CTI-CMM Maturity Assessment

Executive Report

Project: Demo Assessment - Complete Example
Assessment Date: November 20, 2025

Executive Summary

This report presents a comprehensive Cyber Threat Intelligence Capability Maturity Model (CTI-CMM) assessment for **Demo Assessment - Complete Example**. The assessment evaluates current maturity levels across 11 stakeholder domains and provides a strategic roadmap for achieving target maturity levels.

Key Findings:
• **11** of 11 domains have been assessed
• **11** domains have target maturity levels defined
• **11** domains require improvement to reach their targets

Current Maturity Distribution

• **CTI0:** 4 domains (36%)
• **CTI1:** 5 domains (45%)
• **CTI2:** 2 domains (18%)

Maturity Level Overview

Domain	Current Level	Target Level	Gap
ASSET	CTI1	CTI2	1 level
THREAT	CTI2	CTI3	1 level
RISK	CTI0	CTI1	1 level
ACCESS	CTI1	CTI2	1 level
SITUATION	CTI0	CTI1	1 level
RESPONSE	CTI1	CTI2	1 level
THIRD-PARTIES	CTI0	CTI1	1 level
FRAUD	CTI1	CTI2	1 level
WORKFORCE	CTI0	CTI1	1 level
ARCHITECTURE	CTI1	CTI2	1 level
PROGRAM	CTI2	CTI3	1 level

Strategic Roadmap

Domain	Current → Target	Priority	Owner
ASSET	CTI1 → CTI2	90-Day Goal	John Smith
THREAT	CTI2 → CTI3	6-Month Goal	Sarah Johnson
RISK	CTI0 → CTI1	Quick Win	Mike Davis
ACCESS	CTI1 → CTI2	90-Day Goal	Lisa Chen
SITUATION	CTI0 → CTI1	Quick Win	Tom Wilson
RESPONSE	CTI1 → CTI2	90-Day Goal	Emma Brown
THIRD-PARTIES	CTI0 → CTI1	Long-term	David Lee
FRAUD	CTI1 → CTI2	6-Month Goal	Anna Martinez
WORKFORCE	CTI0 → CTI1	Long-term	Chris Taylor
ARCHITECTURE	CTI1 → CTI2	90-Day Goal	Patricia White
PROGRAM	CTI2 → CTI3	Long-term	Robert Anderson

Gap Analysis by Priority

Quick Win

RISK (CTI0 → CTI1)
Required Practices: 4 practices need to be implemented

- **RISK-1.a:** Threats relevant to the organization are understood and their relation to the risk management strategy, at least in a basic manner. *(Task: Risk Integration, Priority: Quick Win, Owner: Mike Davis, Target: 2025-12-20)*
- **RISK-1.b:** Collaboration with risk management stakeholders is conducted in an ad hoc manner.
- **RISK-2.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.
- **RISK-2.b:** The CTI program maintains a basic understanding of organizational assets, controls, operating environment, and risk posture.

Notes: Quick win opportunity. Basic risk management integration with CTI.

SITUATION (CTI0 → CTI1)
Required Practices: 3 practices need to be implemented

- **SITUATION-2.a:** Integrate CTI into security operations
- **SITUATION-1.a:** CTI insights are provided in an ad hoc manner for short-term trends and observations that lead to immediate COAs. *(Task: Situational Awareness, Priority: Quick Win, Owner: Tom Wilson, Target: 2025-12-20)*
- **SITUATION-1.b:** Collection is focused primarily on all threats relevant specifically to the organization.

Notes: Establish basic situational awareness capabilities.

90-Day Goal

ASSET (CTI1 → CTI2)
Required Practices: 6 practices need to be implemented

• **ASSET-1.b:** Alerts about previously unidentified assets are delivered in a timely manner to identify and remediate risk of exposure. *(Task: Q1 Infrastructure, Priority: Quick Win, Owner: John Smith, Target: 2025-12-20)*
• **ASSET-1.c:** Intelligence includes contextualized insights and threat assessments to continuously improve asset discovery practices and predict future scenarios based on the threat environment. *(Task: Q1 Infrastructure, Priority: Quick Win, Owner: John Smith, Target: 2025-12-20)*
• **ASSET-2.b:** Intelligence supports proactive risk mitigation efforts by providing contextualized insights, predictive assessments, and alerting about threats and vulnerabilities that could affect priority assets. *(Task: Q2 Configuration, Priority: 90-Day Goal, Owner: John Smith, Target: 2026-02-18)*
• **ASSET-3.c:** Alert dissemination is integrated into repeatable workflows for ASSET domain triage and rapid response, advancing early detection warnings for priority assets.
• **ASSET-3.d:** Intelligence on emerging threats and exploits supports rapid response and remediation, reducing the window of exposure for assets.
• **ASSET-3.e:** Intelligence identifies vulnerabilities that directly affect priority assets, allowing the organization to prioritize patching efforts. (see THREAT)
Notes: Focus on critical asset inventory and configuration management. Key priority for Q1.

ACCESS (CTI1 → CTI2)
Required Practices: 6 practices need to be implemented
• **ACCESS-3.a:** Monitor privileged access using threat intelligence
• **ACCESS-1.c:** Alert dissemination is integrated into repeatable and automated workflows for ACCESS domain rapid triage and response. *(Task: Identity Management, Priority: 90-Day Goal, Owner: Lisa Chen, Target: 2026-02-18)*
• **ACCESS-1.d:** Intelligence and associated indicators, related to emerging malware targeting identities and identity systems is delivered to enhance early warning detections and proactive mitigation measures. *(Task: Access Controls, Priority: 90-Day Goal, Owner: Lisa Chen, Target: 2026-02-18)*
• **ACCESS-2.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)
• **ACCESS-2.d:** Insights regularly influence proactive adjustments to enhance access control requirements and thresholds based on the threat environment, including MFA strategies and password resets.
• **ACCESS-2.e:** Collection is extended to focus on identity-related threats relevant to the organization's industry and geographic representation. (see SITUATION)
Notes: Enhance identity and access management with threat intelligence insights.

RESPONSE (CTI1 → CTI2)
Required Practices: 10 practices need to be implemented
• **RESPONSE-1.c:** Events detected by the IR team are regularly enriched with CTI insights and context to improve response efficacy. *(Task: Incident Response, Priority: 90-Day Goal, Owner: Emma Brown, Target: 2026-02-18)*
• **RESPONSE-1.d:** CTI insights are used for immediate control gap detection analysis and rapid remediation, conducted in a mostly automated manner. *(Task: Response Automation, Priority: 90-Day Goal, Owner: Emma Brown, Target: 2026-02-18)*
• **RESPONSE-2.c:** Manual research and pivoting on TTPs and IoCs is being conducted to contextualize incidents and improve remediation.
• **RESPONSE-2.d:** Findings are documented in a stand-alone CTI report and can be incorporated into or accompany the IR report.
• **RESPONSE-2.e:** Automated intelligence is used to enrich the IR process.
• **RESPONSE-3.c:** IR time is reduced through automation. Key prevention measures are implemented with IoCs and TTPs from trusted sources.
• **RESPONSE-3.d:** Artificial intelligence (AI) and machine learning (ML) are used for analysis of TTP mapping (MITRE TRAM).
• **RESPONSE-3.e:** Incident TTPs are mapped to the MITRE ATT&CK; framework and reviewed against current detection and prevention capabilities.
• **RESPONSE-3.f:** Enrichment of SOC internal indicators and data continues with intelligence via TIP or automation.

• **RESPONSE-3.g:** Partnership with the threat hunting team is initiated for ongoing collaboration. (see THREAT)
Notes: Improve incident response with CTI-driven automation.

ARCHITECTURE (CTI1 → CTI2)
Required Practices: 7 practices need to be implemented

• **ARCHITECTURE-1.c:** The CTI program regularly advises on gaps in cybersecurity architecture based on threat landscape trends. (see THREAT) *(Task: Security Architecture, Priority: 90-Day Goal, Owner: Patricia White, Target: 2026-02-18)*
• **ARCHITECTURE-1.d:** Elements of the cybersecurity architecture plan are integrated into the process of creating the organization's threat profile. (see THREAT) *(Task: Security Architecture, Priority: 90-Day Goal, Owner: Patricia White, Target: 2026-02-18)*
• **ARCHITECTURE-2.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.
• **ARCHITECTURE-2.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.
• **ARCHITECTURE-3.c:** CTI tools and infrastructure are integrated with IR platforms to provide context and accelerate investigations.
• **ARCHITECTURE-3.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)
• **ARCHITECTURE-3.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.
Notes: Integrate CTI into security architecture design.

6-Month Goal

THREAT (CTI2 → CTI3)
Required Practices: 13 practices need to be implemented

• **THREAT-1.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. *(Task: Threat Intelligence Platform, Priority: 6-Month Goal, Owner: Sarah Johnson, Target: 2026-05-19)*
• **THREAT-1.h:** Polling for fresh indicators occurs on very regular cadences where relevant (e.g., hourly or daily for indicators with high entropy). *(Task: Threat Intelligence Platform, Priority: 6-Month Goal, Owner: Sarah Johnson, Target: 2026-05-19)*
• **THREAT-1.i:** False positives are identified and accounted for regularly.
• **THREAT-1.j:** Threat context (e.g., type of threat, attack stage, detection time stamps for relevance) is provided for most indicators to aid operator awareness.
• **THREAT-1.k:** Ingested indicators connect to automation playbooks and trigger COAs where relevant (e.g., automating implementation of low-regret blocking or phishing response).
• **THREAT-1.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.
• **THREAT-2.d:** Threat modeling is routinely developed to identify and contextualize priority threats relevant to the organization.
• **THREAT-2.e:** CTI products regularly highlight opportunities for detecting relevant threat activity within event log data.
• **THREAT-3.e:** RFIs are issued and fulfilled to provide context for new, original threat hunting hypotheses/abstracts (see the TaHiTI Threat Hunting Methodology2 for further details).
• **THREAT-4.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.

... and 3 more practices

Notes: Strategic initiative to become industry leader in threat intelligence. Requires significant investment.

FRAUD (CTI1 → CTI2)

Required Practices: 10 practices need to be implemented

• **FRAUD-1.e:** Integration of ISAC and peer sharing into the organization's processes is done in a mostly ad hoc manner. *(Task: Fraud Detection, Priority: 6-Month Goal, Owner: Anna Martinez, Target: 2026-05-19)*

• **FRAUD-1.f:** Automated monitoring is in place for mentions of common fraud indicators including business email compromise (BEC), short message service (SMS) phishing, invoice fraud, social engineering directed toward customers, and other relevant activity. *(Task: Fraud Detection, Priority: 6-Month Goal, Owner: Anna Martinez, Target: 2026-05-19)*

• **FRAUD-1.g:** A cross-functional working group is dedicated to identifying and sharing current and emerging threats on a recurring cadence.

• **FRAUD-1.h:** Threat context input is provided to the organization's training and education material and is aligned with observed cyber threat activities.

• **FRAUD-2.e:** Automation is used to detect malvertising campaigns and SEO poisoning for disruption actions.

• **FRAUD-2.f:** Automated alerting for adversary targeting, including brand impersonation, is used.

• **FRAUD-2.g:** Automated identification and disruption of phishing kits targeting the organization's brand(s) is used.

• **FRAUD-2.h:** Memberships in private intel sharing channels are utilized to track and mitigate risk from specific threat actors and campaigns.

• **FRAUD-3.c:** The CTI team provides intelligence to drive the creation of fraud-specific automation and detections for anomalous customer sign-ins and sessions indicating potential ATO activity.

• **FRAUD-3.d:** Feedback loops are created to include the CTI team when users (customers and employees) report suspicious behavior indicative of customer ATO activity.

Notes: Enhance fraud detection with cybercriminal intelligence.

Long-term

THIRD-PARTIES (CTI0 → CTI1)

Required Practices: 5 practices need to be implemented

• **THIRD-PARTIES-1.a:** Free/open-source tools and social media are used to detect third-party risk. *(Task: Vendor Risk, Priority: Long-term, Owner: David Lee, Target: 2026-11-20)*

• **THIRD-PARTIES-1.b:** Third parties are documented and classified based on business continuity requirements

• **THIRD-PARTIES-2.a:** Selected personnel are assigned to monitor and triage potential third-party exposures involving top-tier vendors.

• **THIRD-PARTIES-2.b:** Alerts are provided in an ad hoc manner for third-party incidents gleaned primarily from open sources.

• **THIRD-PARTIES-3.a:** Contracts are available and include Third-Party main contacts and communication channels.

Notes: Long-term initiative to integrate CTI into third-party risk management.

WORKFORCE (CTI0 → CTI1)

Required Practices: 6 practices need to be implemented

• **WORKFORCE-1.a:** CTI insights are regularly used to inform cybersecurity awareness and skills assessment strategies. *(Task: Security Awareness, Priority: Long-term, Owner: Chris Taylor, Target: 2026-11-20)*

• **WORKFORCE-1.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.

• **WORKFORCE-2.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.

• **WORKFORCE-3.a:** Workforce development efforts are understood by the CTI program and it provides management with inputs as requested.
• **WORKFORCE-2.b:** Insights provided by the CTI program are generally relevant to the organization, but not necessarily aligned to specific organizational units or job roles.
• **WORKFORCE-2.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)
Notes: Build CTI workforce capabilities over time.

PROGRAM (CTI2 → CTI3)
Required Practices: 9 practices need to be implemented
• **PROGRAM-1.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. *(Task: Program Excellence, Priority: Long-term, Owner: Robert Anderson, Target: 2026-11-20)*
• **PROGRAM-1.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. *(Task: Program Excellence, Priority: Long-term, Owner: Robert Anderson, Target: 2026-11-20)*
• **PROGRAM-2.g:** CTI program activities are periodically reviewed and improved upon to ensure they align with and support the cybersecurity program strategy.
• **PROGRAM-2.h:** CTI activities are independently reviewed to ensure conformance with cybersecurity policies and procedures, periodically and according to defined triggers, such as process changes.
• **PROGRAM-2.i:** The CTI program addresses and enables the achievement of legal and regulatory compliance, as appropriate.
• **PROGRAM-2.j:** 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.
• **PROGRAM-2.k:** The effectiveness of activities in the PROGRAM domain is evaluated and tracked for the purpose of continuous improvement.
• **PROGRAM-3.e:** Up-to-date policies or other organizational directives define requirements for activities in the PROGRAM domain and CTI program documentation is "living documents."
• **PROGRAM-3.f:** Responsibility, accountability, and authority for the performance of activities in the PROGRAM domain are assigned to personnel.
Notes: Strategic goal: Mature CTI program to industry-leading level.

Recommendations

1. Prioritize Quick Wins: Focus on 2 domains marked as 'Quick Win' to build momentum and demonstrate early value.

2. Foundation Building: 4 domain(s) are at CTI0 level. Establish basic CTI capabilities in these areas first.

4. Resource Planning: Review the Gap Analysis section to identify required data sources and allocate budget accordingly.

5. Regular Assessment: Conduct bi-annual assessments to track progress and adjust targets as capabilities mature.