# TREADSTONE 71

# CYBER AND THREAT INTELLIGENCE FOURTH QUARTER 2020 MATURITY ASSESSMENT AND TRAINING COMBO

Treadstone 71

# Maturity & Training Combo

## Cyber Intelligence Maturity Assessment - Online training of Certified Cyber Intelligence Analyst Your Company Focused Customization

## Tier 1 Cyber Intelligence Maturity Assessment - Overview

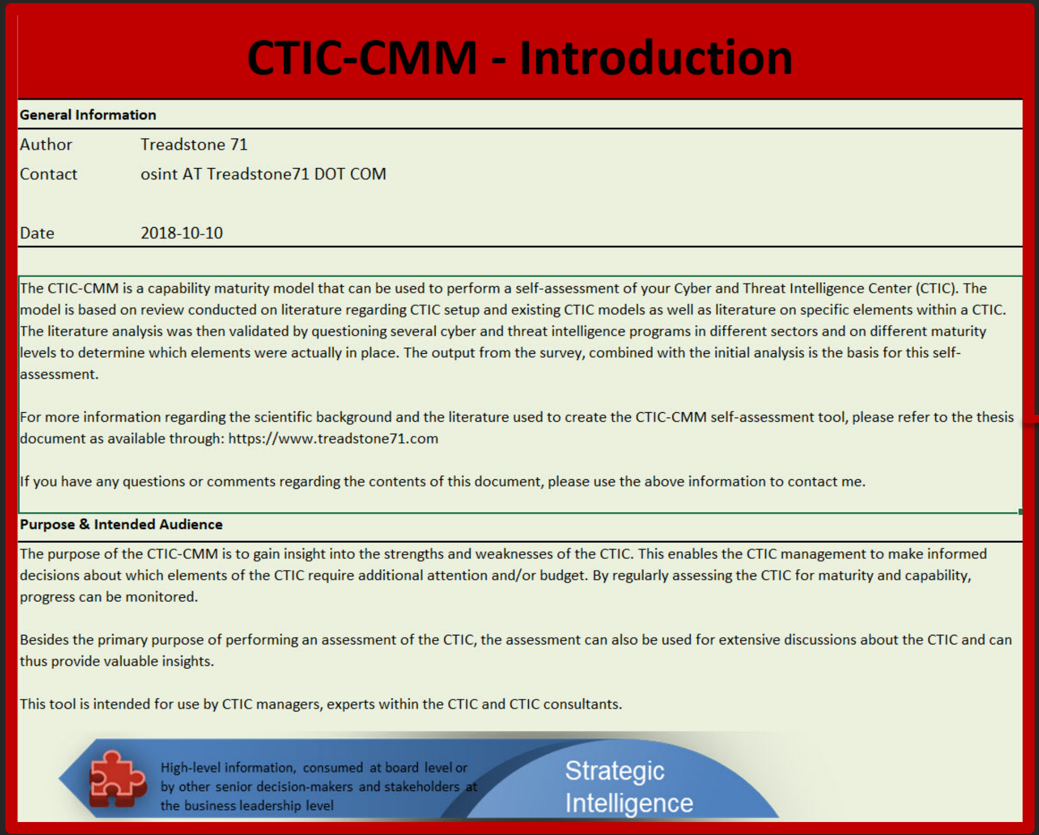
- In-depth questionnaire - we provide oversight for you to complete the questionnaire
  - Customization – Stakeholder interviews
  - Questionnaire update
  - Maturity level targets
- Artifact review
  - Analysis of questionnaire results - we will request supporting documentation firsthand (secure review after signing your NDA) to validate the scoring
- Create the Assessment Report (review and brief with core team)
  - Final adjustments
- Final report delivery, point-of-contact brief
- Online executive brief of the results

- NOTE: There are additional (optional) Tiers for the assessment that require more time

# Q42020 Maturity & Training Combo

- Tier 1
  - We guide you through the self-assessment questionnaire – how to complete the questionnaire
    - Review the questions so you can gather your artifacts
    - 10 days to complete on your end
    - 10 days to complete on our end
  - Update the assessment
  - Provide a 1-2 page written corresponding to the final assessment
  - Recommendations
  - Modifications to existing cyber intelligence lifecycle training
    - Adjust training based on gaps
    - Mix, match, update

# Cyber and Threat Intelligence Maturity Assessment



## CTIC-CMM - Introduction

**General Information**

| | |
|---|---|
| Author | Treadstone 71 |
| Contact | osint AT Treadstone71 DOT COM |
| Date | 2018-10-10 |

The CTIC-CMM is a capability maturity model that can be used to perform a self-assessment of your Cyber and Threat Intelligence Center (CTIC). The model is based on review conducted on literature regarding CTIC setup and existing CTIC models as well as literature on specific elements within a CTIC. The literature analysis was then validated by questioning several cyber and threat intelligence programs in different sectors and on different maturity levels to determine which elements were actually in place. The output from the survey, combined with the initial analysis is the basis for this self-assessment.

For more information regarding the scientific background and the literature used to create the CTIC-CMM self-assessment tool, please refer to the thesis document as available through: https://www.treadstone71.com

If you have any questions or comments regarding the contents of this document, please use the above information to contact me.

**Purpose & Intended Audience**

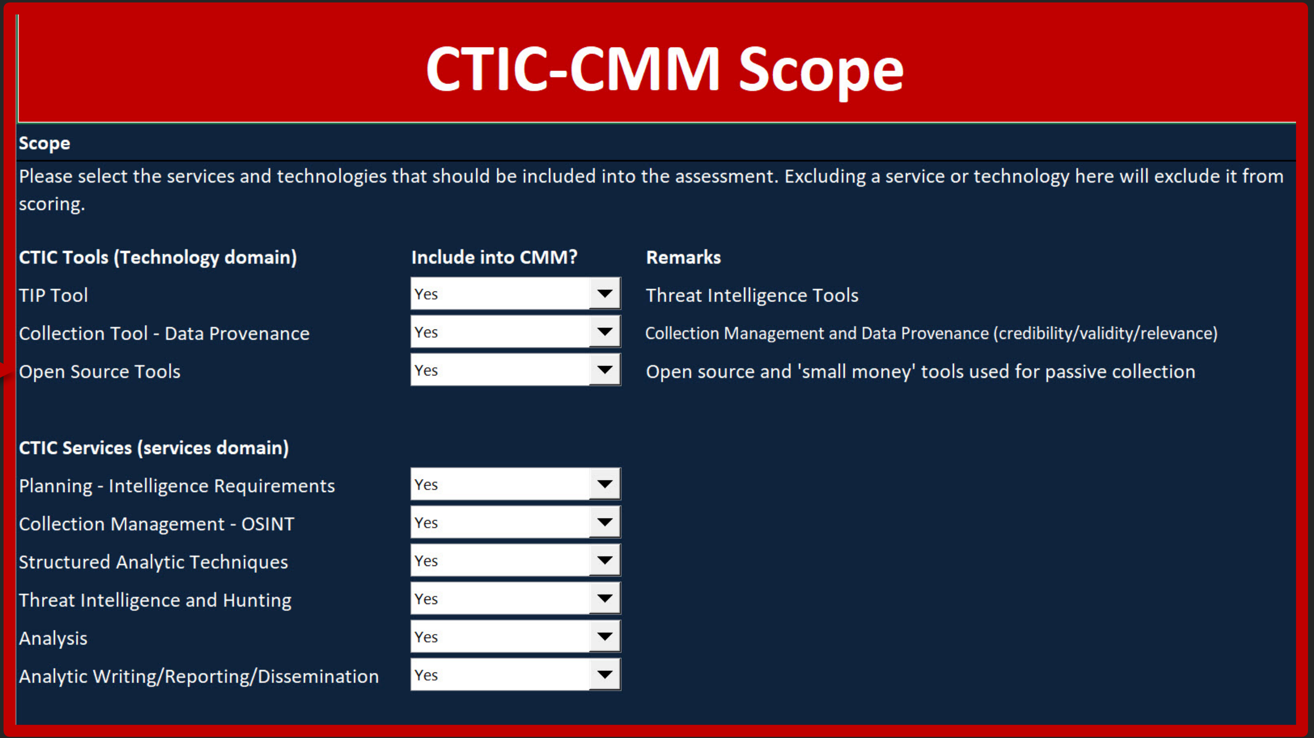
The purpose of the CTIC-CMM is to gain insight into the strengths and weaknesses of the CTIC. This enables the CTIC management to make informed decisions about which elements of the CTIC require additional attention and/or budget. By regularly assessing the CTIC for maturity and capability, progress can be monitored.

Besides the primary purpose of performing an assessment of the CTIC, the assessment can also be used for extensive discussions about the CTIC and can thus provide valuable insights.

This tool is intended for use by CTIC managers, experts within the CTIC and CTIC consultants.

High-level information, consumed at board level or by other senior decision-makers and stakeholders at the business leadership level

Strategic Intelligence



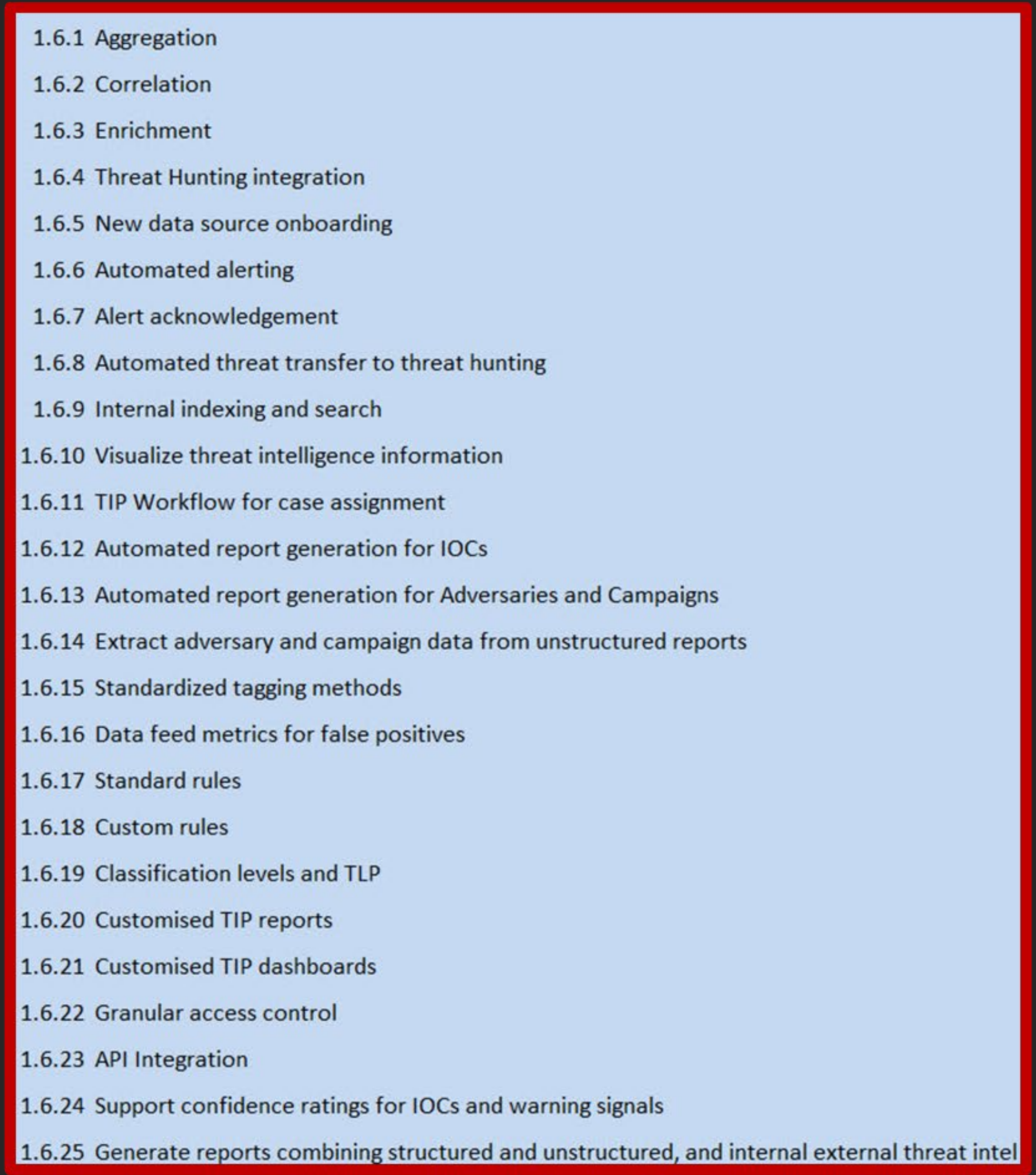
## CTIC-CMM Scope

**Scope**

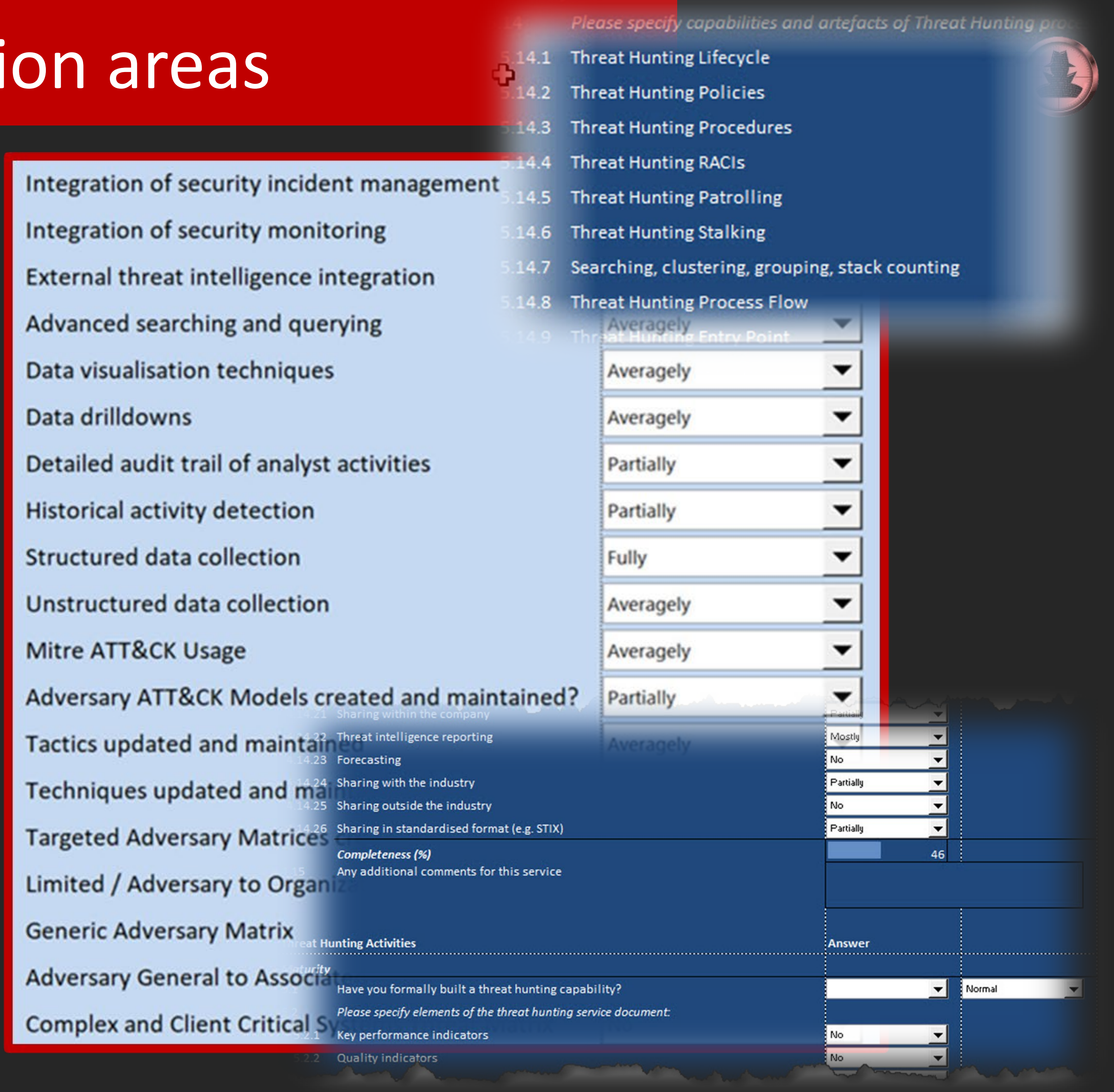
Please select the services and technologies that should be included into the assessment. Excluding a service or technology here will exclude it from scoring.

| **CTIC Tools (Technology domain)** | **Include into CMM?** | **Remarks** |
|---|---|---|
| TIP Tool | Yes | Threat Intelligence Tools |
| Collection Tool - Data Provenance | Yes | Collection Management and Data Provenance (credibility/validity/relevance) |
| Open Source Tools | Yes | Open source and 'small money' tools used for passive collection |
| | | |
| **CTIC Services (services domain)** | | |
| Planning - Intelligence Requirements | Yes | |
| Collection Management - OSINT | Yes | |
| Structured Analytic Techniques | Yes | |
| Threat Intelligence and Hunting | Yes | |
| Analysis | Yes | |
| Analytic Writing/Reporting/Dissemination | Yes | |

# Sample question areas



1.6.1 Aggregation
1.6.2 Correlation
1.6.3 Enrichment
1.6.4 Threat Hunting integration
1.6.5 New data source onboarding
1.6.6 Automated alerting
1.6.7 Alert acknowledgement
1.6.8 Automated threat transfer to threat hunting
1.6.9 Internal indexing and search
1.6.10 Visualize threat intelligence information
1.6.11 TIP Workflow for case assignment
1.6.12 Automated report generation for IOCs
1.6.13 Automated report generation for Adversaries and Campaigns
1.6.14 Extract adversary and campaign data from unstructured reports
1.6.15 Standardized tagging methods
1.6.16 Data feed metrics for false positives
1.6.17 Standard rules
1.6.18 Custom rules
1.6.19 Classification levels and TLP
1.6.20 Customised TIP reports
1.6.21 Customised TIP dashboards
1.6.22 Granular access control
1.6.23 API Integration
1.6.24 Support confidence ratings for IOCs and warning signals
1.6.25 Generate reports combining structured and unstructured, and internal external threat intel



| | |
|---|---|
| Integration of security incident management | |
| Integration of security monitoring | |
| External threat intelligence integration | |
| Advanced searching and querying | Averagely |
| Data visualisation techniques | Averagely |
| Data drilldowns | Averagely |
| Detailed audit trail of analyst activities | Partially |
| Historical activity detection | Partially |
| Structured data collection | Fully |
| Unstructured data collection | Averagely |
| Mitre ATT&CK Usage | Averagely |
| Adversary ATT&CK Models created and maintained? | Partially |
| Tactics updated and maintained | Averagely |
| Techniques updated and mai | |
| Targeted Adversary Matrices | |
| Limited / Adversary to Organiz | |
| Generic Adversary Matrix | |
| Adversary General to Associat | |
| Complex and Client Critical Sy | |

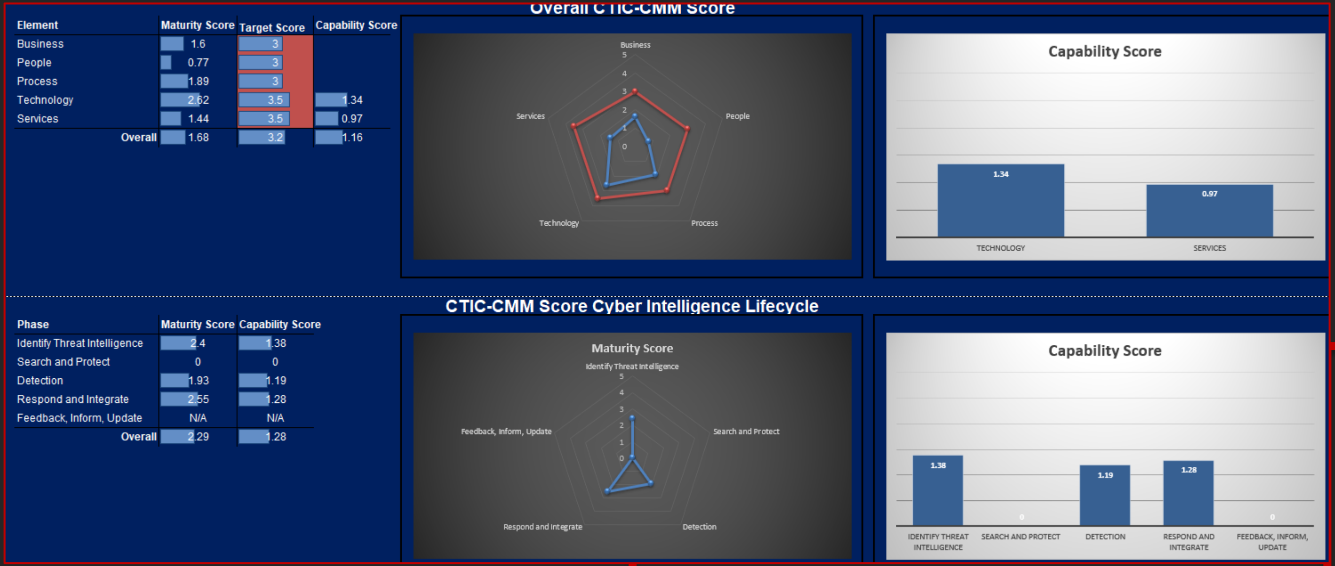
*Please specify capabilities and artefacts of Threat Hunting pro*

5.14.1 Threat Hunting Lifecycle
5.14.2 Threat Hunting Policies
5.14.3 Threat Hunting Procedures
5.14.4 Threat Hunting RACIs
5.14.5 Threat Hunting Patrolling
5.14.6 Threat Hunting Stalking
5.14.7 Searching, clustering, grouping, stack counting
5.14.8 Threat Hunting Process Flow
5.14.9 Threat Hunting Entry Point

| | | |
|---|---|---|
| 4.21 | Sharing within the company | Partially |
| 4.22 | Threat intelligence reporting | Mostly |
| 4.23 | Forecasting | No |
| 4.24 | Sharing with the industry | Partially |
| 4.25 | Sharing outside the industry | No |
| 4.26 | Sharing in standardised format (e.g. STIX) | Partially |
| | *Completeness (%)* | 46 |
| 15 | Any additional comments for this service | |

| | Threat Hunting Activities | Answer | |
|---|---|---|---|
| | *Maturity* | | |
| 1 | Have you formally built a threat hunting capability? | | Normal |
| 2 | *Please specify elements of the threat hunting service document:* | | |
| 5.2.1 | Key performance indicators | No | |
| 5.2.2 | Quality indicators | No | |

# Result Charts

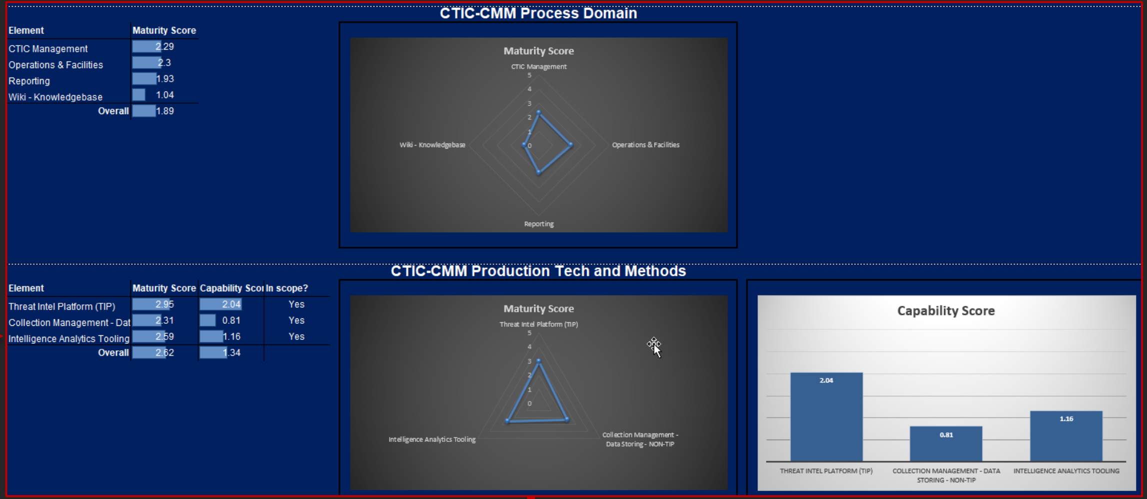


## Overall C TIC-CMM Score

| Element | Maturity Score | Target Score | Capability Score |
|---|---|---|---|
| Business | 1.6 | 3 | |
| People | 0.77 | 3 | |
| Process | 1.89 | 3 | |
| Technology | 2.62 | 3.5 | 1.34 |
| Services | 1.44 | 3.5 | 0.97 |
| Overall | 1.68 | 3.2 | 1.16 |

## CTIC-CMM Score Cyber Intelligence Lifecycle

| Phase | Maturity Score | Capability Score |
|---|---|---|
| Identify Threat Intelligence | 2.4 | 1.38 |
| Search and Protect | 0 | 0 |
| Detection | 1.93 | 1.19 |
| Respond and Integrate | 2.55 | 1.28 |
| Feedback, Inform, Update | N/A | N/A |
| Overall | 2.29 | 1.28 |



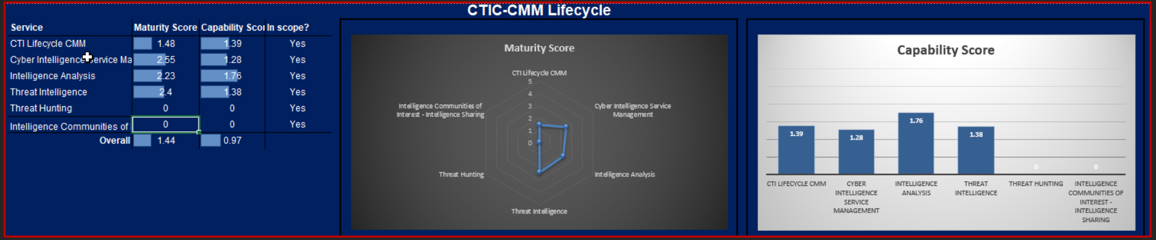
## CTIC-CMM Process Domain

| Element | Maturity Score |
|---|---|
| CTIC Management | 2.29 |
| Operations & Facilities | 2.3 |
| Reporting | 1.93 |
| Wiki - Knowledgebase | 1.04 |
| Overall | 1.89 |

## CTIC-CMM Production Tech and Methods

| Element | Maturity Score | Capability Scor | In scope? |
|---|---|---|---|
| Threat Intel Platform (TIP) | 2.95 | 2.04 | Yes |
| Collection Management - Dat | 2.31 | 0.81 | Yes |
| Intelligence Analytics Tooling | 2.59 | 1.16 | Yes |
| Overall | 2.62 | 1.34 | |

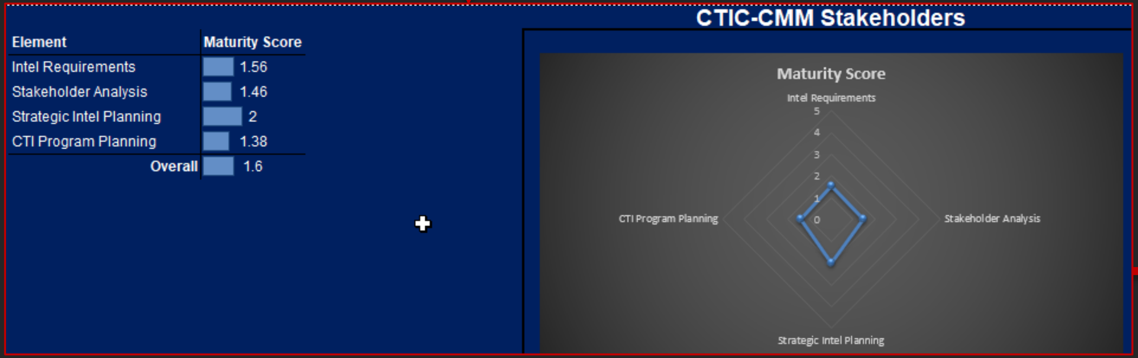
Maturity Score
Threat Intel Platform (TIP)
5
4
3
2
1
0
Collection Management - Data Storing - NON-TIP
Intelligence Analytics Tooling
Capability Score
2.04
0.81
1.16
THREAT INTEL PLATFORM (TIP)
COLLECTION MANAGEMENT - DATA STORING - NON-TIP
INTELLIGENCE ANALYTICS TOOLING



## CTIC-CMM Lifecycle

| Service | Maturity Score | Capability Scor | In scope? |
|---|---|---|---|
| CTI Lifecycle CMM | 1.48 | 1.39 | Yes |
| Cyber Intelligence Service Ma | 2.55 | 1.28 | Yes |
| Intelligence Analysis | 2.23 | 1.76 | Yes |
| Threat Intelligence | 2.4 | 1.38 | Yes |
| Threat Hunting | 0 | 0 | Yes |
| Intelligence Communities of | 0 | 0 | Yes |
| Overall | 1.44 | 0.97 | |

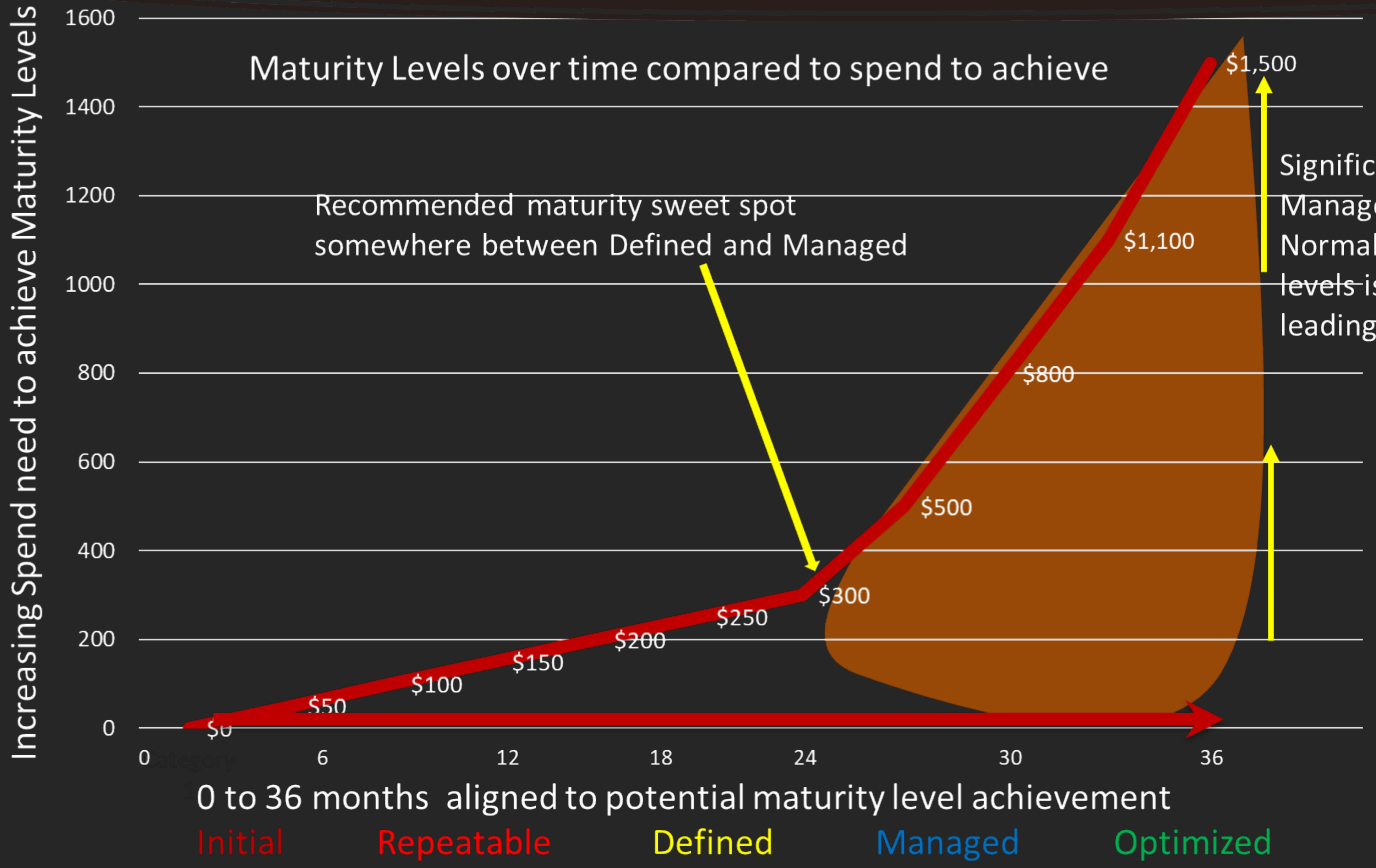
Maturity Score
CTI Lifecycle CMM
5
4
3
2
1
0
Cyber Intelligence Service Management
Intelligence Analysis
Threat Intelligence
Threat Hunting
Intelligence Communities of Interest - Intelligence Sharing
Capability Score
1.39
1.28
1.76
1.38
0
0
CTI LIFECYCLE CMM
CYBER INTELLIGENCE SERVICE MANAGEMENT
INTELLIGENCE ANALYSIS
THREAT INTELLIGENCE
THREAT HUNTING
INTELLIGENCE COMMUNITIES OF INTEREST - INTELLIGENCE SHARING



## CTIC-CMM Stakeholders

| Element | Maturity Score |
|---|---|
| Intel Requirements | 1.56 |
| Stakeholder Analysis | 1.46 |
| Strategic Intel Planning | 2 |
| CTI Program Planning | 1.38 |
| Overall | 1.6 |

# Understand the Cyber Intelligence Maturity Levels – Diminishing Returns



Recommended maturity sweet spot somewhere between Defined and Managed

Significant spend to achieve Managed and Optimized. Normal achievement of highest levels is difficult to maintain leading to additional spend.

Note: Spend numbers used for this example are arbitrary and set to demonstrate Diminishing Return on Investment

# TREADSTONE 71

# CYBER AND THREAT INTELLIGENCE FOURTH QUARTER 2020 MATURITY ASSESSMENT AND TRAINING COMBO

Treadstone 71