CTI CMM

CYBER THREAT INTELLIGENCE CAPABILITY MATURITY MODEL

Industry Inspired. Industry Led.

While this publication is designed to provide accurate information regarding the subject matter covered, it is provided on an “as is” and “with all faults” basis, and the authors are not rendering legal, technical, or other professional services. While the authors have used their best efforts in preparing this publication, they make no representations or warranties with respect to this publication, including, but not limited to, the accuracy or completeness of the contents thereof, and specifically disclaim representations or warranties of any kind, express or implied, including, but not limited to, any warranties of merchantability, non-infringement, or fitness for a particular purpose. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional when appropriate. The authors shall not be liable for any loss of profit or any other type of damages, including but not limited to special, incidental, consequential, personal, or other damages, whether or not arising from any reliance on this publication.

For permissions, visit **cti-cmm.org**.

Cyber Threat Intelligence Capability Maturity Model

Version 1.0

Contents

Acknowledgements

The CTI-CMM is the product of a collective effort by a diverse group of 27 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 Lead:

- Michael DeBolt, Intel 471

Program Co-Lead:

- Colin Connor, IBM

Domain and Section Leads

- Nicole Beckwith, Kroger
- Gert-Jan Bruggink, Venation
- John Doyle, Mandiant
- John Holland, IntL8
- Brian Mohr, Reqfast

Platinum Contributors

- John Fokker, Trellix
- Clay Hamilton, Autodesk
- Kevin Holvoet, Centre for Cybersecurity Belgium (CCB)
- Michel Mollema, Northwave Cyber Security
- Alexander Perez Palma, Workday
- Lauren Proehl, Marsh McLennan
- Kobe Shwartz, Signify
- Scott Small, Tidal Cyber
- John Suver, CTI Financial Services Sector

Special Thanks To:

- Louise Brown
- Yonatan Israel Garzon, Mastercard
- Coleman Kane, DeepSeas
- Ian Thompson, BP
- Jurgen Visser, Gojek
- Nathan Weilbach

Advisors

- Freddy Dezeure, Advisor
- Michael Haas, Kroger
- Rick Holland, ReliaQuest
- Joseph Opacki, Advisor
- Andreas Sfakianakis, SAND

Foreword

With threats coming at us at an unprecedented pace, the need for mature cyber threat intelligence (CTI) programs is critical. For a large organization like Kroger, the stakes are high — not only for financial loss, but also in maintaining customer trust and operational resilience. This new model sheds light on how to easily implement CTI into your day to day operations and move teams toward developing or enhancing their capabilities.

For decision makers and leaders this model serves as a way to navigate the complexities of CTI and drive intelligence based business decisions. The framework reduces risk by promoting a greater understanding of CTI's role in safeguarding your assets and landscape.

As you read through this maturity model consider what pieces are easily implemented into your organization's program today, and what you can plan for tomorrow. By embracing this model, companies like Kroger can stay ahead of the ever evolving threat landscape.

— *Michael Haas, Vice President, Information Security, The Kroger Co.*

The cyber threat landscape is unrelenting, growing in scale and impact year after year. Defenders are overwhelmed and seeking ways to reduce risks and protect their organizations' critical assets. CTI is a vital capability in addressing the threat landscape. Although CTI has existed for well over a decade, many organizations are still early in their journeys and have yet to realize its full potential. This CTI-CMM will help organizations assess their current maturity level and provide a blueprint to grow their program. It will be useful across the spectrum of tactical, operational, and strategic intelligence work and benefit practitioners and leaders alike. I wish I had this framework when I was building out my first CTI team years ago.

Diversity is a critical foundation of any intelligence shop; analysts who look the same, sound the same, and come from a similar background will produce flawed intelligence products. As expected, a diverse group of intelligence professionals developed this model based on their extensive experience. As a result, there will be critical takeaways for everyone, from advanced teams wanting to become leading teams to teams just starting. I encourage readers to leverage this model in their programs and use it as a playbook to take their CTI programs to the next level.

— *Rick Holland, Vice President, Chief Information Security Officer, ReliaQuest*

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 CTI program relies on its ability to bring value to your 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 your CTI program, it is necessary to build your 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 requires alignment with the capabilities of each stakeholder it supports. This CTI Capability Maturity Model (CTI-CMM) is designed to support your CTI team in building its 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 — constant improvement is crucial for success.

- The model is not claimed by a single commercial party.

1.2.2. Shared Principles

- Contextualizing threat intelligence 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
Initiate the CTI-CMM project	October 2023	Complete
Define purpose and scope of the model	November 2024	Complete
Create model development approach and objectives	December 2024	Complete
Publish and present “sneak peek” at SANS CTI Summit	January 2024	Complete
Finalize a first draft version of the CTI-CMM	July 2024	Complete
Gather and review advisor feedback	July 2024	Complete
Conduct pilot test and external validation	July 2024	Complete
Publish CTI-CMM version 1	Aug. 5 2024	Complete
Review community feedback	October 2024	Pending
Publish CTI-CMM version 1.1, including • Community feedback • FRAUD domain	December 2024	In Progress

Publish Appendices, including: • CTI Metrics and Measurements • CTI Data Source Descriptions and Matrix	Q1 2025	In Progress
Publish model assessment tool	Q2 2025	Pending
Publish model templates, guides, samples (examples: program plans, stakeholder management guides, etc.)	2025	Pending

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
- 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:** Introduces the model and details the model's purpose, intended audience, and the organization of the content within this document.
- **Section 3:** Describes the three CTI foundations that guide 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, 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.

- **Decision-makers:** Sections 1, 2, and 3
- **Leaders or 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 it supports; therefore, it was not developed in a vacuum. 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

[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

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

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 threat intelligence 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 lifecycle to collect, process, analyze, and deliver 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 Appendix B.

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, and aligning initiatives with organizational goals, producing high-level reports and risk assessments.
- **Operational CTI** supports specific campaigns, providing relevant and actionable intelligence for infrastructure, security operations, incident response, and threat intelligence 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 such as law enforcement agencies may use "Strategic, Tactical, Operational" in their organizational order from top to bottom, flipping the last two terms. 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.**

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

3.4. CTI Program Foundations

This section covers fundamental elements of a CTI program. The establishment of these core components creates a foundation for maturity and capability.

> **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 Oversight and Governance Documentation**
> **– Establish the CTI Program Strategy**
> **– Establish and Maintain the CTI Program**

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.

> **Key Concept: 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 risk to critical infrastructure and organizational objectives.

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

> Key Concept: 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**

4. How the Model is Organized

Similar to the C2M2, the CTI-CMM is organized into 10 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.

Domain	Domain Purpose	CTI Mission
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.

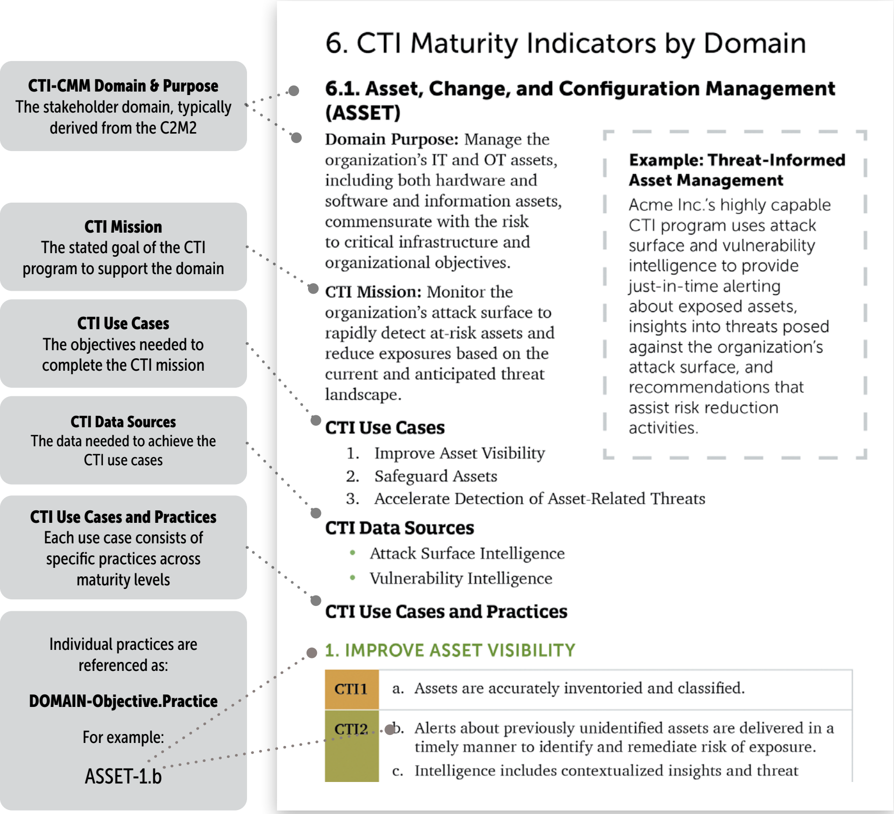
Domain	Domain Purpose	CTI Mission
Event and Incident Response, Continuity of Operations RESPONSE	Establish and maintain plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity events and incidents and to sustain operations during cybersecurity incidents 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 threat intelligence insights and recommendations.
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.

Domain	Domain Purpose	CTI Mission
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 MANAGEMENT	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.

Domain	Domain Purpose	CTI Mission
Fraud and Abuse Management ***(Coming soon)*** 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.

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.



CTI-CMM Domain & Purpose
The stakeholder domain, typically derived from the C2M2

CTI Mission
The stated goal of the CTI program to support the domain

CTI Use Cases
The objectives needed to complete the CTI mission

CTI Data Sources
The data needed to achieve the CTI use cases

CTI Use Cases and Practices
Each use case consists of specific practices across maturity levels

Individual practices are referenced as:

DOMAIN-Objective.Practice

For example:

ASSET-1.b

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.

Example: Threat-Informed Asset Management
Acme Inc.'s highly capable 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.

CTI Use Cases

1. Improve Asset Visibility
2. Safeguard Assets
3. Accelerate Detection of Asset-Related Threats

CTI Data Sources

- Attack Surface Intelligence
- Vulnerability Intelligence

CTI Use Cases and Practices

1. IMPROVE ASSET VISIBILITY

CTI1	a. Assets are accurately inventoried and classified.
CTI2	b. Alerts about previously unidentified assets are delivered in a timely manner to identify and remediate risk of exposure. c. Intelligence includes contextualized insights and threat

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 ad-hoc or unplanned, with a focus on reactive intelligence that delivers short-term results.
CTI2 Advanced	• Advanced practices are performed at a higher level than CTI1. • Practices are mostly planned and routine, with a focus on proactive and predictive intelligence that delivers short- and intermediate-term results.
CTI3 Leading	• Leading practices are performed at a higher level than CTI2. • Practices include a focus on prescriptive intelligence and recommendations that deliver long-term strategic results. • Practices are measurable and aligned to business outcomes.

5. How to Use This Model

The CTI-CMM is meant to be used as a reference framework 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.

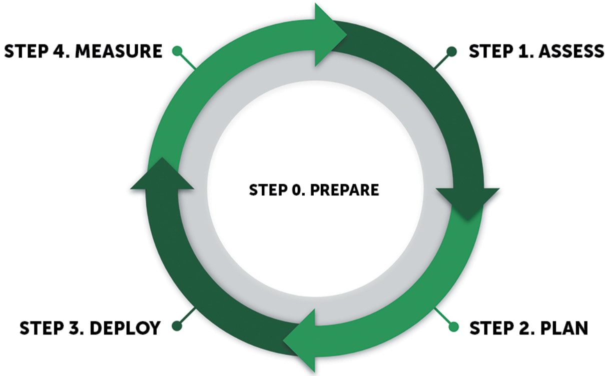


Figure 2. CTI-CMM Implementation Process

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 Appendix B.

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?

> **Key Concept: 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.

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?

The authors have seen a variety of frameworks 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.

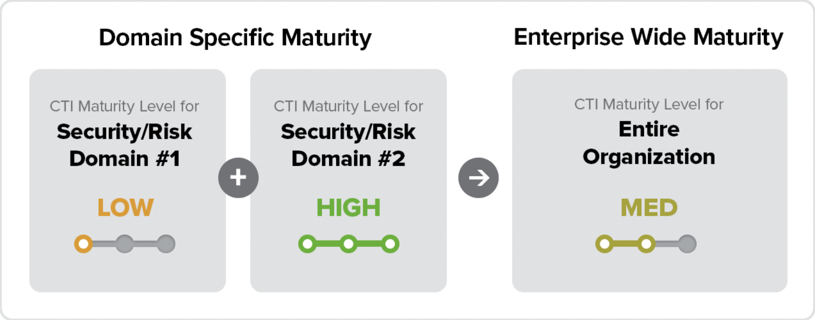


Figure 3. Domain-Specific and Enterprise Maturity Level Relationship

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.

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. Improve Asset Visibility
2. Safeguard Assets
3. Accelerate Detection of Asset-Related Threats

CTI Data Sources

- Attack Surface Intelligence
- Vulnerability Intelligence
- Dark Web Intelligence
- Breach Intelligence
- Open Source Intelligence

Example: Threat-Informed Asset Management

Acme Inc.’s highly capable 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 threat intelligence that shapes asset deployment and configuration strategies.

CTI Use Cases and Practices

1. IMPROVE ASSET VISIBILITY

CTI1	a. Assets are accurately inventoried and classified.
CTI2	b. Alerts about previously unidentified assets are delivered in a timely manner to identify and remediate risk of exposure. c. Intelligence includes contextualized insights and threat assessments to continuously improve asset discovery practices and predict future scenarios based on the threat environment.
CTI3	d. Intelligence regularly includes prescriptive threat analysis and recommendations to support asset discovery and risk assessments. e. Intelligence supports regulatory requirements by providing evidence-based information on how assets are protected against known threats. f. ASSET domain objectives focused on identifying and prioritizing mitigation efforts are regularly informed by threat intelligence insights to ensure a comprehensive view of the organization's ecosystem.

2. SAFEGUARD ASSETS

CTI1	a. A tiered and prioritized list of assets — based on their targeting, criticality, vulnerability, and potential impact in case of attack or exposure — is maintained by the CTI program.
CTI2	b. Intelligence supports proactive risk mitigation efforts by providing contextualized insights, predictive assessments, and alerting about threats and vulnerabilities that could affect priority assets.
CTI3	c. Intelligence includes prescriptive threat analysis and recommendations to protect current and pre-deployed assets and change configurations based on the threat environment.

	d. ASSET domain risk reduction strategies are consistently informed by threat intelligence insights. e. Intelligence program is part of the asset purchase cycle informing the organization about risks to certain appliances/tools (e.g., specific hardware that has been targeted in the past).

3. ACCELERATE DETECTION OF ASSET-RELATED THREATS

CTI1	a. Selected personnel are assigned to monitor and triage potential threats and vulnerabilities impacting priority assets. b. Alerts about threats against priority assets are delivered at least in an ad hoc manner.
CTI2	c. Alert dissemination is integrated into repeatable workflows for ASSET domain triage and rapid response, advancing early detection warnings for priority assets. d. Intelligence on emerging threats and exploits supports rapid response and remediation, reducing the window of exposure for assets. e. Intelligence identifies vulnerabilities that directly affect priority assets, allowing the organization to prioritize patching efforts. (see THREAT)
CTI3	f. Continuous monitoring is extended to include all assets across each tier level. g. Intelligence about the threat environment is used to continuously refine and improve detection strategies and security posture, enabling the organization to focus efforts on protecting the most critical assets based on threat intelligence insights.

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. Improve Detection Engineering
3. Enhance Threat Hunting
4. Inform Offensive Security Operations
5. Improve Patch Prioritization

CTI Data Sources

- Attack Surface Intelligence
- Dark Web Intelligence
- Adversary Intelligence
- Malware Intelligence
- Vulnerability Intelligence
- Open Source Intelligence
- Breach Intelligence

Example: Threat-Informed 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 in a mostly ad hoc manner (e.g., over email) to support prevention and blocking.
CTI2	b. IoC/B/As are collected from external feeds (usually segmented by specific types of threats, e.g., phishing hosts, botnets, command-and-control (C2) hosts) and delivered directly to security technologies (e.g., security information and event management (SIEM) or firewall solutions) in a mostly automated fashion. c. Indicator ingestion and pruning occurs on regular cadences (e.g., weekly or daily).
	d. Ad hoc steps are taken to account for identified false positives. e. Some level of threat context (e.g., type of threat, attack stage) is also provided to aid operator awareness. f. Threat context input is provided to the organization's training and education material and is aligned with observed cyber threat activities.
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. Polling for fresh indicators occurs on very regular cadences where relevant (e.g., hourly or daily for indicators with high entropy). i. False positives are identified and accounted for regularly. j. Threat context (e.g., type of threat, attack stage, detection time stamps for relevance) is provided for most indicators to aid operator awareness.

CTI3	k. Ingested indicators connect to automation playbooks and trigger COAs where relevant (e.g., automating implementation of low-regret blocking or phishing response). l. Original indicators are identified within 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. IMPROVE DETECTION ENGINEERING

CTI1	a. Alerts about adversaries actively posing potential threats to the organization are delivered in a mostly 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 threat intelligence 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 highlight opportunities for detecting relevant threat activity within event log data.

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 ad hoc 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 infrastructure.
CTI3	e. RFIs are issued and fulfilled to 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 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.

[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.

	e. Insights focus on threats pertaining to the organization's unique threat profile but also novel procedures that may not yet be actively abused 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 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 dark web 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.

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 controls by identifying relevant threats and estimating likelihood and potential impact.

CTI Use Cases

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

CTI Data Sources

- Risk Management Framework, Processes, and Systems (including Risk Register)
- Vulnerability Intelligence
- Dark Web Intelligence
- Breach Intelligence
- Attack Surface Intelligence
- Identity Intelligence

Example: Threat-Informed Risk Management

Acme Inc.'s CTI team possesses an in-depth understanding of the company's risk management framework, 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 threat intelligence, including insights on vulnerabilities, dark web 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 organization's risk management strategy and framework are understood, at least in a basic manner. b. Collaboration with risk management stakeholders is conducted in an ad hoc manner.
CTI2	c. CTI practices are initially aligned to the organization's risk management strategy and framework at least in an ad hoc manner, focused on translating insights to risk in limited CTI processes. 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 are aligned and synchronized with a risk framework adopted by the organization, such as NIST 800-30[3] and the NIST Cybersecurity Framework.[4] g. CTI insights are used to prioritize risk-based decisions and actions based upon the threat landscape. If possible, risks identified from CTI insights are integrated into risk management dashboards. (see ARCHITECTURE) h. CTI establishes a governance model for continuous alignment with risk management strategies, with a focus on implementing automation and enhancing processes. (see PROGRAM)

[3] https://csrc.nist.gov/pubs/sp/800/30/r1/final

[4] https://www.nist.gov/cyberframework

2. IMPROVE RISK DECISIONS, ASSESSMENTS, AND CONTROLS

CTI1	a. Threats are identified, analyzed, and triaged for response at least in an ad hoc manner and mostly independent of the organization's risk management strategy. b. The CTI program maintains a basic understanding of organizational assets, controls, operating environment, and risk posture.
CTI2	c. A process for integrating CTI into risk assessments is created and used to inform basic risk controls and mitigations efforts. d. CTI insights are leveraged for risk assessment methodologies, at least in an ad hoc manner. e. Risk-based controls are intermittently assessed and adjusted using CTI insights.
CTI3	f. CTI practices proactively advise and inform risk mitigation and management strategies across the organization, including risk scenario planning and simulation exercises. (see SITUATION) g. Risk assessment models and processes routinely leverage CTI insights. h. Risk-based controls and decisions are routinely and continuously assessed and adjusted using CTI insights.

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
- Vulnerability Intelligence
- Dark Web Intelligence
- Breach Intelligence
- Identity Intelligence

Example: Threat-Informed 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 threat intelligence 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	c. Alerts about leaked or compromised credentials and identities from open and commercial sources are delivered at least in an ad hoc manner. d. Alerts about vulnerabilities impacting identity-related systems that threaten unauthorized access or identity compromise are delivered in an ad hoc manner for patch prioritization. (see THREAT)
CTI2	e. Alert dissemination is integrated into repeatable and automated workflows for ACCESS domain rapid triage and response. f. Intelligence on emerging malware and associated indicators is delivered to enhance early warning detections and proactive mitigation measures.
CTI3	g. Continuous monitoring is extended to identity-related threats posed by third parties. (see THIRD-PARTIES) h. 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. i. Intelligence includes contextualized insights and threat assessments to continuously improve identity-related discovery practices and predict future scenarios to enhance detections.

2. FORTIFY IDENTITY AND ACCESS PROTECTION

CTI1	a. The CTI program 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. The CTI program 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. 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. Insights regularly inform the creation of threat scenarios and simulations to test, validate, and adjust authentication and access controls and mitigations. (see THREAT) g. 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

- Current Events in the Organization (including IT operations, M&A, and more)
- Dark Web Intelligence
- Open Source Intelligence
- Geopolitical Intelligence
- ISACs
- Trust Groups

Example: Threat-Informed Situational Awareness

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.

Acme fuses information from multiple sources including open source news feeds, information sharing and analysis center (ISAC) partners, industry trust groups, commercial threat intelligence 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.

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, closed, and commercial sources. b. Insights are provided in an hoc manner for short-term trends and observations that lead to immediate COAs. c. Collection is focused primarily on all threats relevant specifically to the organization.
CTI2	d. A systematic process, such as the one described in the ENISA Cybersecurity Threat Landscape Methodology,[5] is implemented to routinely produce CTLs. e. CTL scope is mostly tactical and operational, delivering insights that provide short- to medium-term results. f. CTL audience and dissemination is to most enterprise stakeholder domains. g. CTL focus is primarily on priority threats and trends specific to the organization.
CTI3	h. CTL scope is extended to include deliverables that regularly provide prescriptive intelligence to inform long-term strategic decision-making and align with risk reduction strategies. (see RISK) i. CTL audience and dissemination is to all enterprise stakeholder domains based on PIRs. (see PROGRAM) j. CTL focus is extended to include threats, events, and trends relevant to the organization's industry and geographic representation. (see THREAT)

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

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

- Breach Intelligence
- Attack Surface Intelligence
- Adversary Intelligence
- Malware Intelligence
- Open Source Intelligence
- Internal Event Data

Example: Threat-Informed 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.

1. STRENGTHEN PRE-INCIDENT PREPAREDNESS

CTI1	a. Event and incident data is collected and correlated with external open and commercial sources to rapidly detect and remediate threats in an automated manner. b. CTI insights and context are provided in an ad hoc manner to enrich event data, reduce false positives, and hasten response.
CTI2	c. Events detected by the IR team are regularly enriched with CTI insights and context to improve response efficacy. d. CTI insights are used for immediate control gap detection analysis and rapid remediation, conducted in a mostly automated manner.
CTI3	e. CTI insights include threat landscape assessments 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 in conjunction with the Kill Chain and Diamond Model, and findings are shared in real time to the IR team. b. Findings are documented as the incident progresses through the lifecycle phases. CTI insights are incorporated into the IR report.
CTI2	c. Manual research and pivoting on TTPs and IoCs is being conducted to contextualize incidents and improve remediation. d. Findings are documented in a stand-alone CTI report and can be incorporated into or accompany the IR report. e. Automated intelligence is used to enrich the IR process.

CTI3	f. IoCs and related intelligence are integrated into the threat intelligence platform (TIP) and existing security stack. g. Automated intelligence is 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)

2. ENHANCE POST-INCIDENT RECOVERY AND CONTINUITY OF OPERATIONS

CTI1	a. TTPs are presented against the Kill Chain, Diamond Model, and MITRE ATT&CK to highlight detection and prevention gaps. b. Enrichment of SOC internal indicators and data continues with intelligence via manual ingestion.
CTI2	c. IR time is reduced through automation. Key prevention measures are implemented with IoCs and TTPs from trusted sources. d. Artificial intelligence (AI) and machine learning (ML) are used for analysis of TTP mapping (MITRE TRAM).
CTI2	e. Incident TTPs are mapped to the MITRE ATT&CK framework and reviewed against current detection and prevention capabilities. f. Enrichment of SOC internal indicators and data continues with intelligence via TIP or automation. g. Partnership with the threat hunting team is initiated for ongoing collaboration. (see THREAT)
CTI3	h. Threat hunting activities are enriched through CTI and runbooks are enriched based on threat actor TTPs. (see THREAT) i. Automated and semi-automated CTI runbooks are used for enrichment. 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 threat intelligence insights and recommendations.

CTI Use Cases

1. Accelerate Detection of Third-Party Threats
2. Mitigate Third-Party Risk Exposure

CTI Data Sources

- Dark Web Intelligence
- Attack Surface Intelligence
- Breach Intelligence
- Vulnerability Intelligence

Example: Threat-Informed 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 and Practices

1. ACCELERATE DETECTION OF THIRD-PARTY THREATS

CTI1	a. Vendors are tiered based on their risk rating assessments. b. Vendors are categorized by demographics including industry and geography.
CTI2	c. Specialized third-party risk management (TPRM) tooling is used to catalog, monitor, and record changes to vendor risk ratings based on the threat environment. d. Intelligence about threats against third parties regularly includes predictions and contextualization to reduce risks posed by current and anticipated threats.
CTI3	e. Intelligence about threats against third parties regularly includes prescriptive analysis and recommendations to proactively protect the organization against current and anticipated incidents.

2. MITIGATE THIRD-PARTY RISK EXPOSURE

CTI1	a. Selected personnel are assigned to monitor and triage potential third-party exposures involving top-tier vendors. b. Alerts are provided in an ad hoc manner for third-party incidents gleaned primarily from open sources.
CTI2	c. Continuous and automated monitoring and alerting is in Continuous and automated monitoring and alerting is in place for top-tier vendors to alert of potential threats emanating from open and commercial sources. d. Intelligence about third-party exposures consistently includes predictive analysis about the likelihood and impact of a potential threat against the organization.
CTI3	e. Monitoring is extended to include all vendors across each tier level.

f. Intelligence includes prescriptive analysis about recommended COAs to reduce risk of exposure to the organization via third-party incidents.

g. Detections and playbooks are created and regularly tuned based on the threat environment and organizational risk.

6.8. 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

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

Example: CTI 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 on at least an ad hoc basis. b. Insights provided by the CTI program are generally relevant to the organization, but not necessarily aligned to specific organizational units or job roles.

CTI1	c. Workforce training/education initiatives are supported by CTI insights on at least an ad hoc basis 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 the CTI team 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 is 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.

6.9. 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 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. T

CTI Use Cases

1. Inform Architecture Strategy to Improve Infrastructure Resilience
2. Support Prioritization of Cybersecurity Initiatives
3. Drive CTI Tools and Infrastructure Integration

CTI Data Sources

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

Example: CTI 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 and organizational behavior.

CTI Use Cases and Practices

1. INFORM ARCHITECTURE STRATEGY TO IMPROVE INFRASTRUCTURE RESILIENCE

CTI1	a. Organizational cybersecurity architecture strategy is understood by the CTI team and support is provided on at least an ad hoc basis. b. The CTI team is familiar with the personnel responsible for cybersecurity architecture planning and views them as stakeholders of the CTI program.
CTI2	c. The CTI program regularly advises on gaps in cybersecurity architecture based on threat landscape trends. (see THREAT) d. Elements of the cybersecurity architecture plan are integrated into the process of creating the organization's threat profile. (see THREAT)
CTI3	e. Cybersecurity architecture is proactively reviewed on a routine basis to ensure it accounts for changes in the organization's risk analysis information (see RISK) and threat profile. (see THREAT)

2. SUPPORT PRIORITIZATION OF CYBERSECURITY INITIATIVES

CTI1	a. Recommendations are provided on at least an ad hoc basis for cybersecurity architecture initiatives based upon the organization's threat landscape. (see THREAT) b. The CTI program uses the organization's Asset Inventory system, Change Management Database (CMDB), and Risk Register (see RISK) to gain a basic understanding of organizational assets, controls, operating environment, and risk posture.
CTI2	c. The CTI team leverages the Asset Inventory system and CMDB to help advise on newly discovered vulnerabilities, determine potential impact, and provide focused insights.

CTI2	d. A standardized approach to using business impact analysis, risk analysis information (see RISK), and threat profiling (see THREAT) is used to produce recommendations and guidance on the establishment and maintenance of the cybersecurity architecture.
CTI3	e. The CTI program maintains awareness of key cybersecurity architecture initiatives and proactively prepares inputs. f. Teams responsible for cybersecurity architecture trust the CTI program and routinely engage it for insights and support.

3. DRIVE CTI TOOLS AND INFRASTRUCTURE INTEGRATION

CTI1	a. Use of CTI tools across the organization is ad hoc and largely stand-alone. CTI tools are used almost exclusively for threat intelligence research and correlation. b. Integration with IR platforms is ad hoc and implemented only as organization’s risk analysis (see RISK) and threat profile require. (see THREAT)
CTI2	c. CTI tools and infrastructure are integrated with IR platforms to provide context and accelerate investigations.
CTI2	d. CTI tools and infrastructure are integrated with monitoring and detection technologies — such as SIEM, firewall, proxy, intrusion prevention system (IPS), web application firewall (WAF), or endpoint detection and response (EDR) solutions — to enhance and automate prevention and detection processes. (see RESPONSE) e. Identity and access protection capabilities are fortified to prevent attacks, such as credential stuffing and account takeover (see ACCESS), through the integration of CTI tools and infrastructure.
CTI3	f. CTI tools and infrastructure are used to support implementation of ML models for anomaly detection, behavioral analytics, and threat prediction.

6.10. 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: Empower informed decision-making for the entire cybersecurity program by aligning CTI operations to the organization’s strategic goals and delivering tailored intelligence inputs to inform cybersecurity decision-making from tactical to strategic levels.

CTI Use Cases

1. Integrate and Align CTI Program Strategy
2. Maintain and Improve CTI Program
3. Support Cybersecurity Management in Program Alignment Efforts

CTI Data Sources

- Applicable Data Sources from Other Domains
- Cybersecurity Organization’s Cybersecurity Program Documentation
- Organizational Annual Reporting (10-K, 8-K, Annual Report, etc.)
- Organization’s Objectives and Key Results (OKRs) (also including strategic directives)

Example:CTI 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 is essential during periods of business expansion, globalization, and when protecting high-value assets and sensitive data. Acme Inc is driven by the lessons learned from past incidents, mandates from the board and executive leadership, and the need to align cybersecurity efforts with broader business objectives and risk tolerance levels.

CTI Use Cases and Practices

1. INTEGRATE AND ALIGN CTI PROGRAM STRATEGY

CTI1	a. The organization has a CTI program strategy, which may or may not align to the organization's greater cybersecurity program and is managed in an ad hoc manner. CTI program strategic documentation is incomplete and/or not up to date.
CTI2	b. The CTI program strategy defines goals and objectives for the organization's CTI activities along with the structure and organization of the program. 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. The CTI program strategy defines the organization's approach to provide program oversight and governance for CTI activities. d. The cybersecurity program strategy identifies any applicable standards compliance frameworks that must be satisfied by the CTI program (e.g., FFIEC, NIST CSF, NIS2, ISO27001, SOX, GLBA, etc.).
CTI3	e. The CTI program strategy is updated periodically and according to defined triggers, such as business changes, or changes to the risk and threat profile. f. The CTI program strategy closely aligns its objectives and key results to the organization's cybersecurity program objectives, ensuring all domains, especially WORKFORCE and ARCHITECTURE, are working in concert.

2. MAINTAIN AND IMPROVE CTI PROGRAM

CTI1	a. Senior management with proper authority provides support for the CTI program, at least in an ad hoc or informal manner.

CTI2	b. The CTI program is established according to the organization's overall cybersecurity program strategy. c. Senior management sponsorship for the CTI program is visible and active. d. Responsibility for the CTI program is assigned to a role with sufficient authority. e. Stakeholders for CTI program management activities are identified and actively involved.
CTI3	f. CTI program activities are periodically reviewed and improved upon to ensure they align with and support the cybersecurity program strategy. g. CTI activities are independently reviewed to ensure conformance with cybersecurity policies and procedures, periodically and according to defined triggers, such as process changes. h. The CTI program addresses and enables the achievement of legal and regulatory compliance, as appropriate. i. The CTI element collaborates with external entities to contribute to the development and implementation of cybersecurity standards, controls, guidelines, leading practices, lessons learned, and emerging technologies.
CTI3	j. The effectiveness of activities in the PROGRAM domain is evaluated and tracked for the purpose of continuous improvement.

3. SUPPORT CYBERSECURITY MANAGEMENT IN PROGRAM ALIGNMENT EFFORTS

CTI1	a. No practice at MIL1.
CTI2	b. Documented procedures are established, followed, and maintained for activities in the PROGRAM domain. c. Adequate resources (people, funding, and tools) are provided to support activities in the PROGRAM domain.

CTI3	d. Up-to-date policies or other organizational directives define requirements for activities in the PROGRAM domain and CTI program documentation is “living documents.” e. Responsibility, accountability, and authority for the performance of activities in the PROGRAM domain are assigned to personnel. f. Personnel performing activities in the PROGRAM domain have the skills and knowledge needed to perform their assigned responsibilities. (see WORKFORCE) g. The effectiveness of activities in the PROGRAM domain is evaluated and tracked for the purpose of continuous improvement.

Appendices

A. 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
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	C2M2

Term	Definition	Source
	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. 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.	HSPD-7

Term	Definition	Source
	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.	
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

Term	Definition	Source
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
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
multifactor authentication (MFA)	An authentication method requiring the user to provide additional verification factors to access a resource online.	CTI-CMM

Term	Definition	Source
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 con-	CTI-CMM

Term	Definition	Source
	cerning 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, vulnerabilities within the organization, and the potential consequences of different risk 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

Term	Definition	Source
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
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
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.[6]	NIST
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

[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

B. 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 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 threat intelligence 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 threat intelligence 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 threat intelligence.
- ***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

threat intelligence.

Academic and Research Institutions:

- ***Universities and Research Centers:*** Conduct cybersecurity research and develop new threat intelligence 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.

C. Strategic, Operational, and Tactical Overview

	Definition	Typical Responsibilities	Typical CTI Products
Strategic	Strategic threat intelligence 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 threat intelligence 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 threat intelligence sharing with industry peers and partners. • Translate strategic insights into concrete operational plans.	• Threat Intelligence 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 threat intelligence 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.

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**.