION PROTECTION

CTI1	a. Manual intelligence collection and analysis is done at least in an ad hoc manner for adversary targeting including brand impersonation on corporate domains and social media accounts impersonating corporate brands and individuals. b. CTI insights inform decisions on a range of cybersecurity defenses, including MFA strategies (e.g., limiting SMS or phone-based authentication where possible) and other controls designed to disrupt brand impersonation attempts. c. CTI tracks threat actors associated with fraud and abuse targeting their brand(s). (see THREAT) d. CTI tracks phishing kits being used against the organization's brand(s).
CTI2	e. Automation is used to detect malvertising campaigns and SEO poisoning for disruption actions. f. Automated alerting for adversary targeting, including brand impersonation, is used. g. Information shared in trust groups is utilized to track and mitigate risk from specific threat actors and campaigns. (see RISK)
CTI3	h. Automated identification and disruption of phishing kits targeting the organization's brand(s) is used.

	i. CTI provides actionable intelligence for implementation of canary tokens on Amazon Web Services (AWS) keys, sensitive documents, hostnames, and URLs (web app exposed) to detect unwanted access or attempts to access.

3. ENHANCE ACCOUNT TAKEOVER (ATO) DETECTION

CTI1	a. CTI tracks forums, sites, and threat actors associated with fraud and abuse targeting their brand(s) to facilitate customer ATO attacks. b. Manual identification of leaked customer credentials and accounts for sale on forums, social media, or websites is sent to relevant teams for immediate action.
CTI2	c. CTI provides intelligence to drive the creation of fraud-specific automation and detections for anomalous customer sign-ins and sessions indicating potential ATO activity. d. Feedback loops are created to include CTI when users (customers and employees) report suspicious behavior indicative of customer ATO activity.
CTI3	e. CTI continuously delivers intelligence to drive the proactive deployment of cyber deception technologies (e.g., honeypots, canary tokens, honey accounts) and prescribe prevention methods that enable rapid containment of customer credential misuse. f. CTI provides intelligence on likely threat activity to support penetration tests and purple and red team engagements to test for social engineering (cyber and physical) and actively audit security controls.

6.9. Workforce Management (WORKFORCE)

Domain Purpose: Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel commensurate with the risk to critical infrastructure and organizational objectives.

CTI Mission: Support hardening of the human element of the organization's attack surface by enhancing workforce management initiatives with insights into adversary tactics and organization- specific risks.

CTI Use Cases

1. Support and Safeguard Human Resources Practices
2. Support Development of Training and Education Assets
3. Support Cybersecurity Management in Workforce Development Efforts

CTI Data Sources

- Cybersecurity Workforce Development Strategy and Related Documents
- Internal Training Resources, Function-Specific Training Strategy, and Related Policy Documents
- Organization-Specific Cybersecurity Strategy, Policies, and Standards

Example: CTI3 Leading Program Support to Cybersecurity Workforce Management

Acme Inc.'s CTI team is actively engaged in supporting workforce development efforts. It leverages its understanding of threat and organization-specific risk to provide insights that inform defensive planning efforts and actions. Such insights may include which adversaries are targeting certain employee types and with what tactics, empowering security awareness, human resources, and workforce development teams to allocate training that aligns to these high-risk groups.

Whereas many organizations apply a "one-size-fits-all" approach to cybersecurity training and education, Acme recognizes not all employees are likely to be targeted by the same adversaries and in the same way, and that not all employees are equal in regard to the impact upon the organization should they be compromised. By aligning the nature, intensity, and frequency of cybersecurity training with the commensurate risk for individual roles, the organization is able to rightsize its efforts by training the right people, in the right way, at the right time.

CTI Use Cases and Practices

1. SUPPORT AND SAFEGUARD HUMAN RESOURCES PRACTICES

CTI1	a. CTI insights are regularly used to inform cybersecurity awareness and skills assessment strategies. b. Direct communications – and at least periodic engagement – with workforce management leadership consistently help identify cyber-related skills required for safe and effective operations of the workforce.
CTI2	c. On a periodic basis, CTI provides inputs to personnel vetting/screening procedures to inform hiring decisions and to minimize potential insider threat risks. d. CTI insights are consistently applied to inform the development of organization-specific plans for data/technology access needs, separation, and transfer procedures.
CTI3	e. Personnel vetting procedures are tailored to individual positions based on risk analysis (see RISK) of the job role and the organization's threat profile. (see THREAT)

	f. Screening tools used to assess the cybersecurity awareness of candidates and inform follow-on/remedial training requirements are developed and updated with CTI insights.

2. SUPPORT DEVELOPMENT OF TRAINING AND EDUCATION ASSETS

CTI1	a. Working relationships with the teams handling development and delivery of workforce training/education have been developed and engagement occurs at least in an ad hoc manner. b. Insights provided by the CTI program are generally relevant to the organization, but not necessarily aligned to specific organizational units or job roles. c. Workforce training/education initiatives are supported by CTI insights at least in an ad hoc manner and primarily related to significant changes in threat or vulnerability activity. (see THREAT)
CTI2	d. Security policy guidance, such as data protection and secure communication practices, is regularly reviewed by the CTI program — as are IR findings and other security reporting — to determine alignment of training/education initiatives with observed threat activity. e. Training/education teams are engaged on a routine basis to ensure alignment of materials and approaches with the organization's threat profile. f. CTI products and insights are routinely integrated into cybersecurity training and education efforts. g. Cybersecurity training materials are regularly reviewed by CTI to ensure the knowledge, skill, and ability gaps addressed in the curriculum are aligned with the organization's threat profile.
CTI3	h. CTI insights are used to assist with tailoring cybersecurity awareness activities to individual job roles as appropriate for the organization's threat profile. (see THREAT) i. The continuous improvement of training programs and education materials is facilitated by CTI insights into the current and anticipated threat landscape. (see PROGRAM) j. CTI insights are regularly leveraged for simulation exercises including phishing and social-engineering attacks. (see THREAT) k. Regular review and evaluation are conducted to measure the effectiveness of CTI inclusion in workforce development efforts and improvements are made as appropriate.

3. SUPPORT CYBERSECURITY MANAGEMENT IN WORKFORCE DEVELOPMENT EFFORTS

CTI1	a. Workforce development efforts are understood by the CTI program and it provides management with inputs as requested.
CTI2	b. The effort to identify high-risk job roles and support management in developing workforce-centric mitigation strategies is led by the CTI program. c. Procedures and activities associated with CTI support to workforce management efforts are documented, followed, and maintained to ensure effective and ongoing support.
CTI3	d. The CTI program is intimately familiar with workforce management operations and has developed proficiency at pairing content with delivery mechanisms to help optimize impact.

e. Changes in the organization's threat profile that are likely to impact workforce management efforts are routinely briefed to cybersecurity leadership.

f. Contributions to workforce management efforts are tracked, evaluated, and routinely reported to leadership.

6.10. Cybersecurity Architecture (ARCHITECTURE)

Domain Purpose: Establish and maintain the structure and behavior of the organization's cybersecurity architecture, including controls, processes, technologies, and other elements, commensurate with the risk to critical infrastructure and organizational objectives.

CTI Mission: Support the effort to develop a robust and resilient cybersecurity architecture by providing insights into cyber threats targeting the organization and recommending mitigation options around controls, processes, technologies, and other elements.

CTI Use Cases

1. Support Strategy Development for the Cybersecurity Architecture
2. Support Maintenance of the Cybersecurity Architecture
3. Support Compliance Efforts for the Cybersecurity Architecture

CTI Data Sources

- Organization IT and Cybersecurity Architecture
- Organization-Specific Cybersecurity Strategy, Policies, and Standards
- Threat and Vulnerability Management Data Sources

Example: CTI3 Leading Program Support to Cybersecurity Architecture

Acme Inc.'s CTI team actively supports efforts to conceptualize and develop a more robust and resilient IT architecture. Corporate leadership understands the need to move away from reactive posture and mitigative solutions and toward taking a more proactive posture that anticipates threats over the horizon. The CTI team leverages the trust it has built with senior leadership, its close ties with adjacent IT and information security (infosec) functions, and its vantage point at the intersection of IT and business operations to provide insights that inform and guide the organization's architecture.

Acting as a trusted advisor, the CTI team works with IT and infosec peers to identify categories of threats and related mitigation technologies and paradigms in an effort to proactively address emerging and future threats. Working in tandem with peers and leadership, the CTI team is able to inform near-term decision-making around existing technologies and approaches while simultaneously supporting strategy development that will shape future acquisition, organizational behavior, and product management (as applicable).

CTI Use Cases and Practices

1. SUPPORT STRATEGY DEVELOPMENT FOR THE CYBERSECURITY ARCHITECTURE

CTI1	a. CTI is familiar with key personnel involved in cybersecurity architecture strategy and program development activities, providing input in at least an ad hoc manner.
CTI2	b. CTI has established communication channels and trusted relationships with cybersecurity architecture leadership or significant stakeholders, leveraging both regularly to proactively provide input to support cybersecurity architecture strategy and program development as intelligence insights are developed. (see THREAT)
CTI3	c. CTI is fully integrated into the processes that shape the cybersecurity architecture strategy, leveraging its unique vantage point within the enterprise to provide novel insights such as risks associated with changes in the threat landscape and vendor practices or products that may impact enterprise cybersecurity architecture. (see THREAT)

2. SUPPORT FOR CYBERSECURITY ARCHITECTURE THROUGH CONTINUOUS THREAT MODELING

CTI1	a. CTI is engaged on an ad hoc basis by cybersecurity architecture personnel to address specific questions about technologies, exploitation of vulnerabilities, or other threat-related insights in support of architecture-planning activities.
CTI2	b. CTI is sufficiently familiar with the cybersecurity architecture to identify threats that cut across cybersecurity functions (potentially "slipping through the cracks" between teams) or risks manifested through the exploitation of multiple technologies and reports these regularly to the cybersecurity architecture team. c. CTI reports for the cybersecurity architecture team regularly include recommendations for mitigating threats at the enterprise level.
CTI3	d. CTI prepares contextualized reporting and recommendations for the architecture team on a regular cadence of trends impacting controls, processes, technologies, and other elements that require enterprise-wide solutioning to resolve (e.g., discovery of extensive shadow IT, changes to product capabilities, foreign acquisition of vendors, etc.)

3. SUPPORT FOR CYBERSECURITY ARCHITECTURE THROUGH POLICY & COMPLIANCE ALIGNMENT

CTI1	a. CTI informs the architecture team of changes to CTI infrastructure (new tools, data storage solutions, etc.) on an ad hoc basis. b. CTI reports noncompliant controls, processes, technologies, and other elements it discovers in the course of its duties to the architecture team in at least an ad hoc manner.
CTI2	c. CTI informs architecture stakeholders in advance of changes to CTI infrastructure and provides insights into how those changes — and any resulting capabilities — might enhance or degrade enterprise cybersecurity outcomes. e d. CTI aligns capabilities development and technology acquisition with cybersecurity architecture needs while ensuring compliance with policies and controls.
CTI3	e. CTI has documented procedures for engaging with incident response and other teams to develop novel intelligence reporting based on internal cybersecurity events that represent unrealized risk to the enterprise cybersecurity architecture and does so on a recurring basis. f. CTI helps shape the cybersecurity architecture by leveraging its "trusted advisor" status to inject policy insights at the intersection of cybersecurity and business operations.

6.11. Cybersecurity Program Management (PROGRAM)

Domain Purpose: Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with both the organization's strategic objectives and the risk to critical infrastructure.

CTI Mission: Support the enterprise cybersecurity program by aligning CTI operations to the program strategy, providing organization-specific insights that support cybersecurity program maturation, and delivering decision support to cybersecurity program management teams.

Example: CTI3 Leading Program Support to the Cybersecurity Program

Acme Inc established its CTI program to support its cybersecurity strategy in facing an increasing number of sophisticated cyber threats, complex IT infrastructures, and stringent regulatory and compliance requirements. Acme's CTI program provides critical support as the cybersecurity program enables business expansion, safeguards high-value assets and sensitive data, and ensures enterprise compliance.

NOTE: This Domain — as all others — maps directly to the C2M2. That is, it describes how CTI should support the larger cybersecurity program; as opposed to describing the structure of the CTI program itself.

CTI Use Cases

1. Align CTI Program with Enterprise Cybersecurity Strategy
2. Support Maturation of the Enterprise Cybersecurity Program

CTI Data Sources

- Applicable Data Sources from Other Domains
- Enterprise Cybersecurity Program Documentation
- Corporate Annual Reporting (8-K, 10-K, Annual Report, etc.)
- Cybersecurity Program Performance Management Documentation (OKR, KPI, etc.)

CTI Use Cases and Practices

1. ALIGN CTI PROGRAM WITH ENTERPRISE CYBERSECURITY STRATEGY

CTI1	a. CTI is aware of the enterprise cybersecurity strategy and provides inputs and support to its development in at least an ad hoc manner.
CTI2	b. CTI understands the enterprise cybersecurity strategy and leverages that understanding to provide focused inputs and development support on a regular basis. c. The CTI program strategy and priorities are formally documented and aligned with the organization's cybersecurity mission, strategic objectives, and risk to critical infrastructure and assets. d. CTI applies its understanding of the cybersecurity program strategy to inform the development of CTI capabilities that are compliant and aligned to cybersecurity program goals.
CTI3	e. CTI goals and performance standards are mapped to the performance management frameworks (OKR, KPI, etc.) used by the enterprise cybersecurity program, ensuring they are working in concert.

	f. CTI is fully integrated into the processes that shape the cybersecurity program strategy and leverages its unique vantage point within the enterprise to provide novel insights such as risks associated with business changes, changes in the global threat landscape, and changes in the enterprise threat profile. (see RISK and THREAT)

2. SUPPORT MATURATION OF THE ENTERPRISE CYBERSECURITY PROGRAM

CTI1	a. CTI is familiar with key personnel involved in cybersecurity program management and effectively leverages this access on an ad hoc basis to provide relevant inputs. b. CTI has a basic knowledge of the mission, structure, and functional components of the cybersecurity program, allowing it to craft useful insights on at least an ad hoc basis.
CTI2	c. CTI has established communication channels and trusted relationships with cybersecurity program leadership, leveraging both regularly to provide inputs in support of maturing the cybersecurity program. d. CTI has a solid understanding of the mission, structure, and functional components of the cybersecurity program, allowing delivery of focused and properly contextualized policy inputs.
CTI3	e. CTI is a trusted and equal partner with other cybersecurity and IT functions in providing guidance that shapes the cybersecurity program.

Appendices

A. Stakeholder Overview

Internal Stakeholders

Strategic:

Executive Leadership:

- ***CEO, CFO, CIO, CTO, CISO:*** Responsible for overall strategic decision-making, resource allocation, security architecture, information management, and risk management. They use CTI to inform high-level decisions and set business and cybersecurity priorities.

Operational:

Risk Management and Compliance:

- ***Risk Managers:*** Assess and manage cybersecurity risks. They use CTI to understand threat landscapes and align risk mitigation strategies.
- ***Compliance Officers:*** Ensure adherence to regulatory requirements and standards. They use CTI to maintain compliance with cybersecurity models or frameworks.
- ***Business Unit Leaders:*** Manage specific business functions (e.g., finance, HR, marketing). They use CTI to protect sensitive business information and ensure continuity.
- ***Product Development Teams:*** Integrate security into product design and development. They use CTI to anticipate and mitigate potential threats to products and services.

Legal and Privacy Teams:

- ***Legal Counsel:*** Provides legal advice on cybersecurity matters. They use CTI to understand legal implications of threats and breaches.
- ***Privacy Officers:*** Ensure data privacy and protection. They use CTI to identify and address privacy-related threats.

Tactical:

Security Operations Center*:*

- ***SOC Analysts:*** Monitor and respond to security incidents. They use CTI to detect, analyze, and mitigate threats in real time.
- ***IR Team:*** Handles and investigates security breaches. They rely on CTI for threat context and to develop response strategies.

IT Department:

- ***Network Administrators:*** Manage and secure network infrastructure. They use CTI to implement security controls and protect network resources.
- ***System Administrators:*** Oversee the configuration and maintenance of servers and endpoints. They use CTI to harden systems against known threats.

External Stakeholders

Partners and Vendors:

- ***Third Parties and Supply Chain Partners:*** Collaborate on cybersecurity efforts. They use CTI to ensure the security of interconnected systems and data exchanges.
- ***Managed Security Service Providers (MSSPs):*** Provide outsourced security services. They use CTI to enhance the security posture of their clients.

Customers and Clients:

- ***End Users:*** May receive notifications and guidance based on CTI. They benefit from enhanced security measures informed by CTI.
- ***Business-to-Business (B2B) Clients:*** Expect secure interactions and transactions. They use CTI to ensure the safety of their interactions with the organization.

Communities:

- ***ISACs:*** Facilitate the sharing of CTI among member organizations. They use CTI to promote collective security.

By engaging these stakeholders, an organization can effectively leverage CTI to enhance its cybersecurity posture and resilience against threats.

For governmental bodies, the scope and complexity of stakeholders involved in CTI expand significantly, primarily due to the need for collaboration with other government entities and adherence to national security policies. The following types of stakeholders are typically involved:

Executive Leadership:

- ***Government Officials (e.g., President, Prime Minister, Ministers):*** Make high-level strategic decisions regarding national cybersecurity policies.
- ***National Security Advisors:*** Provide counsel on threats that impact national security and the strategic response.

Cybersecurity Agencies and Departments:

- ***National Cybersecurity Centers:*** Coordinate the nation's cybersecurity efforts, including CTI gathering and dissemination.
- ***Government Computer Security Incident Response Team (CSIRT):*** Responds to cybersecurity incidents across government networks and collaborates with other CSIRTs.

Intelligence and Law Enforcement Agencies:

- ***National Intelligence Agencies (e.g., NSA, GCHQ):*** Gather and analyze intelligence on cyber threats, often focusing on state-sponsored threats and espionage.
- ***Federal Law Enforcement (e.g., FBI, Europol, Interpol):*** Investigate cybercrimes and collaborate on CTI with other agencies and international partners.

Military and Defense Departments:

- ***Cyber Command:*** Oversees the protection of military networks and conducts offensive cyber operations. They use CTI for both defensive and offensive strategies.
- ***Defense Intelligence Agencies:*** Analyze threats to military assets and national defense infrastructure.

Government IT and Security Departments:

- ***IT Departments:*** Manage government networks and infrastructure, implementing security controls informed by CTI.

- ***SOCs:*** Monitor and respond to threats in real time, often coordinating with national cybersecurity centers.

Regulatory and Compliance Bodies:

- ***Regulatory Authorities:*** Ensure government agencies comply with cybersecurity laws and standards. They use CTI to develop regulations and guidelines.
- ***Data Protection and Privacy Offices:*** Focus on protecting citizen data and ensuring privacy, using CTI to identify and mitigate threats.

Sector-Specific Agencies:

- ***Critical Infrastructure Protection Agencies:*** Oversee the security of essential services such as energy, water, and transportation. They rely on CTI to protect these sectors from cyber threats.
- ***Health care, Financial, and Other Sector Regulators:*** Use CTI to safeguard sector-specific critical infrastructure and services.

International Partners and Alliances:

- ***International Cybersecurity Organizations (e.g., NATO, ENISA):*** Collaborate on global cybersecurity initiatives and share CTI.
- ***Bilateral and Multilateral Cybersecurity Agreements:*** Facilitate CTI sharing and cooperative defense strategies between nations.

Public and Private Sector Collaboration:

- ***Public-Private Partnerships:*** Engage with private sector entities to share CTI and improve collective security (e.g., ISACs, industry consortiums).
- ***Private Sector Critical Infrastructure Operators:*** Work closely with government agencies to protect essential services and share CTI.

Academic and Research Institutions:

- ***Universities and Research Centers:*** Conduct cybersecurity research and develop new CTI methodologies.
- ***Think Tanks and Policy Institutes:*** Analyze cybersecurity trends and provide strategic recommendations based on CTI.

Civil Society and Non-Governmental Organizations (NGOs):

- ***Cybersecurity Advocacy Groups:*** Raise awareness and advocate for stronger cybersecurity policies, often collaborating with government entities.
- ***Citizen Groups and NGOs:*** Focus on protecting civil liberties and privacy, using CTI to inform their advocacy efforts.

Interagency Coordination Bodies:

- ***National Security Councils:*** Coordinate cybersecurity policies and responses across various government agencies.
- ***Interagency Working Groups:*** Facilitate communication and collaboration on cybersecurity issues across different governmental bodies.

By involving these stakeholders, a governmental body can effectively leverage CTI to enhance national cybersecurity, protect critical infrastructure, and respond to evolving cyber threats. Collaboration with other government entities, international partners, and the private sector is crucial for a comprehensive and robust cybersecurity posture.

B. Strategic, Operational, and Tactical Overview

	Definition	Typical Responsibilities	Typical CTI Products
Strategic	Strategic CTI provides a high-level overview of the threat landscape, offering insights and predictions about future threats and trends. It is designed for senior executives and decision-makers to inform long-term strategies and policy-making. **Key Characteristics:** • Long-term focus • Broad and high-level • Contextual and trend analysis • Used for planning and resource allocation	• Identify and assess long-term cyber threats and trends. • Inform senior leadership about potential impacts on business objectives and national security. • Guide the development of cybersecurity policies and investment strategies. • Align cybersecurity initiatives with organizational goals and regulatory requirements.	• Threat Landscape Reports: High-level overviews of the evolving threat environment and emerging trends. • Risk Assessments: Evaluations of potential long-term risks to the organization or sector. • Strategic Threat Briefings: Presentations and reports for executives and board members on significant threats and strategic implications. • Forecasting Reports: Predictions on future threat developments and their potential impacts.
Operational	Operational CTI focuses on specific threats and campaigns that are relevant to an organization's operations. It aids in the detection, analysis, and mitigation of attacks and helps in decision-making processes related to preventing and responding to incidents. **Key Characteristics:** • Mid-term focus • Detailed and actionable • Directly supports network operations, security operations, vulnerability management, and incident response • Provides context for specific threats	• Provide actionable intelligence for security operations and incident response teams. • Support the planning and execution of security initiatives and defensive measures. • Coordinate CTI sharing with industry peers and partners. • Translate strategic insights into concrete operational plans.	• CTI Reports: Detailed reports on specific threats, including tactics, techniques, and procedures (TTPs) of adversaries. • Incident Response Plans: Guides and playbooks for responding to specific types of cyber incidents. • Threat Actor Profiles: In-depth analyses of threat actors, including their motivations, capabilities, and attack patterns. • Vulnerability Assessments: Evaluations of system vulnerabilities and recommended mitigation strategies.

Tactical	Tactical CTI provides real-time or near-real-time information about immediate threats and campaigns. It is used by front-line cybersecurity teams to defend against and mitigate active threats. **Key Characteristics:** • Short-term focus • Highly specific and immediate • Directly supports security operations centers (SOCs) and incident response • Focuses on immediate defensive actions	• Provide direct support to security operations centers (SOCs) and incident responders. • Monitor and analyze real-time threat data and alerts. This may be accomplished through detection, enrichment, and threat hunting. • Facilitate the rapid detection, investigation, and mitigation of threats. • Share immediate threat indicators with relevant teams to prevent or respond to attacks.	• Indicators of Compromise (IoCs): Specific data points like IP addresses, file hashes, and URLs associated with known threats. These often may be aggregated into feeds (along with relevant content for each indicator). • Tactical Threat Alerts: Real-time alerts and notifications about active threats and incidents. • Attack Patterns: Detailed descriptions of observed attack techniques and how to recognize them. • Incident Analysis Reports: Post-incident reports detailing the nature of the attack, how it was mitigated, and lessons learned.

C. CTI Metrics and Measurements

CTI teams are often asked to provide leadership with metrics that demonstrate their contributions to improving the cybersecurity posture of an organization and reducing its overall risk. Developing effective CTI metrics is challenging and most organizations struggle when trying to create metrics that reflect systemic impact. As a result, most organizations develop metrics that measure level of effort or throughput vice program maturity growth or stakeholder-specific support.

To address this, the CTI-CMM offers a list of domain-specific metrics that help CTI programs track their maturity on a per stakeholder basis. These metrics are designed to be representational and are by no means a definitive set for which every CTI program needs to apply. Rather, they offer a starting point in which CTI programs can adjust as necessary.

Each metric links to a relevant use case within its domain. As CTI programs advance across the maturity levels, measurement may require close collaboration with partners to determine impact. For the purpose of this model, we provide example metrics at each maturity level in a respective domain with plans to refine and focus in future updates based on community feedback.

ASSET

CTI1 – Foundational	1. Number of ad hoc alerts generated for newly discovered assets through threat-informed insights. 2. Percentage of mandated CTI-relevant controls (from specified frameworks such as NIST CSF or NIS2) that have documented CTI processes, evidence, or artifacts supporting their satisfaction.
CTI2 – Advanced	3. Changes to the organization's threat profile to account for changes in the asset inventory and crown jewels (annually). 4. Number of asset reconfigurations or security control adjustments informed by CTI support. 5. Percentage of high-priority assets covered by proactive CTI risk assessments. 6. Reduction in mean-time-to-detect (MTTD) at-risk assets using attack surface intelligence.
CTI3 – Leading	7. Percentage of assets dynamically updated with threat context using automation. 8. Number of threat-informed decisions made for asset lifecycle management. 9. Percentage of strategic asset acquisitions vetted against CTI risk assessments.

THREAT

CTI1 – Foundational	1. Percentage of CTI reports or alerts that directly influenced incident response decisions. 2. Percentage of IoCs gathered from external sources integrated into security operations. 3. Percentage of incident or alert data mapped to threat models (MITRE ATT&CK, Kill Chain, Diamond Model) and enriched with internal intelligence.
CTI2 – Advanced	4. Percentage of basic threat actor profiles created based on observed activity. 5. Number of threat-informed security insights (including proof of detection logic) that informed patching prioritization decisions. 6. Number of threat actor campaigns tracked and analyzed for targeted industry threats.

	7. Number of threat hunts initiated based on CTI team-sourced intelligence. 8. Number of threat scenarios developed in collaboration with purple/red team for security control testing exercises.
CTI3 – Leading	9. Percentage of predictive CTI reports that successfully forecast attack trends. 10. Number of strategic threat briefings influencing executive-level risk decisions over the past year. 11. Percentage of adversary infrastructure (e.g., C2 servers, phishing domains) proactively identified and blocked using CTI insights. 12. Number of CTI-driven intelligence-sharing collaborations with ISACs or peer organizations that resulted in proactive reduction of risk. 13. Number of geopolitical or macroeconomic factors analyzed within CTI threat modeling. 14. MTTR threats that were identified through CTI insights.

RISK

CTI1 – Foundational	1. Percentage of CTI reports, briefings, and insights that reference impacted organizational assets and partners. 2. Percentage of CTI team members that demonstrate awareness of organizational relevant risk management frameworks (such as NIST's Risk Management Framework SP 800-30) and methods for assessing impact using cyber risk-based frameworks (e.g., Factor Analysis of Information Risk (FAIR) cyber risk quantification model, the Vocabulary for Event Recording and Incident Sharing (VERIS), the Open Worldwide Application Security Project's (OWASP's) Risk Rating Methodology, Information Security Forum (ISF) Quantitative Techniques in Information Risk Analysis, etc.). 3. Percentage of inter-risk assessment models and processes that leverage CTI insights. 4. Number of engagements between CTI and risk management teams.
CTI2 – Advanced	5. Number of risks identified by CTI insights integrated into risk management dashboards. 6. Percentage of CTI reports, briefings, and insights with focus on translating threat insights into risk mitigations (e.g., suggesting PoC detection logic or recommendations to mitigate risk) for consumption by partner action-arm teams. 7. Percentage of CTI products that leveraged risk-based frameworks to provide a common frame of reference when producing content for risk-based stakeholders or senior leadership. 8. Percentage of CTI practices that are aligned and synchronized with the risk framework adopted by the organization.
CTI3 – Leading	9. Number of risk-based decisions and actions where prioritization is based on the cyber threat landscape. Requires capturing insights on how risk and cybersecurity teams use the cyber threat profile to drive coverage decisions, reduce exposure, and identify control gaps. 10. Percentage of stakeholder meetings with risk management that result in collaboration or inclusion of CTI insights into risk assessments, decisions, or adjustment to risk management strategies or processes. 11. Percentage of CTI reports, briefings, and insights where detection logic or recommendations were employed or identified as high quality by partner action-arm teams. 12. Number of risk-based controls and decisions adjusted using CTI insights with measurable improvements (such as improving incident count, cybersecurity expense, or risk quantification).

ACCESS

CTI1 – Foundational	1. Number of changes to access control policies, password resets, account risk level, or network architecture tuning resulting from CTI inputs. 2. Number of leaked credentials identified or access claims CTI identified.
CTI2 – Advanced	3. MTTR identity-related threats after CTI alerting. 4. Percentage of user accounts flagged as high-risk based on behavioral CTI inputs. 5. Percentage of MFA enforcement changes influenced by CTI insights. 6. Percentage of identity-based attack vectors proactively mitigated through threat-informed detection rules.
CTI3 – Leading	7. Number of access control policies dynamically adjusted based on real-time CTI threat landscape. 8. Percentage of insider threat indicators detected and mitigated via CTI-augmented user and entity behavior analytics (UEBA). 9. Number of automated identity security enhancements resulting from CTI inputs. 10. Percentage of security investment decisions in IAM influenced by strategic CTI insights.

SITUATION

CTI1 – Foundational	1. Percentage of intelligence products that integrate relative threat activity to relation with the current threat landscape to include geopolitical events to business impact. 2. Percentage of situational awareness reports that led to a measurable risk reduction action. 3. Percentage of internal incidents that have been enriched using intelligence sources.
CTI2 – Advanced	4. Time to contextualize threats for emerging situations impacting the organization. 5. Percentage of times the collated organizational threat landscape report – cyber threat profile – was used to drive business outcomes. 6. Return on investment tracking across sources, mapped to PIRs answered. 7. Percentage of internal incidents discovered over the past year that have been vetted, normalized, cataloged, and indexed into a centralized knowledge management system such as a TIP.
CTI3 – Leading	8. Impact and number of briefings provided to cybersecurity and risk leaders, security awareness, hunt, incident response, and/or the red team on changes in the cyber threat landscape. 9. Percentage of real-time or near-immediate security decisions informed by CTI insights. 10. Number of CTI-driven scenario planning exercises conducted to prepare for emerging threats. 11. Reduction in security incidents through improved CTI-based situational forecasting.

RESPONSE

CTI1 – Foundational	1. Number of new incidents detected as a direct result of CTI reporting or investigation (distinct from incidents resulting from IoC in third-party feeds). 2. Percentage and number of internal incidents for which the CTI function has provided support or added new collections. 3. Percentage of internal incidents that have been enriched using intelligence sources.
CTI2 – Advanced	4. Percentage of reported incidents correlated and enriched by IoCs resulting in positive discovery. 5. Number of instances where CTI reporting in support of an incident led to direct and substantive actions by stakeholders. 6. Number of new intelligence insights produced from a review of IR cases. 7. Total number of CTI reports that directly contributed to the development or maintenance of a response playbook.
CTI3 – Leading	8. Percentage of IR case escalations that received CTI enrichment and/or support. 9. Total number of response automation workflows (e.g., security orchestration, automation, and response (SOAR) playbooks) that are informed/driven by CTI inputs. 10. Percentage of IR debriefs where CTI insights led to changes in response procedures. 11. Reduction in dwell time (average time a threat remains undetected) based on threat-informed detections.

THIRD-PARTIES

CTI1 – Foundational	1. Number of times CTI notified internal stakeholders of a third-party compromise. 2. Number of critical vulnerabilities in third-party software used by the organization that were reported to cybersecurity and risk stakeholders by CTI. 3. Percentage of IoCs or TTPs collected in third-party compromises that resulted in detections.
CTI2 – Advanced	4. Percentage of CTI reports that included business impact analysis of a potential supply chain breach. 5. Number of times CTI detected a third-party compromise before receiving notification from the third party. 6. Number of times CTI performed a holistic review of supply chain compromises to determine commonality and issue an internal report with security recommendations. 7. Number of internal threat hunts informed by IoCs and TTPs associated with third-party compromises that were collected by CTI.
CTI3 – Leading	8. Number of third-party alerts provided by CTI that resulted in a review and potential reclassification of risk level based on CTI alerts. 9. Number of third-party alerts provided by CTI that resulted in an immediate mitigation action taken.

FRAUD

CTI1 – Foundational	1. Number of valid compromised customer credentials escalated for remediation. 2. Number of domains, social media sites, etc., requested for takedown. 3. Number of threat actor groups tracked for fraud.
CTI2 – Advanced	4. Estimated cost savings to the business due to CTI-informed fraud prevention efforts. 5. Number of honeypot credentials seeding fraud infrastructure and the resulting number of threat actors reported to law enforcement.
CTI3 – Leading	6. Number of CTI-informed automations that prevented ATOs and fraud. 7. Percentage of fraud attempts reduced through CTI-informed automation. 8. Number of fraud prevention mitigations resulting from continuous red team and penetration testing exercises informed by CTI insights. 9. Percentage of executive-level fraud risk decisions influenced by CTI insights.

WORKFORCE

CTI1 – Foundational	1. Number of intelligence products produced with security awareness as a stakeholder with explicit follow up to gauge relevance and utility. 2. Number of engagements with teams that have security awareness responsibilities which led to collaboration opportunities to jointly educate the workforce on cyber threats, security controls, and security policies. 3. Level of awareness among executive leadership that the CTI function is a core contributor in supporting workforce education and awareness on cybersecurity initiatives.
CTI2 – Advanced	4. Number of requests, tickets, or cases HR created seeking support or mitigating actions for prospective candidate or personnel vetting in support of insider threat scenarios directly influenced by CTI-provided insights. 5. Regularity of review of organizational cybersecurity training materials and CTI-suggested inputs for future workforce training and education efforts. 6. Ratio of substantive updates to cybersecurity-related workforce development initiatives relative to changes in the organization's threat profile as a measure of how regularly CTI insights (as represented by changes in the threat profile) are leveraged by workforce development teams.
CTI3 – Leading	7. Percentage of changes made in required training for high-risk or "critical" job roles that require specific cybersecurity and cyber threat awareness based on CTI team-produced work over the past year. 8. Percentage of cybersecurity workforce phishing simulations, tabletop exercises, or other exercises that incorporate CTI inputs or support. 9. Number of products or assets developed by workforce management functions that are directly informed by or include CTI inputs. 10. Measured increase in security awareness among employees due to CTI-driven training or communications (e.g., phishing simulation results or click-through rates on security advisories).

ARCHITECTURE

CTI1 – Foundational	1. Number of unstructured (ad hoc) recommendations provided to architecture teams by CTI. 2. Number of retroactive architecture adjustments made based on CTI inputs that were associated with security incidents.
CTI2 – Advanced	3. Number of non-security IT projects where CTI contributed actionable insights (e.g., M&A, vendor selection, etc.). 4. Percentage of architecture design reviews that cite CTI inputs as informing or justifying the decision. 5. Number of adversary TTPs (MITRE ATT&CK techniques) actively mitigated through security architecture changes. 6. Number of major security control implementations (e.g., Zero Trust adoption, segmentation strategies, etc.) where CTI was actively engaged to support planning and advisory.
CTI3 – Leading	7. Number of CTI reports that resulted in security architecture adjustments. 8. Number of security architecture blueprints that integrate forward-looking CTI insights. 9. Reduction in attack surface exposure resulting from threat-informed architectural transformations. 10. Percentage of business continuity or disaster recovery plans influenced by threat-informed threat scenarios. 11. Number of security technology investments justified, prioritized, or otherwise impacted by CTI-informed risk modeling. 12. Percentage of leadership decisions where CTI insights were leveraged to shape security roadmaps.

PROGRAM

CTI1 – Foundational	1. Number of stakeholders who request CTI products or updates as an indicator of trust and reliance on the CTI program. 2. Count of citations and positive feedback on CTI insights related to cybersecurity program governance and planning objectives and activities. 3. Percentage of CTI data sources mapped to stakeholder requirements as a measure of how efficiently and effectively the CTI function is applying its funding and manpower to support governance and planning for enterprise cybersecurity. 4. Variance in CTI program budget and leadership support from year to year and documented reasoning behind any shifts.
CTI2 – Advanced	5. Number of hours team members are engaged in upskilling efforts throughout the year to ensure skills alignment. 6. Attrition rate of CTI team members. 7. Number of changes made to the organization's cybersecurity strategy, policies, or documented procedures based on insights provided by CTI. 8. Qualitative feedback from stakeholders on the value and usefulness of CTI outputs.
CTI3 – Leading	9. Evaluate how CTI activities support broader business risk mitigation goals by tracking correlations between intelligence-led actions and reductions in risk as measured by risk-reduction metrics. 10. Number of cross-functional teams (e.g., fraud, legal, governance, risk, and compliance (GRC)) actively leveraging CTI outputs for decision-making.

D. CTI Data Source Library

Intelligence Source	Description	Examples
Adversary	Involves the collection, analysis, and interpretation of information about potential threats posed by malicious actors, including hackers, criminal organizations, or nation-state actors. The goal is to understand the TTPs used by these adversaries to anticipate and mitigate their actions.	• Threat actor profiles • Industry or vendor advisories
Attack Surface	Refers to an organization's external public-facing assets where an attacker can attempt to enter or exploit a system, network, or application. Typically, an organization's "attack surface" includes all exposed software, services, assets, and data accessible via the open internet.	• Exposed ports, services, and vulnerabilities • Compromised access credentials or tokens • Domain-related threats
Brand	Refers to the monitoring and remediation of threats to an organization's brand that may harm its reputation and security. Typically, "brand intelligence" focuses on identifying threats that either mimic or target the brand directly.	• Brand impersonation (fake websites, social media accounts) • Phishing and spam using the brand's identity • Domain-related threats (squatting, fraudulent websites) • Fake and counterfeit products
Breach	The collection, analysis, and reporting of information related to data breaches. It focuses on understanding the nature of security incidents where sensitive data is exposed, stolen, or compromised by unauthorized parties.	• SEC Form 8-K Incident Disclosures • Cybercriminal underground sources • Open sources • Social media sources
Cybercriminal Underground	Refers to a virtual ecosystem where threat actors engage in illicit business, share TTPs, and conduct attack planning. It is generally associated with the "dark web" — part of the internet that is not indexed by standard search engines and requires special tools to gain access, such as The Onion Router (Tor) or Invisible Internet Project (I2P) — and in closed sources that require a barrier of entry to access, such as instant messaging chat groups.	• Hacking forums • Illicit marketplaces • Data leak sites (DLSs) • Instant messaging platforms • Private communication channels
Geopolitical	Refers to the monitoring and analysis of international political, economic, military, social, and cyber events that impact the security and risk of an organization's digital systems, networks, data, and people.	• State-sponsored cyber threats • Cybersecurity policy and regulation • Cyber and kinetic warfare • Economic and trade conflicts • Critical infrastructure security • Emerging technologies • Supply chain and third-party risk
Identity	Refers to the collection and analysis of exposed or compromised customer and employee credentials and identities used by threat actors to gain unauthorized access into networks or systems and commit ATO activities.	• Compromised credential dumps and session tokens • Information stealing (infostealer) malware, campaigns, and logs

Intelligence Source	Description	Examples
Internal Organizational Data	Any data or information collected from within an organization's own systems, networks, and programs that can be used to identify potential internal threats or malicious activity.	• System logs • Network traffic analysis • User activity monitoring • Endpoint security data • Vulnerability scans • IR reports • Application logs • Security alerts • Anomalous behavior detection • Internal threat assessments
Malware	Refers to the monitoring, collection, and analysis of malware families, campaigns, infrastructure, and deployment methods.	• Malware behaviors and analytics • Malicious file and network-based indicators • Malware campaign tracking • Botnet infrastructure monitoring • Yara rules and intrusion detection system (IDS) signatures
Open Source	Refers to the collection and analysis of data and information from a wide range of publicly available sources.	• News sites • Leak and paste sites • Code repositories • Threat and IoC feeds
Social Media	Refers to the collection and analysis of data and information from social media platforms.	• Social networking sites (e.g., Facebook, X, LinkedIn, TikTok) • Image-based sites (e.g., Instagram, Pinterest, Flickr) • Video hosting platforms (e.g., YouTube, Snapchat, Vimeo) • Discussion forums (e.g., Reddit, 4Chan, Quora) • Blog and community forums (e.g., Medium, Tumblr)
Trust Groups	Refers to collaborative communities or networks of trusted individuals or organizations that share CTI information with each other for a common purpose to prevent harm.	• ISACs • Government-sponsored • Private or commercial • Informal or ad hoc • Open source or public communities
Vulnerability	The systematic collection, analysis, and dissemination of information about security vulnerabilities in software, hardware, and network components.	• CISA Known Exploited Vulnerability (KEV) • Exploit Prediction Scoring System (EPSS)

E. CTI Data Source Matrix

	Domain										
Intelligence Source	ASSET	THREAT	RISK	ACCESS	SITUATION	RESPONSE	THIRD-PARTIES	FRAUD	WORKFORCE	ARCHITECTURE	PROGRAM
Adversary		■			■	■		■	Coming soon!		
Attack Surface	■	■	■	■		■	■				
Brand								■			
Breach	■	■	■	■		■	■				
Cybercriminal Underground	■	■	■	■	■		■	■			
Geopolitical			■		■		■				
Identity			■	■		■	■	■			
Internal Organizational Data	■	■	■		■	■		■			
Malware		■				■					
Open Source	■	■	■		■	■	■	■			
Social Media							■	■			
Trust Groups					■		■	■			
Vulnerability	■	■	■	■		■	■				

F. Glossary of Key Terms

Term	Definition	Source
10-K	A yearly report all publicly traded companies are required to file with the Securities and Exchange Commission (SEC). The 10-K is usually more detailed than an annual report.	SEC
8-K	The "current report" companies must file with the SEC to announce major events that shareholders should know about, including material security incidents.	SEC
Account takeover (ATO)	When a malicious actor gains unauthorized access to a user's legitimate account, typically through the use of compromised credentials or vulnerabilities exploited against identity management systems. ATO can be used in two ways: Fraud: In this context, ATO is when a financially motivated threat actor gains access to a customer's legitimate online account by exploiting stolen customer credentials or security weaknesses. This unauthorized access enables fraud across a wide spectrum of industries including financial, retail, hospitality, airlines, health care, and telecommunications for financial exploitation, stealing personally identifiable information (PII), and social-engineering attacks. Network iIntrusion: In this context, ATO is when a threat actor gains unauthorized access to a victim's IT environment through compromising a user's account, typically through stolen credentials, phishing, or vulnerability exploitation. This unauthorized access typically enables security breaches, data theft, and operational disruption.	CTI-CMM
Actionable intelligence	Information that is not only accurate and relevant, but also directly useful for making decisions and taking specific actions. This type of intelligence is processed and analyzed to the extent that it provides clear insights and recommendations, allowing individuals or organizations to act upon it effectively. Key characteristics of actionable intelligence include: • *Relevance:* It pertains directly to the decision-making needs of the user. • *Accuracy:* It is based on reliable and verified data. • *Timeliness:* It is delivered in a time frame that allows for effective action. • *Clarity:* It provides clear and understandable insights and recommendations. • *Specificity:* It offers detailed guidance on what actions to take.	CTI-CMM
Ad hoc	In the context of this model, ad hoc (formed or used for aspecial purpose without policy or a plan for repetition) refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much in the way of organizational guidance, such as a prescribed plan (verbal or written), policy, or training. The quality of the outcome may vary significantly depending on who performs the practice; when it is performed; the context of the problem being addressed; the methods, tools, and techniques used; and the priority given a particular instance of the practice. High-quality outcomes may be achieved with experienced and talented personnel, even if practices are ad hoc.	C2M2

Term	Definition	Source
	However, lessons learned in an ad hoc practice are typically not captured at the organizational level, therefore, approaches and outcomes are difficult to repeat or improve across the organization. It is important to note that, while documented policies or procedures are not essential to the performance of a practice in an ad hoc manner, the effective performance of many practices may result in documented artifacts such as a documented asset inventory or a documented cybersecurity program strategy.	
Asset	For the purposes of the model, assets are IT and OT hardware and software assets, as well as information, essential to operating the function. The definition also includes interconnected or interdependent business and technology systems and the environment in which they operate.	C2M2
Critical infrastructure	Assets that provide essential services underpinning society. Nations possess key resources whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction through terrorist attack could have a debilitating effect on security and economic well-being.	HSPD-7
Cyber risk	The possibility of harm or loss due to unauthorized access, use, disclosure, disruption, modification, or destruction of IT, OT, or information assets. Cyber risk is a function of impact, likelihood, and susceptibility.	C2M2
Cyber threat intelligence (CTI)	A discipline focused on understanding the capabilities, intent, motivations, and opportunities of cyber adversaries and their associated TTPs. CTI insights and recommendations arm stakeholders charged with protecting the organization and reducing risk to its technologies, infrastructure, and the people dependent upon it.	CTI-CMM
Cyber threat landscape (CTL)	Intelligence on past, current, and anticipated events, allowing stakeholder audiences to have a contextual and holistic understanding of the threats they face.	Adapted from ENISA
Cybersecurity program	An integrated group of activities designed and managed to meet cybersecurity objectives for the organization or the function. A cybersecurity program may be implemented at either the organization or the function level, but a higher-level implementation and enterprise viewpoint may benefit the organization by integrating activities and leveraging resource investments across the entire enterprise.	C2M2
Diamond model	A method to accurately detail fundamental aspects of all malicious activity, as well as the core analytic concepts used to discover, develop, track, group, and ultimately counter both the activity and the adversary.	The Diamond Model of Intrusion Analysis
Fraud	Wrongful or criminal deception intended to result in financial or personal gain.	CTI-CMM
Impact	Negative consequences of an event or action. Impact is a key component in understanding the severity of a particular risk. Impact from cybersecurity incidents might include response costs, regulatory fines, and lost income from reputation damage.	C2M2

Term	Definition	Source
Indicator of compromise (IOC)	Evidence indicating an organization's system or network has been compromised or otherwise subjected to malicious activity. This can include IP addresses, domain names, URLs, network traffic patterns, file names, file paths, file hashes, and email addresses. IoCs help security professionals identify, detect, and respond to potential security breaches.	CTI-CMM
Intelligence requirement	The minimum information and critical knowledge gap that informs the necessary actions for defenders and decision-makers to protect the organization across strategic, operational, and tactical levels.	CTI-CMM
Information sharing and analysis centers (ISACs)	Help critical infrastructure or industry entities protect their facilities, personnel, and customers from cyber and physical security threats and other hazards. ISACs collect, analyze, and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency.	National Council of ISACs
Kill chain	The Cyber Kill Chain® framework is part of the Intelligence Driven Defense® model for identification and prevention of cyber intrusion activity. The model identifies what the adversaries must complete to achieve their objective.	Lockheed Martin
Malvertising	Practice of incorporating malware in online advertisements.	CTI-CMM
Multifactor authentication (MFA)	An authentication method requiring the user to provide additional verification factors to access a resource online.	CTI-CMM
Objectives and key results (OKRs)	A framework used by individuals, teams, and organizations to define measurable goals and track their outcomes. Using this framework helps combine company-level objectives with the key results used to measure progress.	CTI-CMM
Operational technology (OT)	In the context of this model, OT assets refer to assets that are on the OT segment of the organization's network and are necessary for service delivery or production activities. Examples include industrial control systems, building management systems, fire control systems, process control systems, safety instrumented systems, Internet-of-Things (IoT) devices, and physical access control mechanisms. Most modern control systems include assets traditionally referred to as IT, such as workstations that use standard operating systems, database servers, or domain controllers.	C2M2
Playbook	Outline high-level strategies and address processes holistically. Playbooks are usually not fully automated but include automation in separate pieces of the overall playbook. These can be used in IR and disaster recovery or overall cyber strategy.	CTI-CMM
Practice	An activity described in the model that can be performed by an organization to support a domain objective. The purpose of these activities is to achieve and sustain an appropriate level of cybersecurity for the function commensurate with the risk to critical infrastructure and organizational objectives.	C2M2
Proof of concept (POC)	A demonstration of how a vulnerability, idea, or method of attack works.	CTI-CMM
Risk profile	A comprehensive analysis and listing of the potential risks an organization faces concerning its IT, OT, and information assets. It encompasses the identification, assessment, and prioritization of risks based on their potential impact and likelihood. The risk profile considers both external and internal threats,	CTI-CMM

Term	Definition	Source
	the potential consequences of different risk vulnerabilities within the organization, and scenarios. By evaluating these factors, a risk profile helps organizations understand their exposure to various threats, guiding the implementation of appropriate risk management strategies and mitigation measures to protect their assets and operations.	
Risk register	A structured repository where identified risks and their subsequent mitigations are recorded to support risk management.	C2M2
Runbook	Pertain to the operation and maintenance of specific tasks and can be either manual or automated. Runbooks are usually seen in security orchestration automation and response (SOAR) automation for intelligence gathering, IR, or disaster recovery.	CTI-CMM
Security information and event management (SIEM)	A log collection tool used to analyze logs for security event data and alerting. Typically used for threat and vulnerability management, security IR, and security operations automation and alerts.	CTI-CMM
Security orchestration automation and response (SOAR)	Typically used in tandem with a SIEM, allowing the security operations team to automate tasks related to incident response, intelligence gathering, alerting, and triage for cases. A comprehensive SOAR product, as defined by Gartner, is designed to operate under three primary software capabilities: threat and vulnerability management, security IR, and security operations automation.	CTI-CMM
Skimmer	Device designed to attach to a PoS system or ATM with the intention of stealing or embezzling money.	CTI-CMM
Stakeholder	Any individual, group, or organization that has an interest in or is affected by the activities, outcomes, and performance of the CTI program. The end consumer of intelligence production and decision-maker.	CTI-CMM
Tactics, techniques and procedures (TTPs)	The behavior of an actor. Tactics are high-level descriptions of behavior, techniques are detailed descriptions of behavior in the context of a tactic, and procedures are even lower-level, highly detailed descriptions in the context of a technique. TTPs could describe an actor's tendency to use a specific malware variant, order of operations, attack tool, delivery mechanism (e.g., phishing or watering hole attack), or exploit.[7]	NIST
Threat intelligence platform (TIP)	A software solution that ingests, analyzes, and enriches cyber threat information from various external and internal feeds and sources to detect and correlate anomalous activity.	CTI-CMM
Threat profile	A characterization of the likely intent, capability, and targets for threats to the function. It is the result of one or more threat assessments across the range of feasible threats to the IT, OT, and information assets of an organization and to the organization itself, identifying feasible threats, describing the nature of the threats, and evaluating their severity.	C2M2
User and entity behavior analytics (UEBA)	The use of algorithms and machine learning to baseline user activity and detect anomalies in behavior.	CTI-CMM
Use case	A hypothetical but plausible scenario demonstrating how a typical user might interact with a product, service, or solution to achieve a specific goal.	CTI-CMM

7 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

Changelog

What's new?

This version did not receive substantive changes to the process or the model itself. We have incorporated feedback received on v1.2 and performed significant fine-tuning on the various domain use cases and practices. You keep sharing your feedback, we keep updating it.

Version	Highlights
0.1	Initial draft.
1.0	First version.
1.1	Processed feedback on V1.0. Created FRAUD domain. Introduced a changelog Published model assessment tool BETA.
1.2	Added Appendices D, E, and F Published v1.0 Assessment Tool
1.3	Processed feedback on v1.2

Acknowledgements

The CTI-CMM is the product of a collective effort by a diverse group of industry professionals who volunteered their expertise. This team, representing a wide range of sectors, geographic regions, backgrounds, and experiences, has a proven track record of designing programs and leading teams at the tactical and strategic levels, encompassing both vendor and consumer roles in the public and private sectors.

Program Creator and Lead:

- Michael DeBolt, Intel 471

Version 1.3 Committee Leads

- Gert-Jan Bruggink, Venation
- Neal Dennis, VulnCheck
- John Holland, IntL8
- Kevin Holvoet, Centre for Cybersecurity Belgium (CCB)
- Brian Mohr, HCA Healthcare
- John Suver, Bank of America
- Goncalo Ribeiro, Europol EC3

Program Co-Lead:

- Colin Connor, IBM

Version 1.3 Contributing Members

- Caitlin Fernandez, TD Bank
- Freddy Murstad, NF-CERT
- Prescott Pym, Cosive
- Mark Thomasson, LetsData
- Lance Taylor, Clear

Advisors

- Freddy Dezeure, Advisor
- Michael Haas, Kroger
- Katie Nickels, Red Canary
- Visi Stark, The Vertex Project
- Rick Holland, ReliaQuest
- Joseph Opacki, Advisor
- Andreas Sfakianakis, SAN

To build a successful CTI program, it's essential to focus on the needs of your stakeholders and align your capabilities with their activities to create value for your organization.

Built by industry experts, the CTI Capability Maturity Model (CTI-CMM) can help your team build its capabilities and bridge the gap with stakeholders. Individuals from cross-organizational teams can use this Model to contribute to CTI program maturity.

Join the CTI-CMM Community at **cti-cmm.org**

This publication is sponsored by Intel 471, a leading provider of cyber threat intelligence. Intel 471 empowers security teams to be proactive with relevant and timely solutions driven by our cyber underground insights.

Learn more at **intel471.com**.