Prescott Pym
Chris Horsley

Cosive

AISA

What’s the point of CTI?

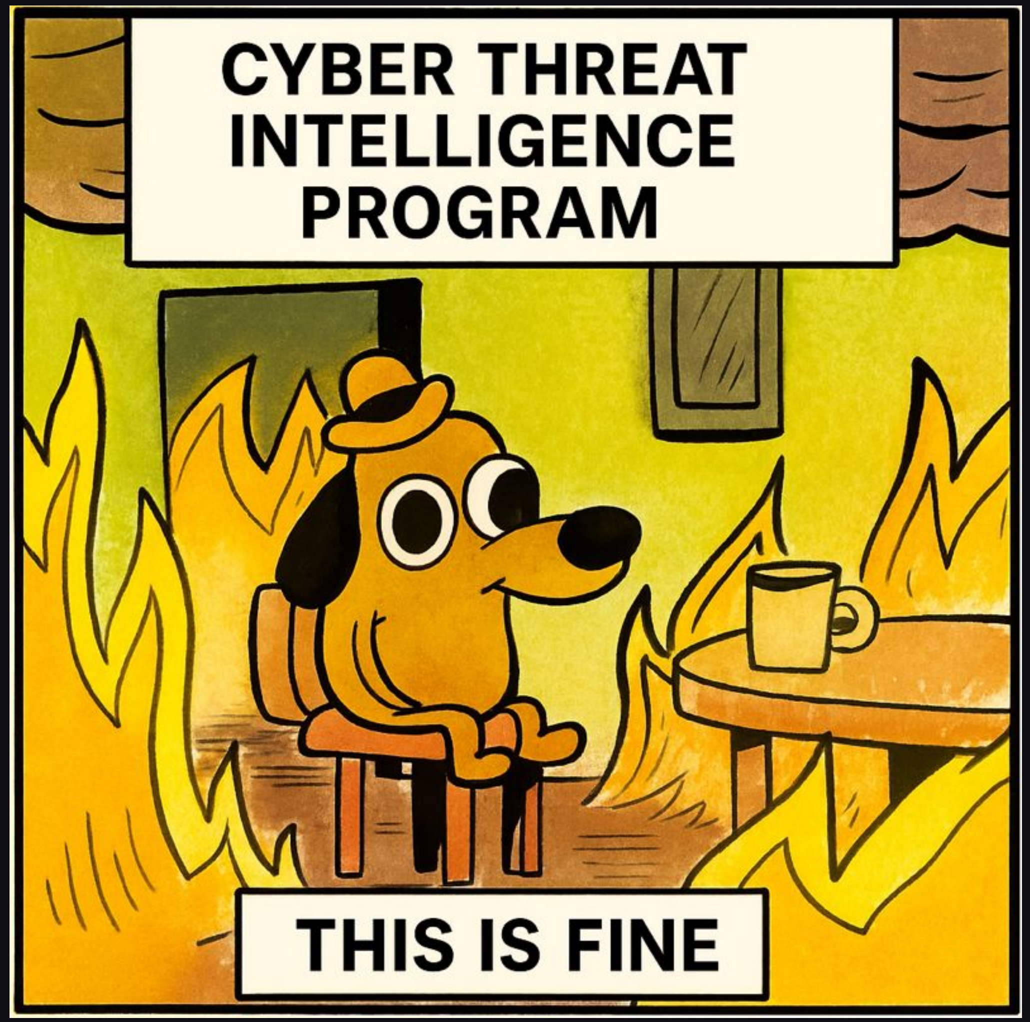
Cyber Threat Intelligence? Do we have a good grasp of what it is?

- A way of communicating risks and threats
- Proactive defence to your organisation
- It translates raw data into actionable insights:
  - Strategically
  - Operationally
  - Tactically
- It helps prioritise and make informed business decisions

Burning questions for CTI

CTI provides context on the following questions:

- Who is targeting us?
- What is the attack methodology?
- Where are we vulnerable?
- When will an attempt be likely?
- Why are we a target?
- How do prevent this happening?



Growing pains: what most CTI programs look like

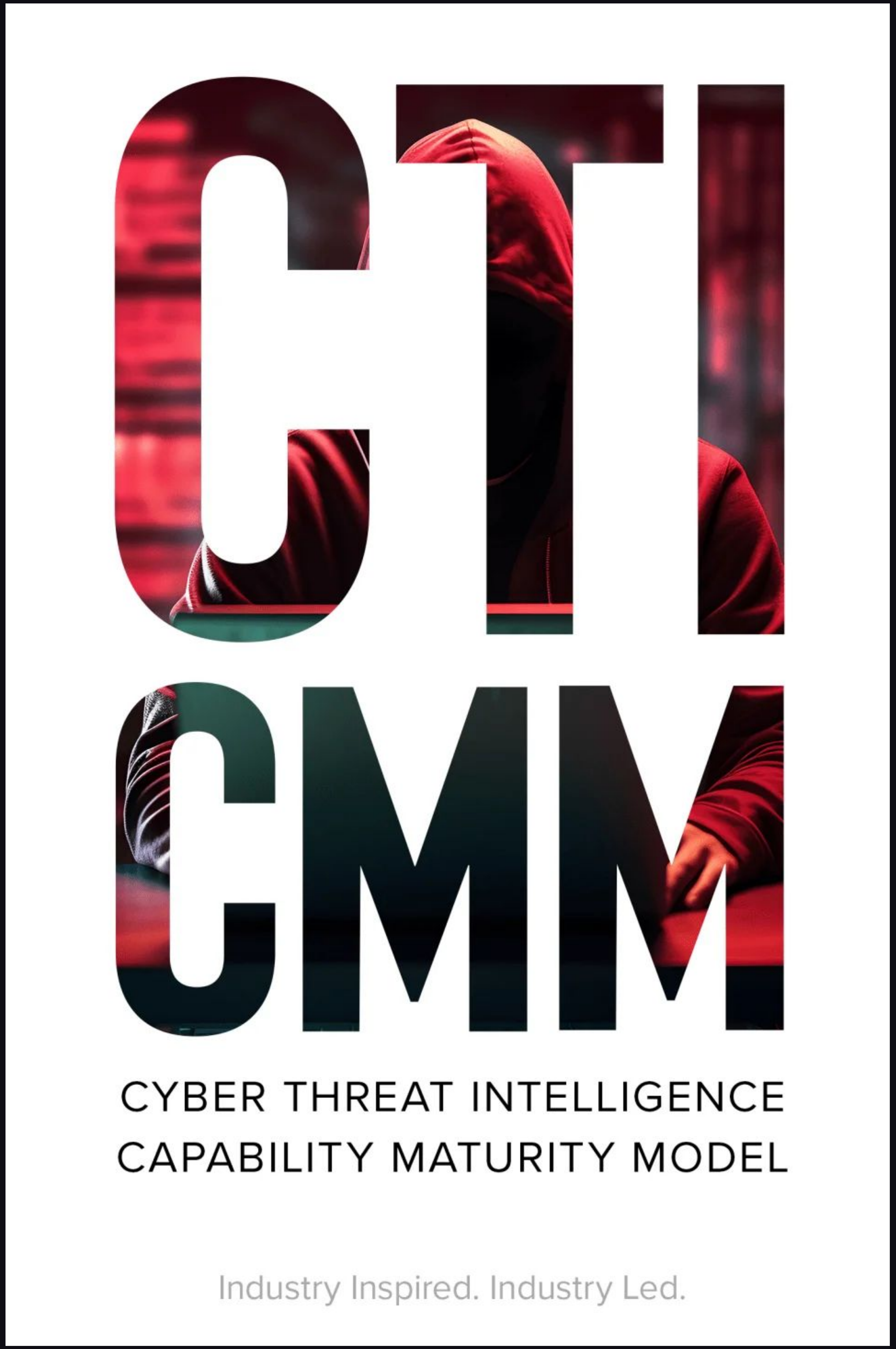
- Focus on only technical indicators
- Not aligned to organisational goals
- Built in isolation to stakeholders
- Not integrated into toolsets
- Trying to do everything at once
- Threats are not modelled
- Limited ongoing governance and metrics
- Measuring the wrong things (e.g. volume)
- Lack of perceived value

These result in processes that go down rabbit holes and don't generate impact to a cyber program

OK, so listen, here's what we know about ShinyHunters / UNC6040 / UNC6395...
1.5 billion Salesforce records stolen
Salesloft-- Driff OAuth tokens compromised
Targets; Google, Cloudfiare, Palo Alto, Zscaler...

Intro to CTI-CMM

- The CTI-CMM aims to solve these problems with a structured program to benchmark CTI programs.
- It is a global community project driven by CTI leaders including Intel 471, IBM, Kroger, Bank of America, Cosive
- Domains help focus review across 11 areas
- Self assess or have someone review your maturity



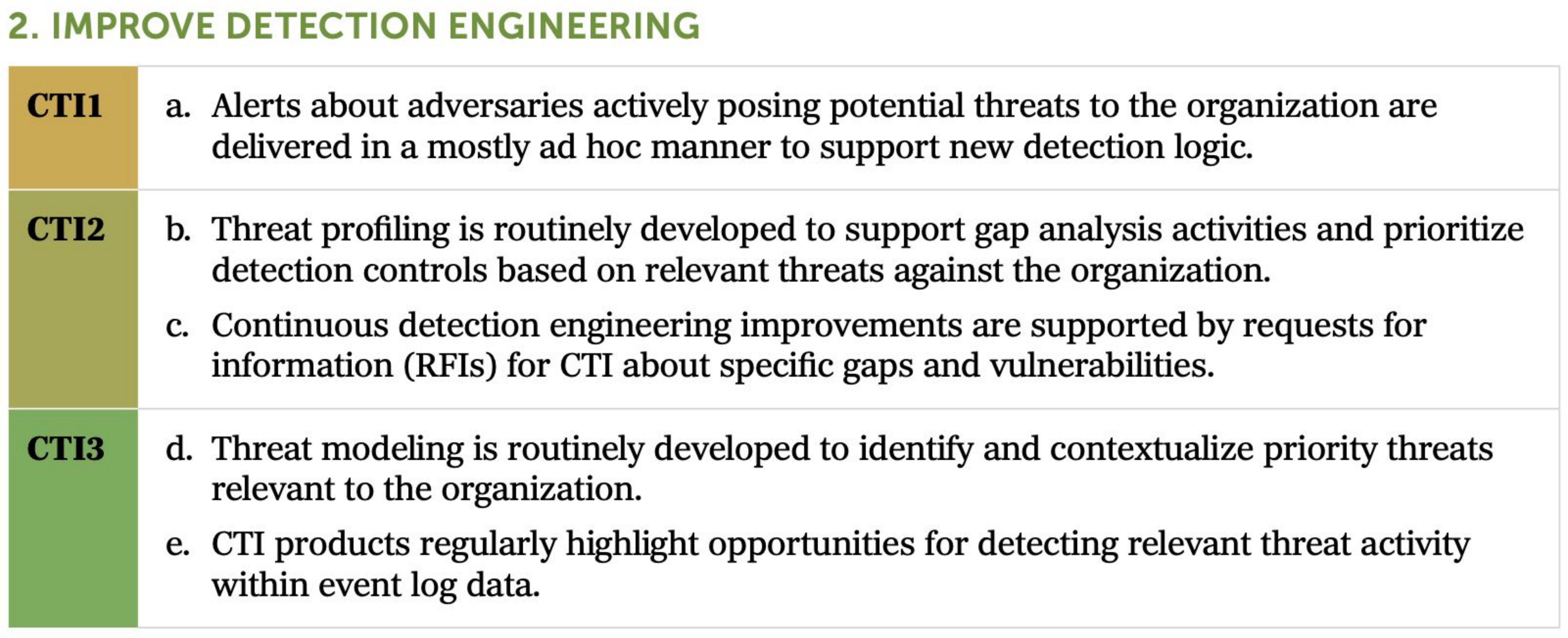
CTI CMM

CYBER THREAT INTELLIGENCE
CAPABILITY MATURITY MODEL

Industry Inspired. Industry Led.

CTI-CMM Maturity Levels

- Processes are rated:
  - CTI1: Foundational
  - CTI2: Advanced
  - CTI3: Leading
- Download at: [cti-cmm.org](cti-cmm.org)



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 CTI about specific gaps and vulnerabilities.
CTI3	d. Threat modeling is routinely developed to identify and contextualize priority threats relevant to the organization.
	e. CTI products regularly highlight opportunities for detecting relevant threat activity within event log data.

Practical CTI-CMM Use

11 Domains

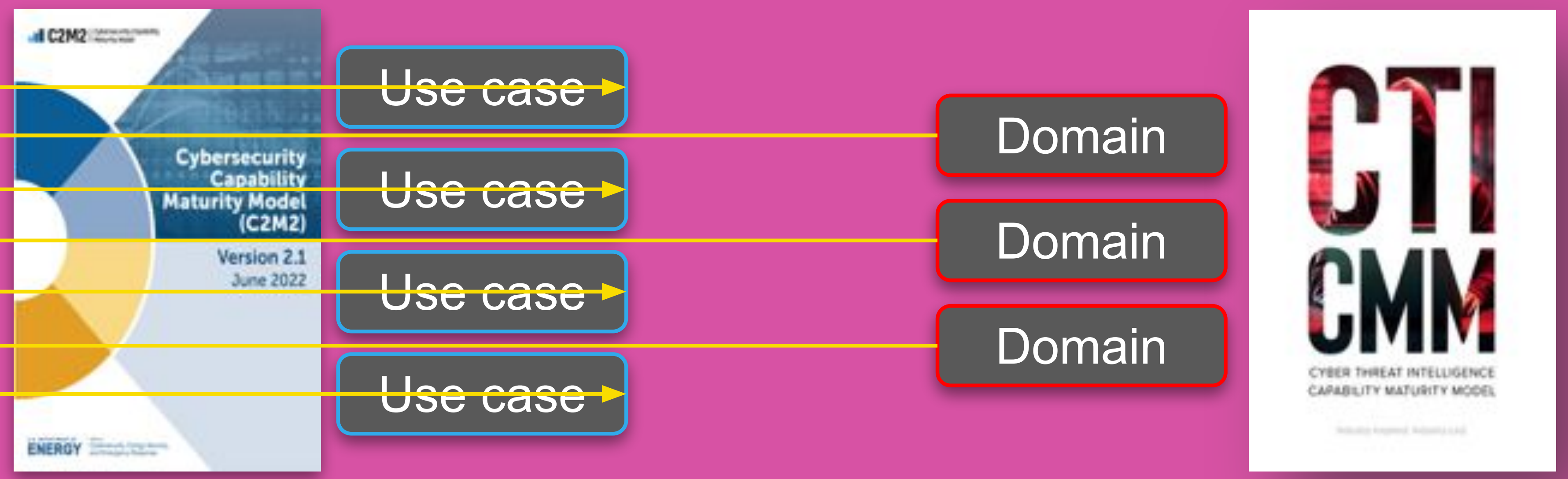
- Asset Management
- Threat & Vuln Management
- Risk Management
- Identity and Access Management
- Situational Awareness
- Incident Response
- Third-Party Risk Management
- Fraud and Abuse Management
- Workforce Management
- Cybersecurity Architecture
- Program Management

2 Main Audiences

Leadership
CTI Directors, Team Leaders
Cybersecurity Executives, Staff

Practitioners
CTI Analysts, Engineers, Stakeholders (SOC, IR, etc.)

Numerous
Integrated
Use Cases

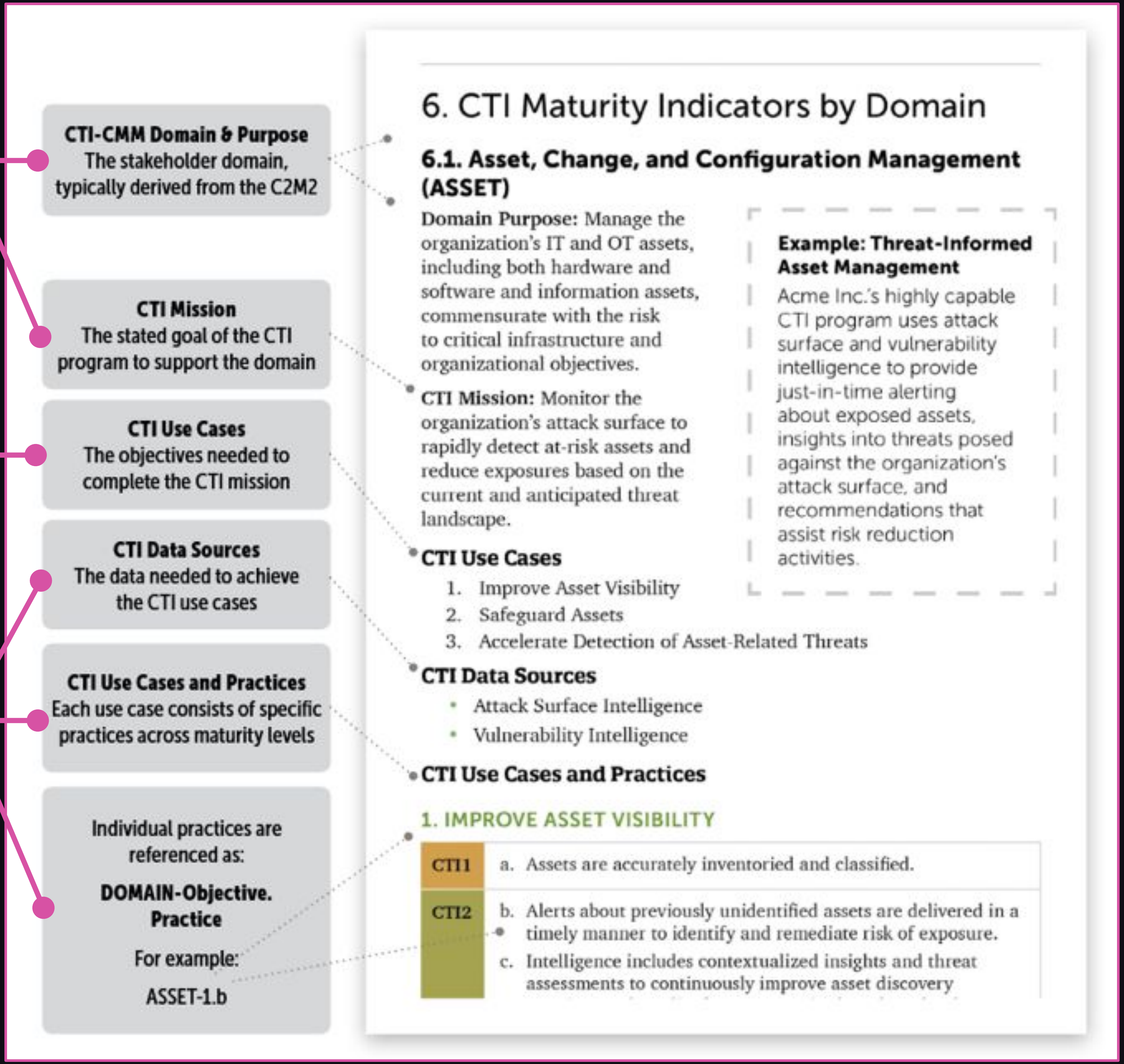

C2M2
Cybersecurity Capability Maturity Model (C2M2)
Version 2.1
June 2022
ENERGY
Use case
Use case
Use case
Use case
Domain
Domain
Domain
CTI CMM
CYBER THREAT INTELLIGENCE CAPABILITY MATURITY MODEL

CTI-CMM domain example

WHAT?

SO WHAT?

NOW WHAT?



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 assessments to continuously improve asset discovery

DETAILS?

Go there

CTI is a nebulous buffet

CTI-CMM is a menu

CTI-CMM domains in 45 seconds each

Domain 1: ASSET

Know assets, reduce exposure

“Oh, we’re using Salesloft Drift?”

Domain 2: THREAT

Know your enemy, hunt threats

“Solarwinds C2 domain in logs?”

Domain 3: RISK

Strategic CTI for better decisions

“SAP attacks up 400% over 3 years”

Domain 4: ACCESS

Cred abuse, access control

“Our creds just appeared on a forum”

Domain 5: SITUATION

Understand threat landscape

“We’ll soon have datacentres in an active warzone”

Domain 6: RESPONSE

Learn from incidents, do better

“How did lateral movement occur in VPN attacks?”

Domain 7: THIRD-PARTIES

Manage supplier risk

“Does our MSP use Kaseya VSA?”

Domain 8: FRAUD

Financial fraud, brand abuse

“How do phishers act in banking platforms?”

Domain 9: WORKFORCE

Training, insiders, shady applicants

“Telltale signs of an NK applicant”

Domain 10: ARCHITECTURE

Build stronger systems

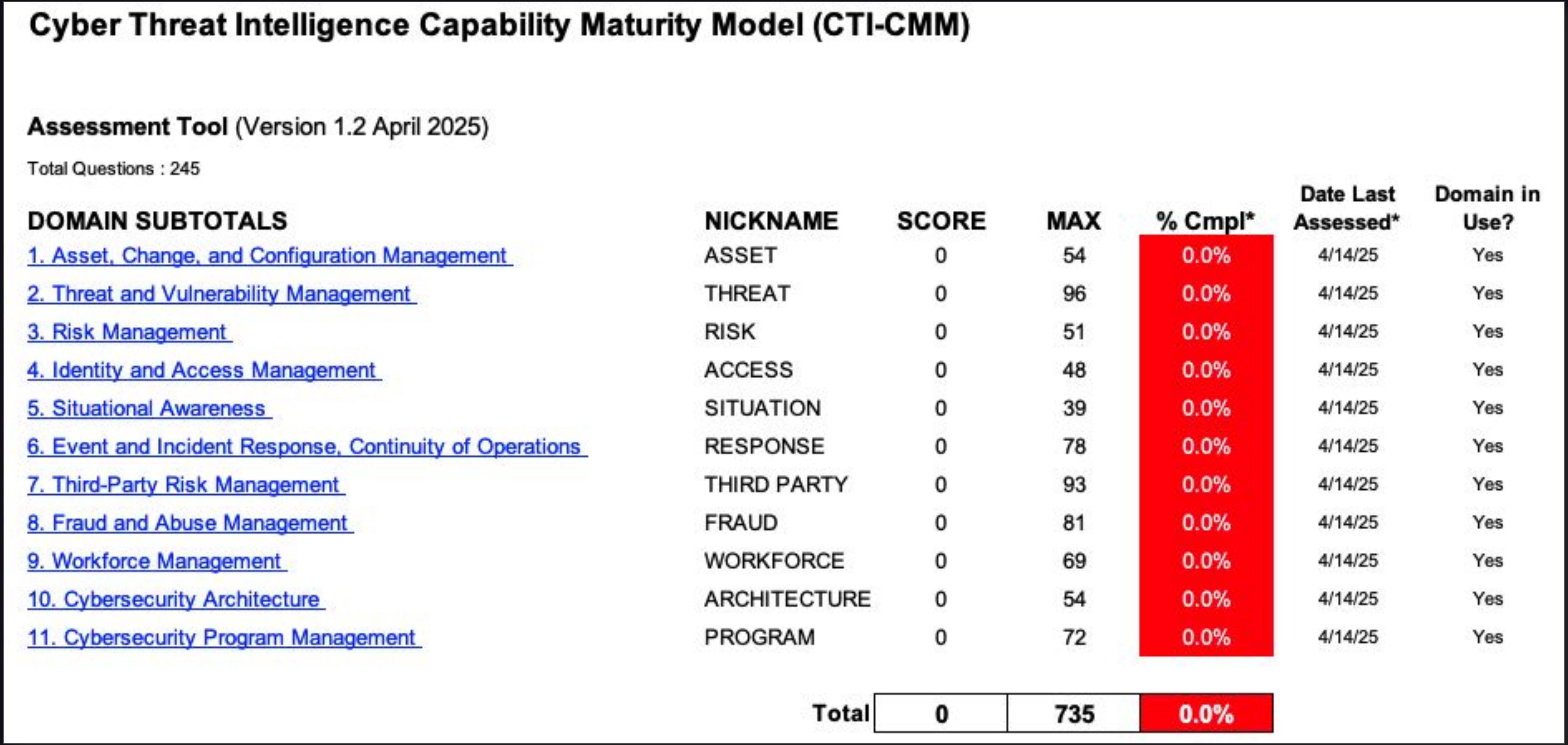
Limit fallout when malware executes in our CI/CD pipeline

Domain 11: PROGRAM

Does CTI support cybersecurity programme?

KPIs for CTI value

Assessment tool



Cyber Threat Intelligence Capability Maturity Model (CTI-CMM)

Assessment Tool (Version 1.2 April 2025)

Total Questions : 245

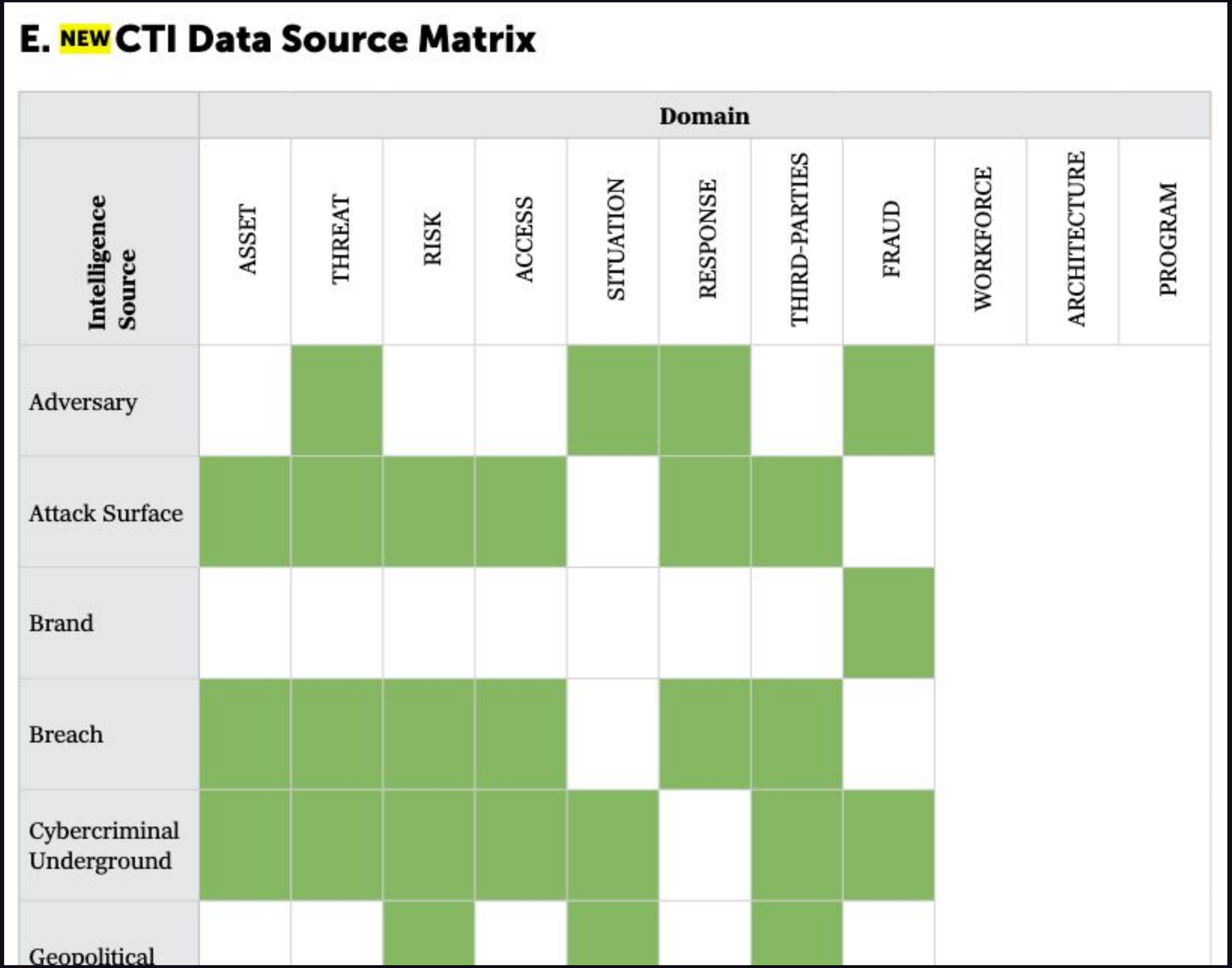
DOMAIN SUBTOTALS	NICKNAME	SCORE	MAX	% Cmpl*	Date Last Assessed*	Domain in Use?
1. Asset, Change, and Configuration Management	ASSET	0	54	0.0%	4/14/25	Yes
2. Threat and Vulnerability Management	THREAT	0	96	0.0%	4/14/25	Yes
3. Risk Management	RISK	0	51	0.0%	4/14/25	Yes
4. Identity and Access Management	ACCESS	0	48	0.0%	4/14/25	Yes
5. Situational Awareness	SITUATION	0	39	0.0%	4/14/25	Yes
6. Event and Incident Response, Continuity of Operations	RESPONSE	0	78	0.0%	4/14/25	Yes
7. Third-Party Risk Management	THIRD PARTY	0	93	0.0%	4/14/25	Yes
8. Fraud and Abuse Management	FRAUD	0	81	0.0%	4/14/25	Yes
9. Workforce Management	WORKFORCE	0	69	0.0%	4/14/25	Yes
10. Cybersecurity Architecture	ARCHITECTURE	0	54	0.0%	4/14/25	Yes
11. Cybersecurity Program Management	PROGRAM	0	72	0.0%	4/14/25	Yes
	Total	**0**	**735**	**0.0%**		

Stakeholders: who might they be?

	Strategic	**Operational**	**Tactical**
Internal	CEO, CFO, CIO, CTO, CISO	Risk Managers, Compliance Officers, Product Development Teams, Privacy Officers	SOC Analysts, IR teams, network / system admins

	Partners	**Customers**	**Communities**
External	Supply Chain MSSPs	End Users B2B Clients	ISACs Threat sharing groups

Intel sources



E. NEW CTI Data Source Matrix

	Domain										
Intelligence Source	ASSET	THREAT	RISK	ACCESS	SITUATION	RESPONSE	THIRD-PARTIES	FRAUD	WORKFORCE	ARCHITECTURE	PROGRAM
Adversary		🟩			🟩	🟩		🟩			
Attack Surface	🟩	🟩	🟩	🟩		🟩	🟩				
Brand								🟩			
Breach	🟩	🟩	🟩	🟩		🟩	🟩				
Cybercriminal Underground	🟩	🟩	🟩	🟩	🟩		🟩	🟩			
Geopolitical			🟩		🟩		🟩				

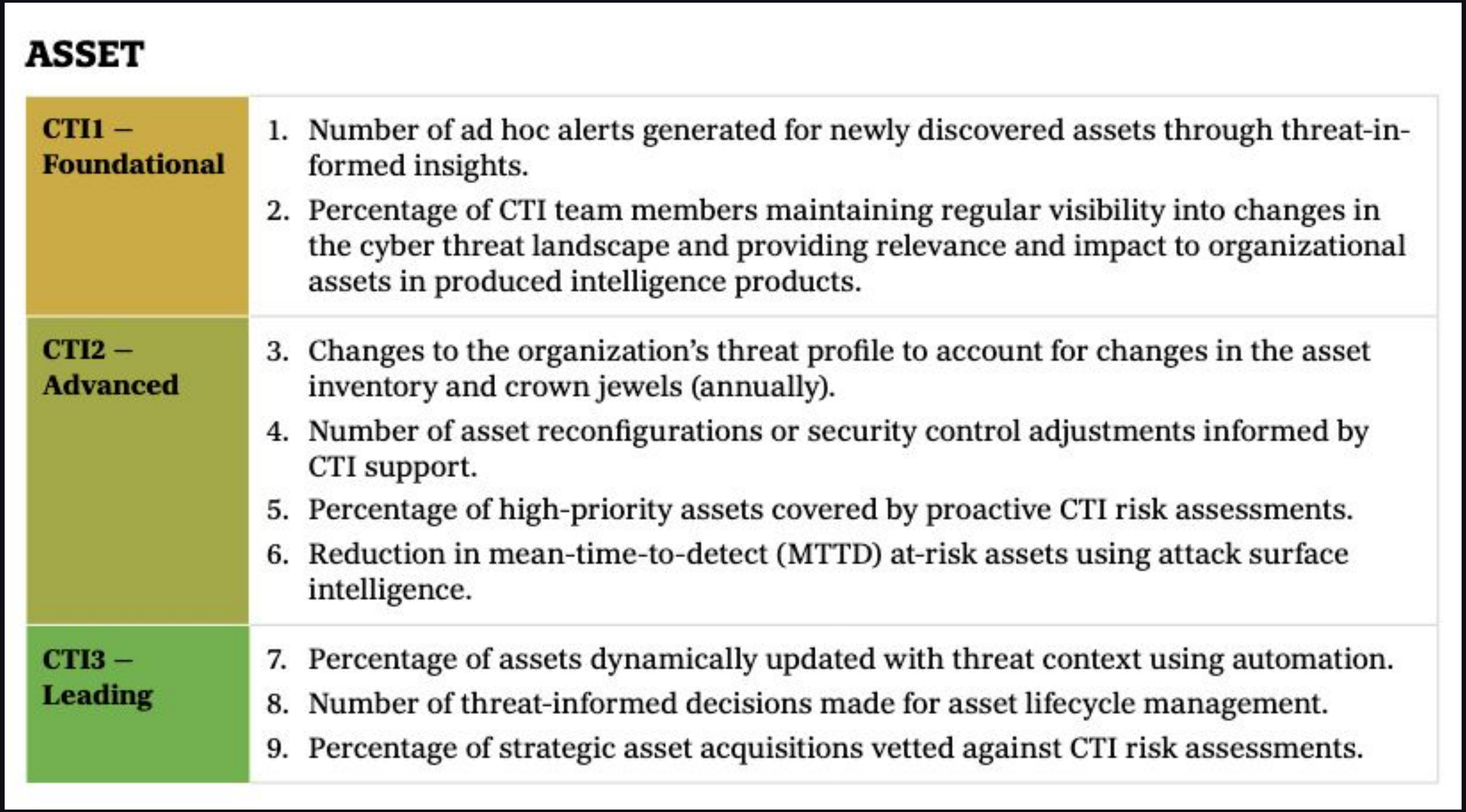
CTI metrics

Show me the incentive, I’ll show you the outcome
- Charlie Munger

CTI metrics

Good	Caution needed
● Asset % considered in CTI ● CTI report % used for decisions	● Detection alert count? ● Number of IoCs

CTI metrics



ASSET

CTI1 – Foundational	1. Number of ad hoc alerts generated for newly discovered assets through threat-informed insights. 2. Percentage of CTI team members maintaining regular visibility into changes in the cyber threat landscape and providing relevance and impact to organizational assets in produced intelligence products.
CTI2 – Advanced	3. Changes to the organization’s threat profile to account for changes in the asset inventory and crown jewels (annually). 4. Number of asset reconfigurations or security control adjustments informed by CTI support. 5. Percentage of high-priority assets covered by proactive CTI risk assessments. 6. Reduction in mean-time-to-detect (MTTD) at-risk assets using attack surface intelligence.
CTI3 – Leading	7. Percentage of assets dynamically updated with threat context using automation. 8. Number of threat-informed decisions made for asset lifecycle management. 9. Percentage of strategic asset acquisitions vetted against CTI risk assessments.

Still being developed!

V1.0: Initial release

V1.1: Added FRAUD domain, added assessment tool

V1.2: Added metrics, feeds

V2.0: late 2025 / early 2026

Contact

Prescott Pym / Chris Horsley
prescott.pym@cosive.com
chris.horsley@cosive.com