MORADO · PROGRAM MATURITY

Operationalizing the CTI Capability Maturity Model.

How Morado helps intelligence teams measure where their program stands, act on the gaps and show progress against the CTI-CMM.

CTI leaders | Security leaders | MSSPs and partners



A roadmap for maturity, and the work of following it.

Intelligence teams are increasingly asked to show what their program delivers and how it is improving. The **Cyber Threat Intelligence Capability Maturity Model (CTI-CMM)** gives them a shared way to do that. Developed by the CTI community, it describes how threat intelligence supports the wider security program across a set of domains, and defines maturity levels that describe what a more capable program looks like in each one.

The model is a roadmap, not a tool. Knowing which practices make a program more mature is the first step. The harder part is putting them into daily operation: collecting the right intelligence, connecting it with the organization's environment, getting it to the people who act, and measuring the result over time.

Where programs get stuck

Fragmented tools

Dark web, brand, vulnerability and third-party intelligence live in separate products, so domains that depend on them are hard to cover consistently.

Requirements on paper

Intelligence requirements, RFIs and stakeholder feedback sit in spreadsheets, so it is hard to show the program answers what the business needs.

No baseline

Without a recorded assessment, there is no way to show where the program started or how far it has come.

How Morado helps

Measure. A built-in CTI-CMM assessment shows where your program stands in each domain, where to improve and how it is progressing over time.

Operationalize. The platform's four modules, Intel Operations, Digital Risk Protection, Exposure Management and Physical Security, give you the capabilities many CTI-CMM domains depend on, connected in one place.

Prove it. Stakeholder feedback, RFIs and reporting show whether the program meets the needs of the people it serves, alongside the assessment results.

How Morado supports the CTI-CMM domains

The CTI-CMM describes how intelligence contributes to each part of a security program. Here is how Morado's capabilities support the domains where threat intelligence plays the largest role.

Risk Management

Identify, assess and reduce the risks facing the organization.

- Threat profile and Priority Intelligence Requirements
- Brand impersonation: domains, ads, social and apps
- Dark web monitoring for exposed credentials and data
- Morado AI to assess relevance to your environment

Threat & Vulnerability Management

Understand threats and the weaknesses they could exploit.

- Exposure Management: discovery and validation
- Threat actor knowledge base
- Exploited vulnerabilities and the actors using them
- TTP coverage against your detection rules

Situational Awareness

Give decision-makers accurate, timely intelligence.

- News Stream matched to your requirements
- Alerts: one prioritized queue across modules
- Articles converted into structured STIX intelligence
- Physical Security for locations and travel

Third-Party Risk Management

Monitor the risk suppliers and partners bring.

- Breaches, leaks and ransomware listings at suppliers
- Dark web mentions of vendors
- Exploited vulnerabilities and disclosures
- Automated third-party breach investigation

Dark web monitoring and brand protection are often the hardest capabilities for a program to add, because they need specialist collection and analysis. In Morado they are part of Digital Risk Protection, so their findings feed the same investigations, workflows and reporting as the rest of your intelligence.

Fraud & Abuse Management Address credential theft, phishing and impersonation.	• Compromised credentials and infostealer logs • Executive and VIP impersonation	• Credential validation workflows in Microsoft Entra • Takedown support within the agreed scope
Event & Incident Response Use intelligence to detect and respond.	• Retrospective hunts for new indicators in your SIEM • Agentic workflows with approval steps	• IOCs pushed to your security tools • Tasks in your ticketing or ServiceNow
Asset, Change & Configuration Know what is exposed.	• External discovery of assets and services • Internal scanner data alongside external findings	• Misconfigurations and vulnerable software
Program Management Run the intelligence program itself.	• Requirements, RFIs and stakeholder accounts • Workspaces for sharing with partners and ISACs	• Investigations, reports and recurring briefings • The built-in CTI-CMM assessment and trend line

Measuring and improving maturity

Morado's CTI-CMM assessment is built into the platform, so the results sit next to the work that changes them.

Assess each domain
Record where your program stands today, and the level you are aiming for.

Find the gaps
See which domains are furthest from their target, and what would close them.

Track progress
Re-assess over time and follow the trend line, so leadership sees the improvement.

Hear from stakeholders
Feedback on reports and the RFIs they raise show whether the program meets their needs.

A practical path

1. **Set your baseline**
   Complete the CTI-CMM assessment in Morado and agree target levels with your stakeholders.
2. **Define your requirements**
   Capture the questions the business needs answered as Priority Intelligence Requirements, and connect them with stakeholders.
3. **Close the biggest gaps first**
   Turn on the capabilities those domains depend on, from dark web monitoring to hunts, coverage checks and exposure validation.
4. **Re-assess and report**
   Re-run the assessment, share progress with leadership, and adjust requirements as the threat picture changes.

For MSSPs. Run the assessment for each customer in its own tenant. A CTI-CMM trend line per customer gives every renewal a clear story of progress.

From a framework to a working program

Whether you are building a first program or maturing an established one, you choose how to run it:

Self-service
Your team operates the platform and its intelligence workflows.

Analyst-supported
Morado analysts add research, investigations, reporting, RFIs and dark web retrieval.

Managed program
Morado runs ongoing intelligence operations within an agreed scope.

Partner delivery
MSSPs and consultancies deliver across customer tenants.

About Morado. Morado is a veteran-owned cyber threat intelligence company headquartered in San Diego, California. Morado combines a threat intelligence platform with analyst services, so security teams and the providers who serve them can see what attackers see and act before they do.

501 W Broadway, Suite 800, San Diego, CA 92101

See your program against the CTI-CMM.
Book a demo, or start a free 2-week trial.

sales@morado.io
morado.io/demo