Best practices for large-scale surveys conducted based on the M3TID framework

3/7/2025

PwC Consulting LLC
Akira Urano

pwc

Who am I

Akira Urano, Senior Associate

PwC Consulting LLC

Expertise

Cybersecurity Threat Research, Threat Intelligence

Background

Intelligence operation in the Japan Maritime Self-Defense Force and a cybersecurity threat research at a major Japanese security vendor.

Also presented research at international conferences such as Black Hat Asia, RSA Conference, M3AAWG, etc.

Agenda

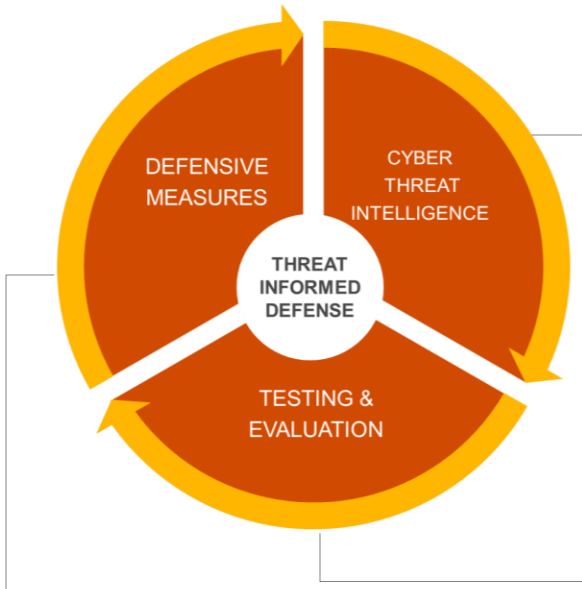
1. **Background**
2. **Methodology**
3. **Insights**
4. **Lessons Learned**
5. **Wrap up**

1

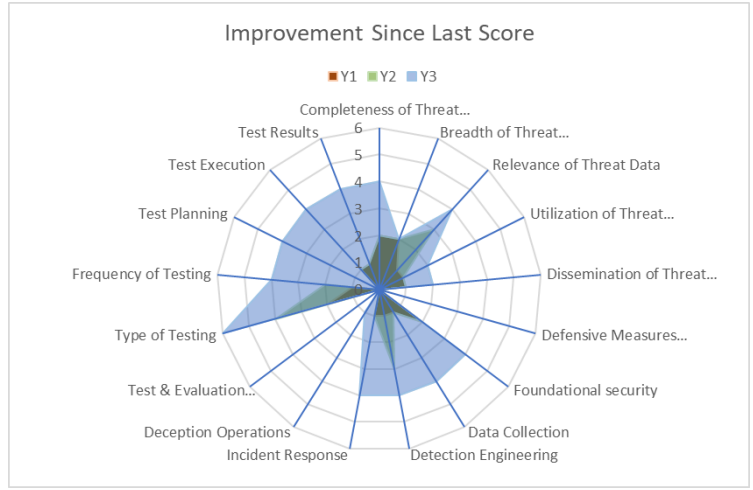
Background

Measure, Maximize and Mature Threat-Informed Defense(M3TID)

M3TID is a maturity model on Threat-informed Defense by MITRE.
Combined with other assessments, it is effective in prioritizing countermeasures.



Dimensions	Key components
Cyber threat intelligence (CTI)	Depth of threat data
	Breadth of threat information
	Relevance of threat data
	Utilization of threat information
	Dissemination of threat reporting
Defensive measures (DM)	Foundational security
	Data collection
	Detection engineering
	Incident response
	Deception operations
Test & evaluation (T&E)	Types of testing
	Frequency of testing
	Test planning
	Test execution
	Test results



https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/measure-maximize-and-mature-threat-informed-defense-m3tid/

Motivation for the large-scale survey

In order to improve the maturity of threat-informed defense based on threat intelligence at Japanese companies, it is first necessary to understand the actual situation. By conducting a large-scale survey using, we thought that we could quantitatively grasp the maturity of threat-informed defense in Japan and propose some recommendations.

Expectations

- Understanding the characteristics of the overall maturity level of Threat-Informed Defense of Japanese companies
- Extracting factors that influence the maturity level (hypotheses: industry, business size, etc.)
- Deriving recommendations

2

Methodology

Survey overview

The survey was conducted online, and responses were received from 200 companies.

Job	Information systems or information security related employees
Position	Section manager level or above
Organization size	Sales of 50 billion yen or more
Survey period	June 2024
Survey method	Online questionnaire
Number of respondents	200

Designing the questions

Questions regarding information about the respondents (industry, number of employees, annual sales, respondent's job title, and level of understanding of security measures) were added, making it possible to group respondents from multiple perspectives.

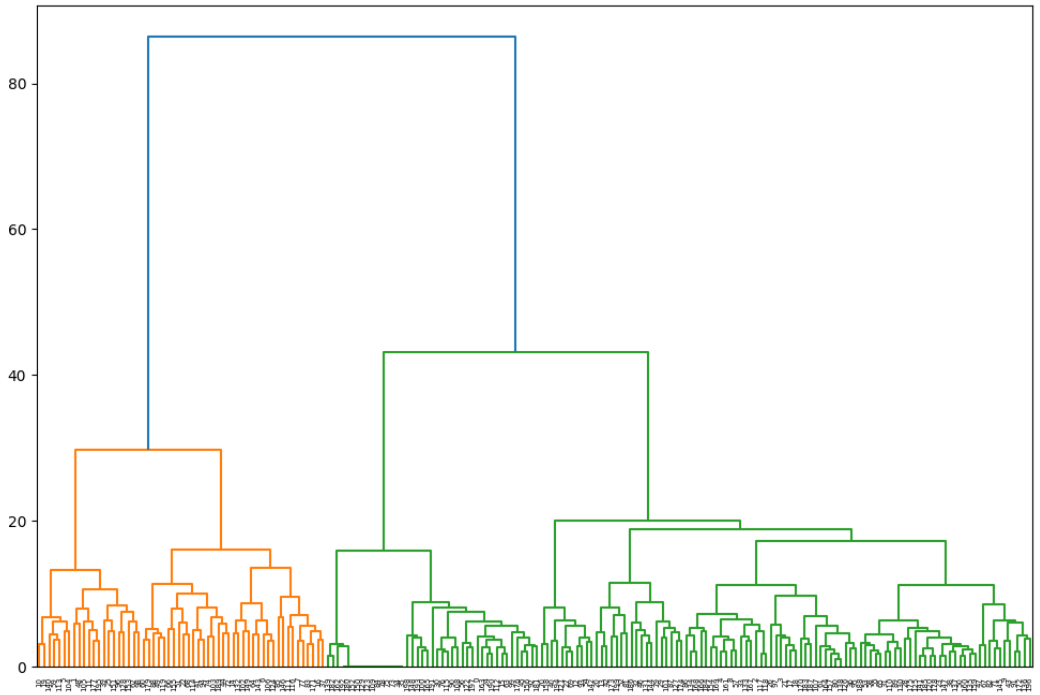
Samples of additional questions	Intention of question design
Q2. Please select your company's sales for the past year. Please select the amount including group companies, etc. A2. (a) Less than 100 million yen (b) 100 million yen - less than 50 billion yen (c) 50 billion yen - less than 100 billion yen (d) 100 billion yen - less than 300 billion yen (e) 300 billion yen - less than 500 billion yen (f) 500 billion yen - less than 800 billion yen (g) 800 billion yen - less than 1 trillion yen (h) 1 trillion - less than 5 trillion yen (i) 5 trillion - less than 10 trillion yen (j) 10 trillion yen or more (k) Unknown	• Want to find correlations between industry and company size and maturity scores. • As qualitative variables, they are easy to process statistically.

Data Analysis

Hierarchical/Non-Hierarchical Cluster analysis on survey responses from 200 Japanese companies using open-source data analysis library.

Hierarchical clustering

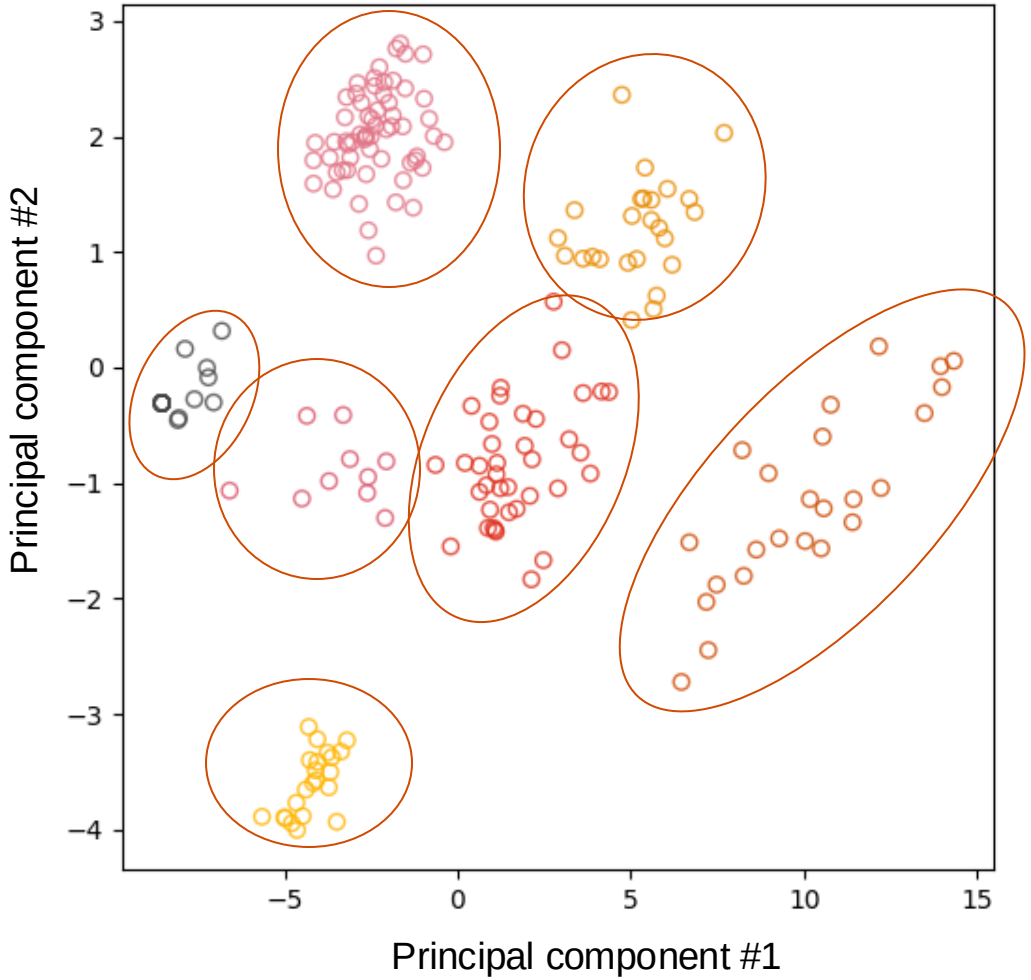
n=200



Roughly divided into 7 or 8 groups.

k-means clustering (Non-Hierarchical)

k=7, n=200



3

Insights

Average maturity of Japanese companies(1)

The average maturity of Japanese companies is 2.0 points for CTI, 1.9 points for DM, and 2.1 points for T&E, which is not a high level of maturity.

Full score: 6.0

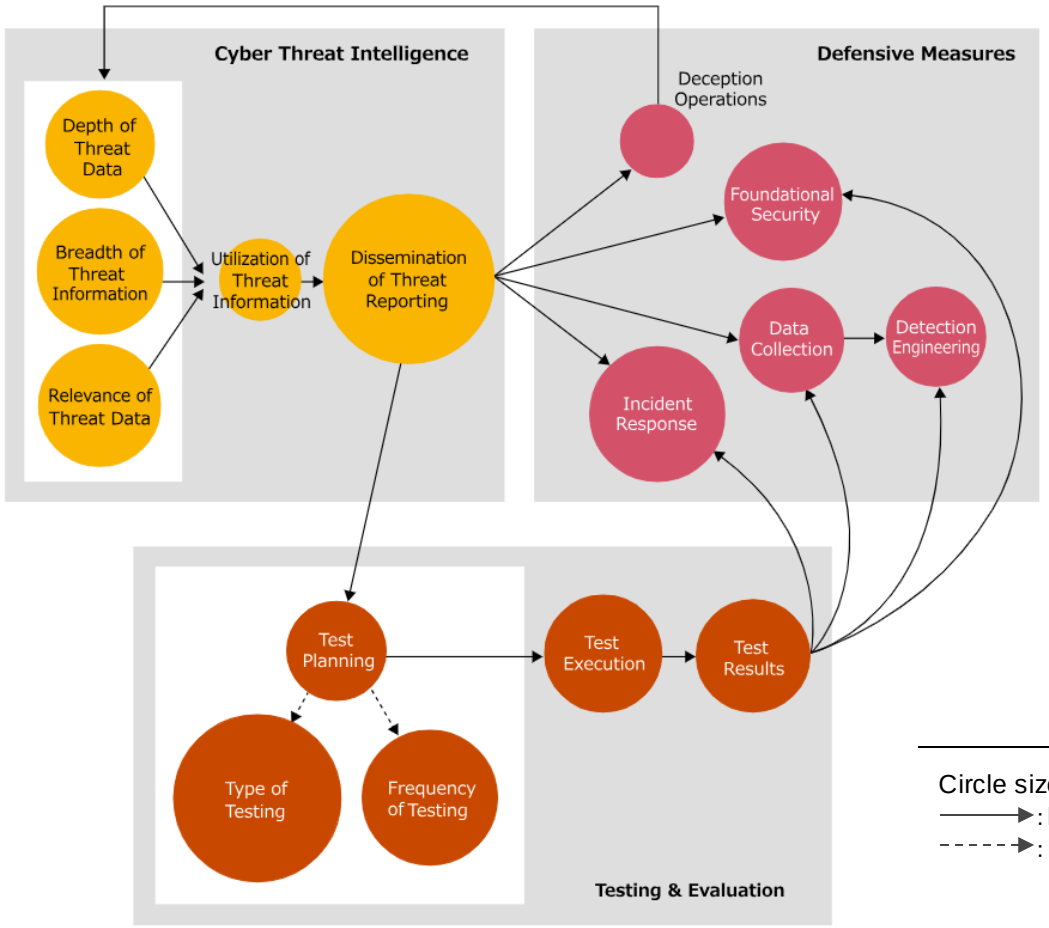
Threat-Informed DefenseDimension	Maturity Score
Overall TID Maturity (weighted)	**33%**
Cyber Threat Intelligence Maturity	2.042
I.1 - Depth of Threat Data	1.945
I.2 - Breadth of Threat Information	2.060
I.3 - Relevance of Threat Data	2.050
I.4 - Utilization of Threat Information	1.740
I.5 - Dissemination of Threat Reporting	2.415
Defensive Measures Maturity	1.919
D.1 - Foundational security	2.015
D.2 - Data Collection	1.910
D.3 - Detection Engineering	1.890
D.4 - Incident Response	2.145
D.5 - Deception Operations	1.635
Testing & Evaluation Maturity	2.065
T.1 - Type of Testing	2.330
T.2 - Frequency of Testing	2.140
T.3 - Test Planning	1.880
T.4 - Test Execution	2.000
T.5 - Test Results	1.975

https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/m3tid-survey.html

Average maturity of Japanese companies(2)

Relatively, the maturity of "Dissemination of Threat Reporting" and "Type of Testing" is high, while the maturity of "Utilization of Threat Information" and "Deception Operations" is low.

Relationship between the average maturity level of Japanese companies and each dimension



Legend

Circle size :Proportional to component maturity
→ : Dependency relationship
- - - → : Inclusion relationship

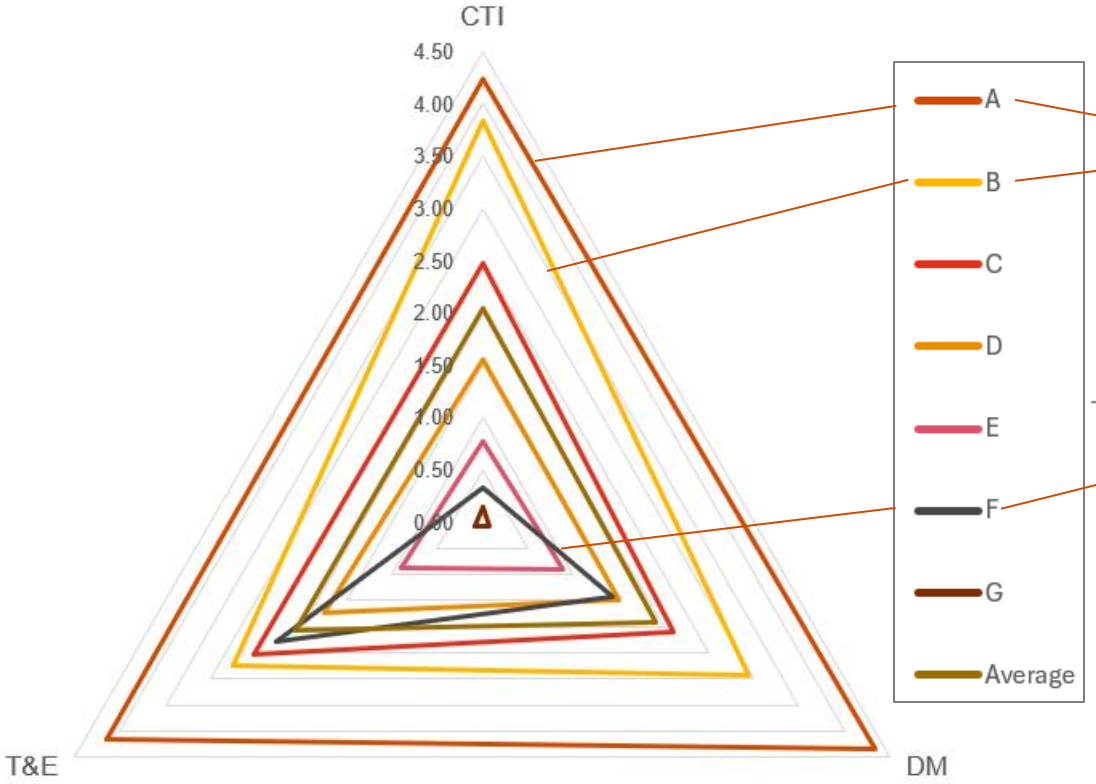
- Threat intelligence is not generated by sufficient analysis of threat information, and security testing and review of countermeasures based on it may be less effective.
- The application of deception technology has not progressed.

https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/m3tid-survey.html

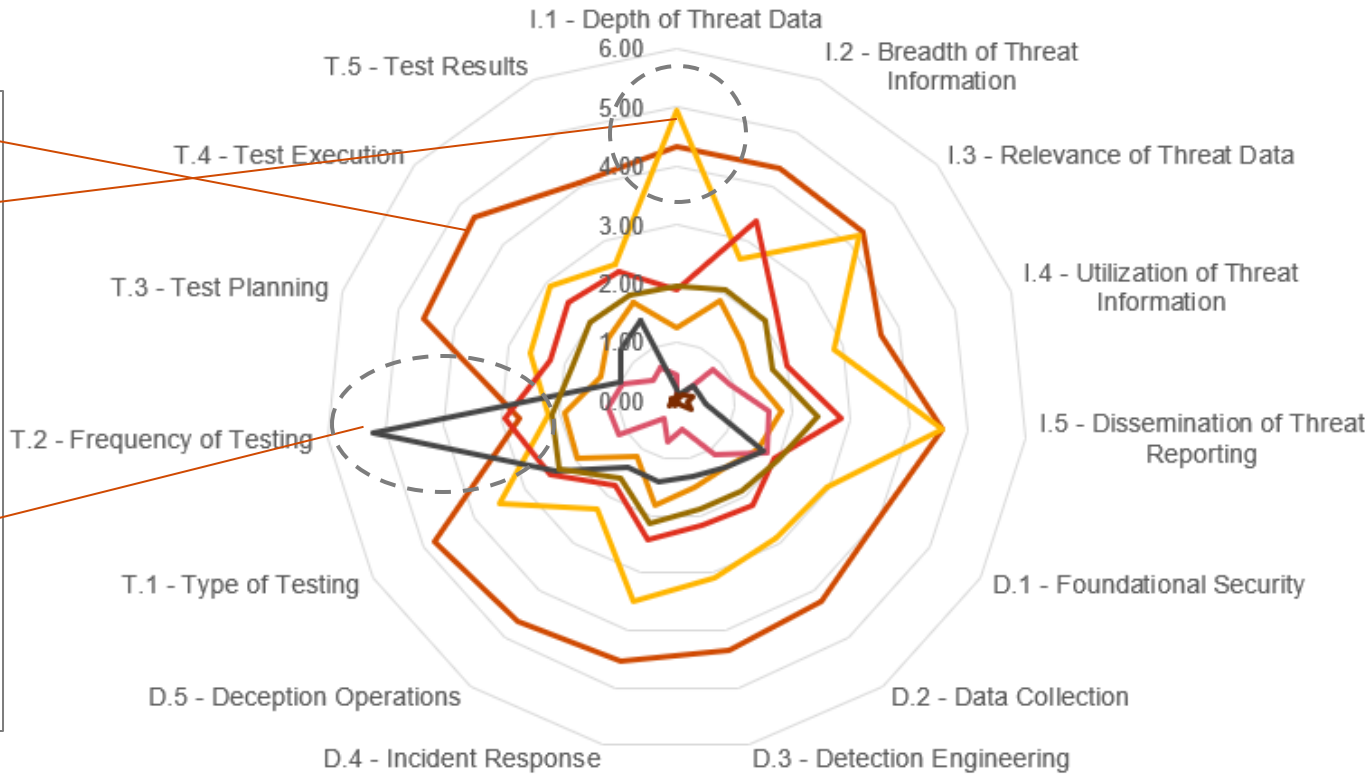
Characteristics of each clustered group

When viewed by dimensions, the shapes are roughly equilateral triangles of different sizes, but when viewed by key components, the characteristics of each group stand out.

By dimensions



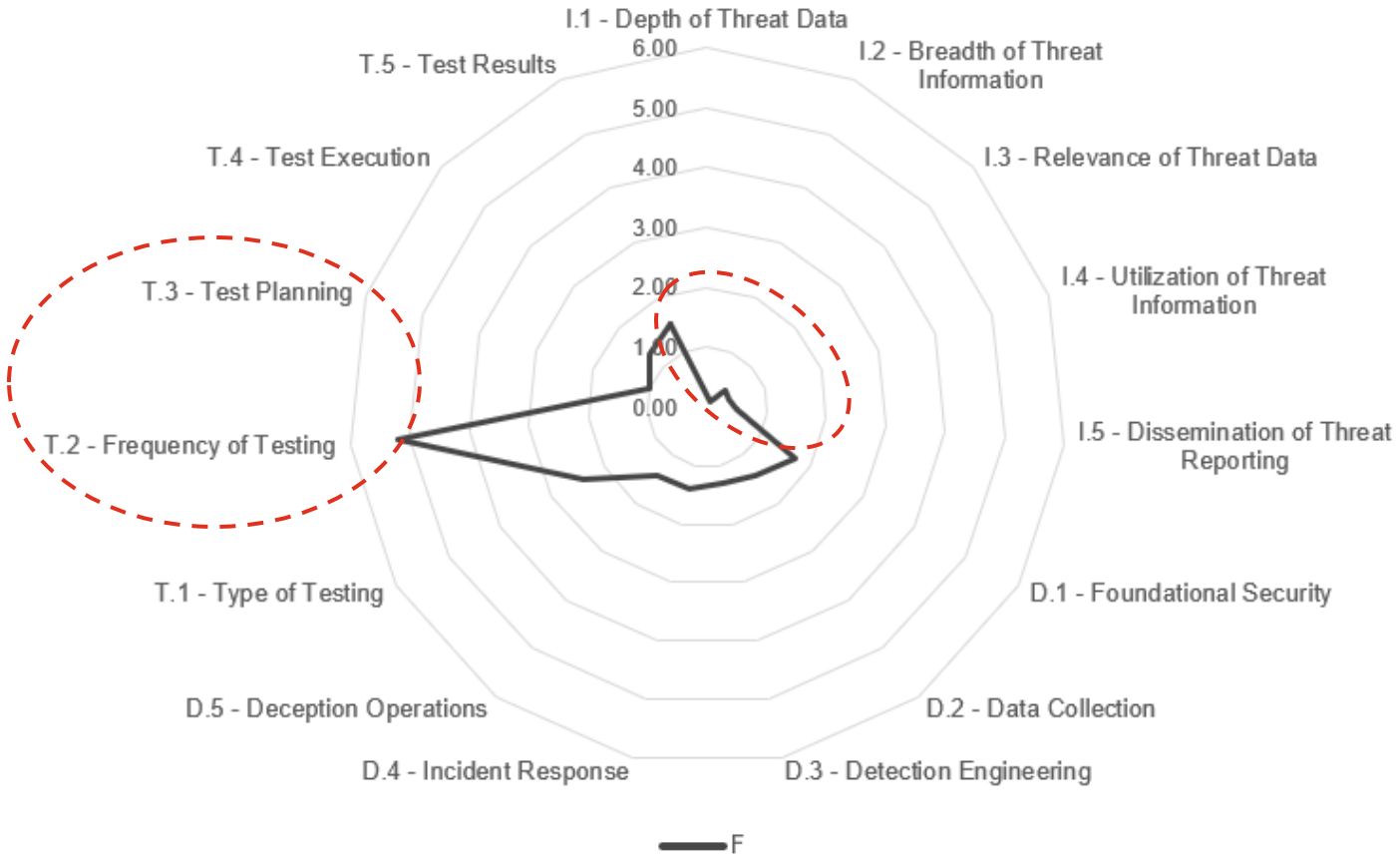
By key components



https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/m3tid-survey02.html

Case Study: Group F

From groups whose chart shapes deviate significantly from a perfect circle, we can make hypotheses about the background circumstances. Based on these hypotheses, we can provide direction for improving the maturity of Threat-Informed Defense.



	Score	Maturity Level	Description
T.2 – Frequency of Testing	5.20	Level 5	Continuous
T.3 – Test Planning	1.00	Level 2	Ad-hoc

+

CTI: Low

Hypothesis: Cybersecurity testing, such as running vulnerability scanning tools, is frequently conducted outside of Threat-Informed Defense activities.

4

Lessons Learned

No space to enter reasons on the survey form

Even if respondents select the same maturity level, the background circumstances are likely to vary depending on the organization to which they belong.
Knowing the details will lead to deeper analysis and concrete recommendations.

Examples of presumed circumstances

- Lack of understanding of Threat-Informed Defense itself
- Limited budget and human resources in charge of security

Sample size is crucial

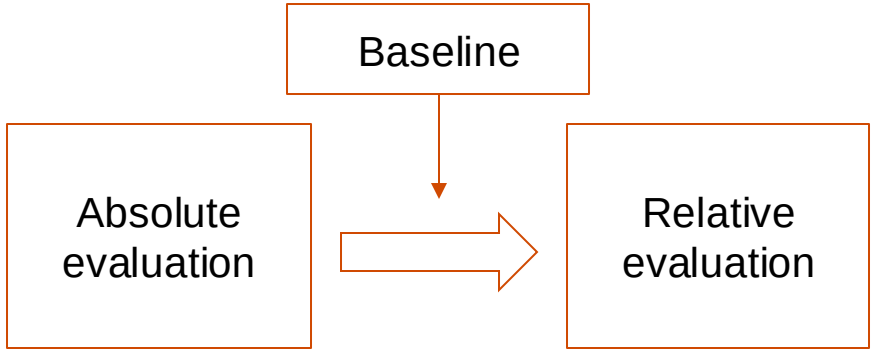
We had initially planned to publish the results of an analysis of trends in maturity scores by industry but decided to cancel this plan because the sample size was small, and the results did not meet statistical significance.

Group by Industry

	CTI	DM	T&E	Count
Industry #1	4.20	3.40	3.80	1
Industry #2	3.40	2.00	2.40	1
Industry #3	2.80	2.53	2.37	6
……..				
Industry #7	2.46	2.15	2.21	30
……..				
Industry #16	1.30	1.50	1.20	2
Industry #17	0.87	0.53	0.53	3
Industry #18	0.45	0.45	0.90	4

n=200

If it were possible to conduct a larger-scale survey, it would be possible to calculate baselines for each group from multiple perspectives, such as by industry and company size.



5

Wrap up

Key takeaways

Motivation	• To grasp the actual state of Threat-Informed Defense of companies in a specific region by applying the M3TID framework
Methodology	• Survey design should be done properly • Data analysis using well-known analytical methods and open-source library
Insights	• Cluster analysis enabled the observation of significant characteristics at key component levels between each group • It is possible to consider background circumstances on a hypothesis basis
Sample size	• The larger the sample size, the easier it is to derive statistically significant results, such as calculating a baseline

Thank you

www.pwc.com/jp