

TLP:CLEAR



NTT DATA
Trusted Global Innovator

IOC-DREAM

-- IOC Distribution in Restricted Environment and Automating response based on MISP

Yifan Wang, Fukusuke Takahashi, Kunio Miyamoto

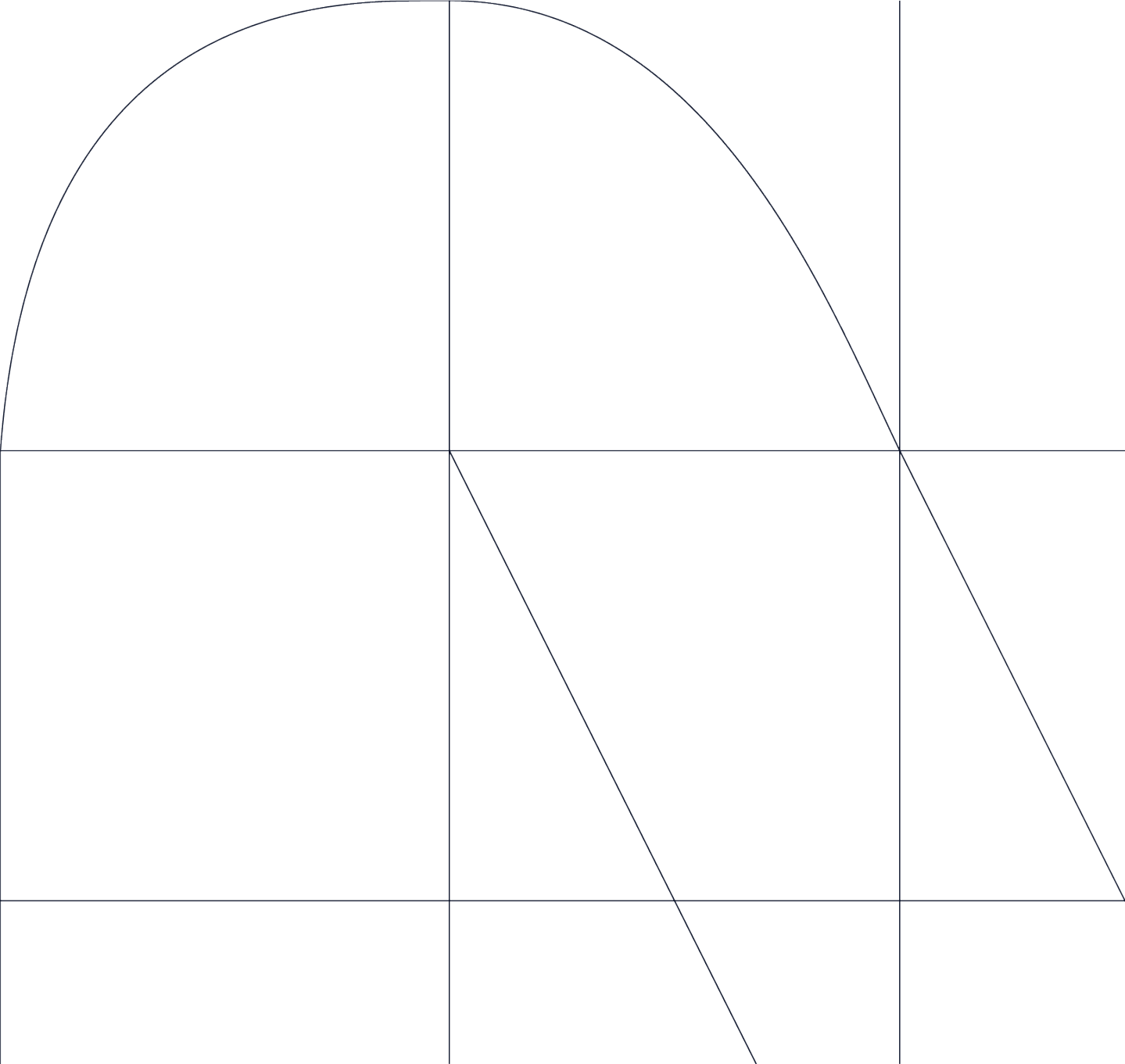
June 5th, 2023

NTT DATA-CERT | Information Security Office | Cyber security engineering department | NTT DATA Corporation

Agenda

- Self Introduction
- Why we choose MISP
- What we implement via MISP
- Integration with others
- Real threat response
- Future work

Introduction



Self Introduction

- NTT DATA-CERT

- CSIRT team of NTT DATA Corporation HQ, established on Jul 1st, 2010 in Tokyo
- Handle internal incident response over 15 years, have over 20 skilled members

- Authors



Yifan Wang

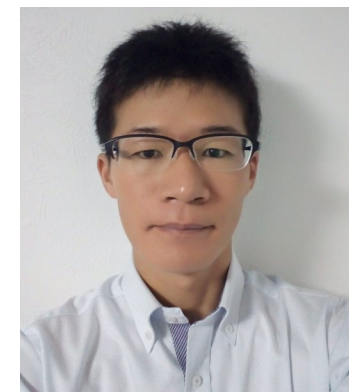
<Yifan.Wang@nttdata.com>

Joined NTTDATA-CERT from 2017, worked on IR, OSINT, SOAR for 6 years

Fukusuke Takahashi

<Fukusuke.Takahashi@nttdata.com>

Joined NTTDATA-CERT from 2018, worked on IR, OSINT, SOAR for 5 years



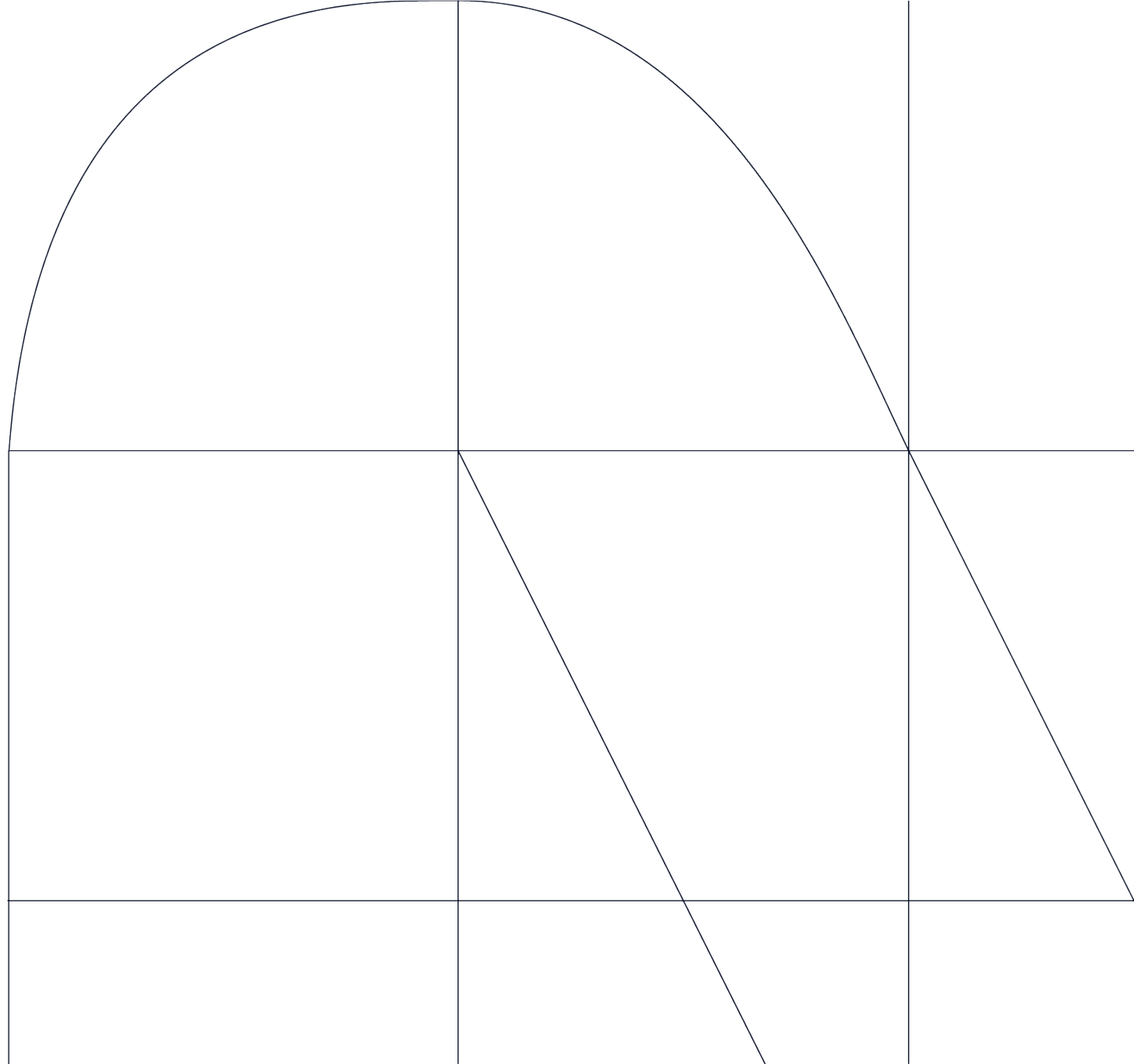
Kunio Miyamoto

<Kunio.Miyamoto@nttdata.com>

Work at NTTDATA-CERT for 13 years(one of NTTDATA-CERT founders)
One of Speaker of 31st Annual FIRST Conference@Edinburgh

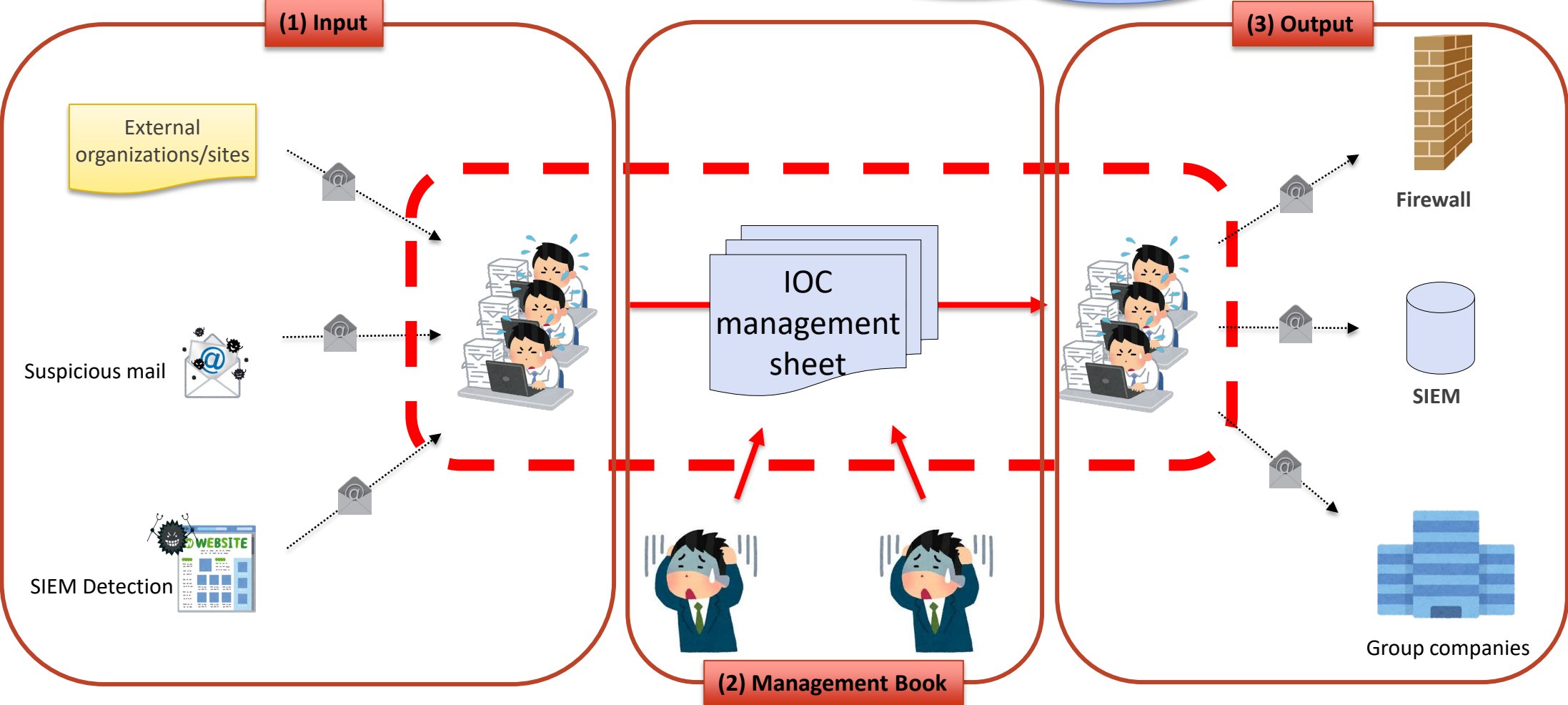


Why we choose MISP



Old workflow (Security Operation)

Give me the automated process!!!

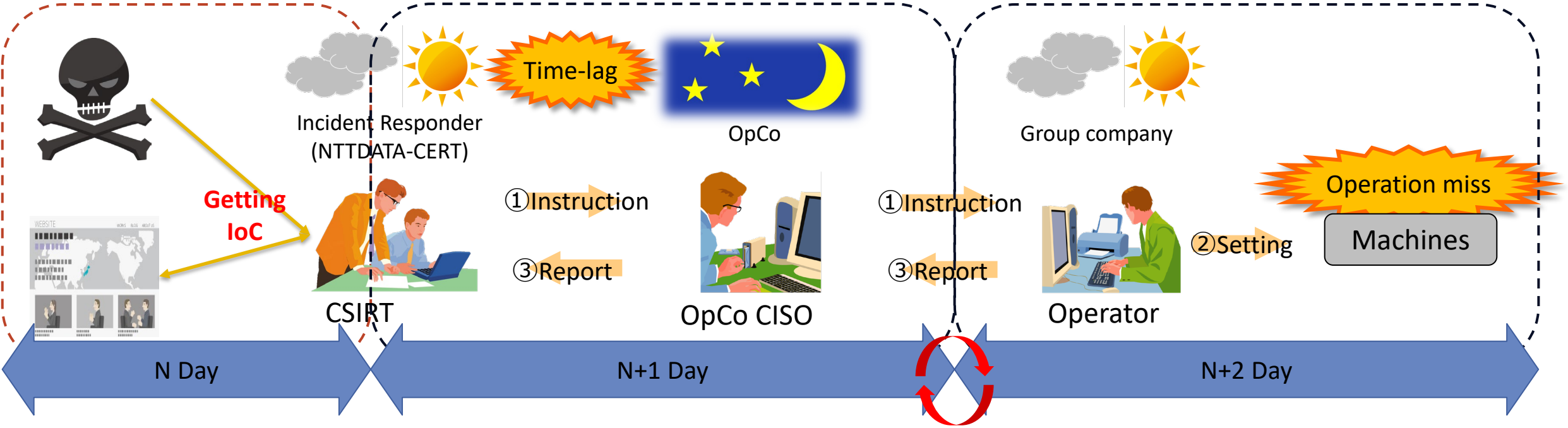


Have to collect threat intelligence due to multiple sources

Have to wait more minutes due to over 10000 IOCs in shared book

Have to deploy on the device due to manual IoC extraction

Old workflow (Threat Sharing)



- In most cases, it would spend over 1 day from distribution to final deployment
 - When some operation miss occurred, there would be a vicious circle for extra N days



Please let me share the IoCs in real-time...

About MISP

- **MISP : Malware Information Sharing Platform**
 - An opensource threat intelligence sharing platform
 - with sharing, storing and correlating functions

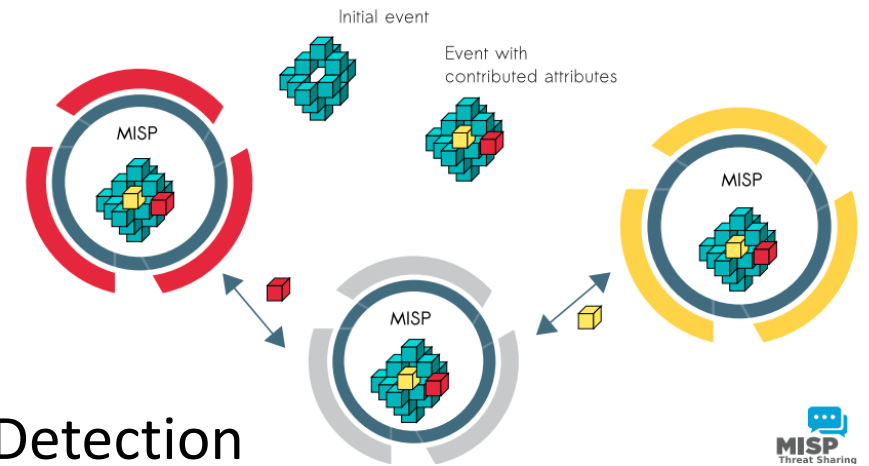
- **MISP Format**

- » **MISP Event :**

- Used to manage each threat
- Commonly created for each Incident/Malware/Detection

- **MISP Attribute :**

- Used to manage each IoC
- Commonly created for each IoC, which is related and included within a MISPEvent

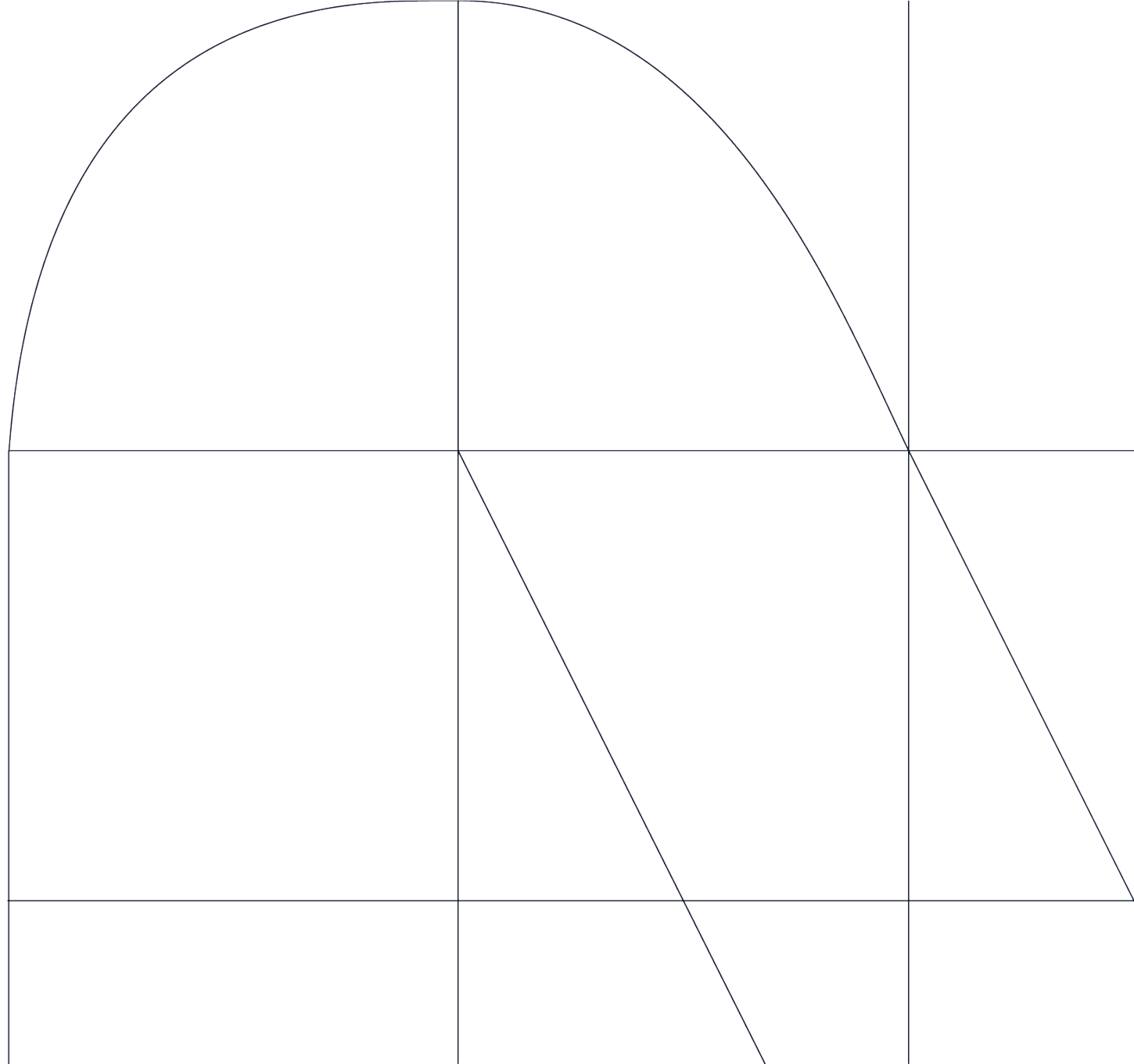


* https://indico.cern.ch/event/595396/contributions/2566371/attachments/1448720/2233260/2017-04-25__MISP_Training_slides.pdf

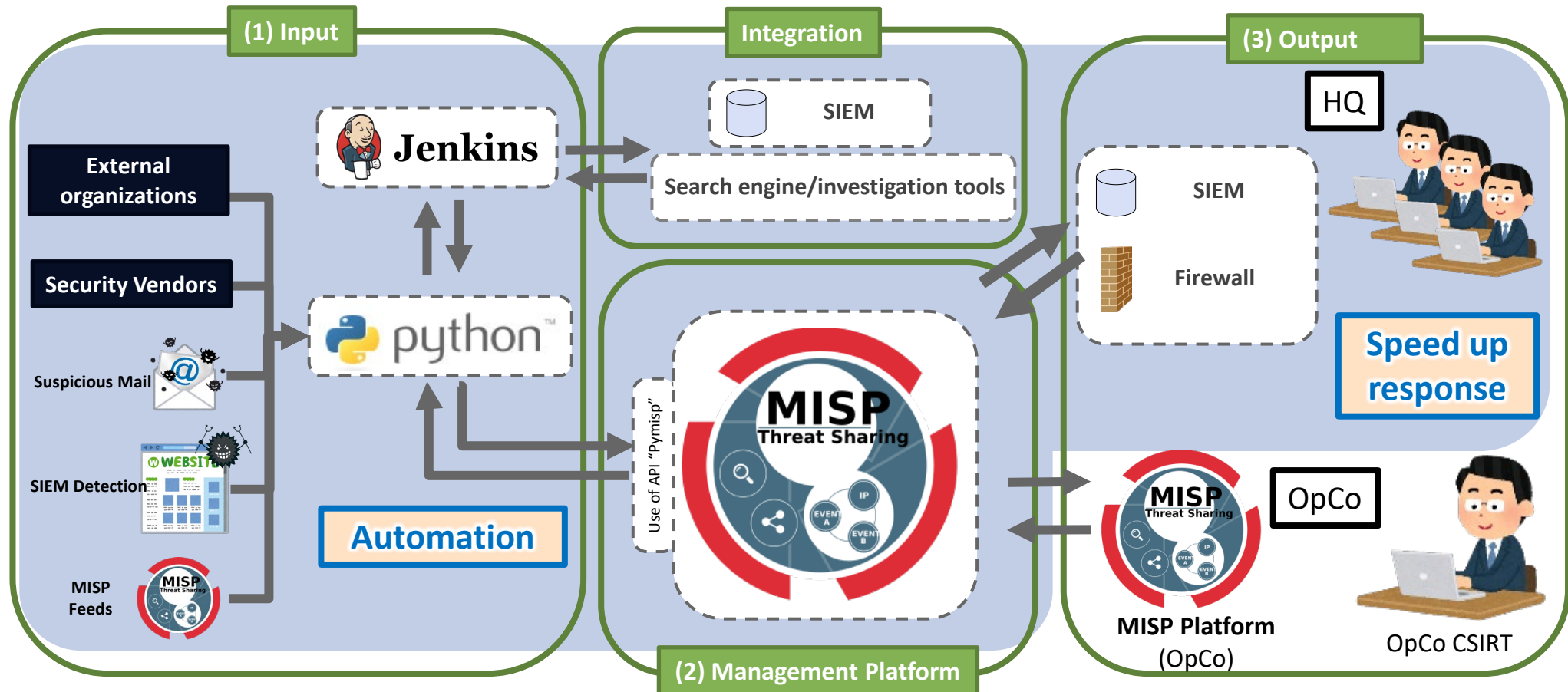
Benefit of MISP integration within NTTDATA Group

1. Optimize SOC workflow and implement SOC automation
 - > Details would be introduced as next slides.
2. Expand available, trusted IoC sources without self-validation
 - > Not only worldwide attacks, some specified/targeted attack information also can be shared as soon as possible.
3. Solve time-lag problem in incident response or other emergency cases.
 - > real-time IoC Sharing is the beginning of real-time auto-response.

What we implement



New Automated workflow based on MISP



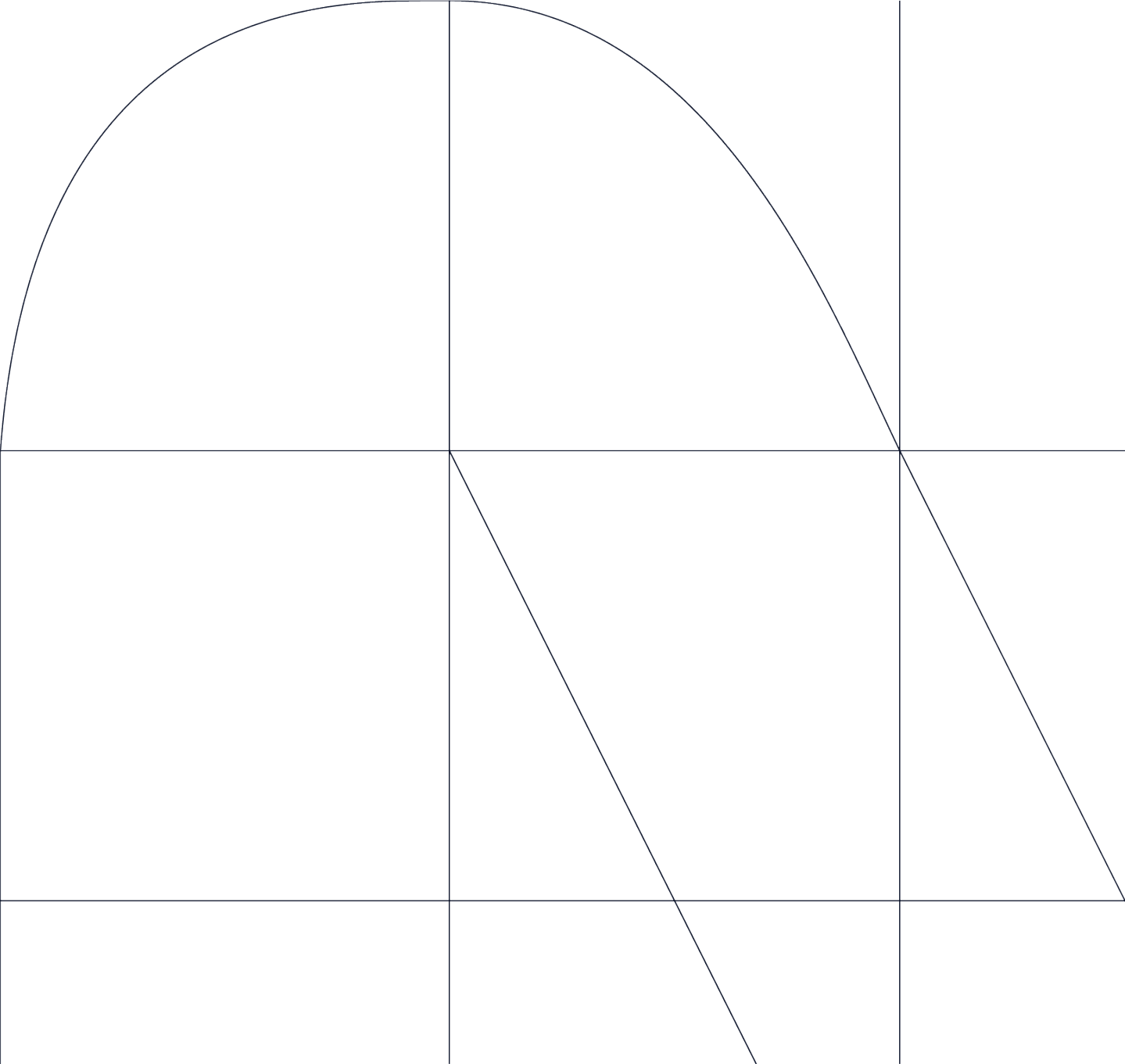
Automate the workflow by API integration 😊
=> over 35000\$/year cost reduction



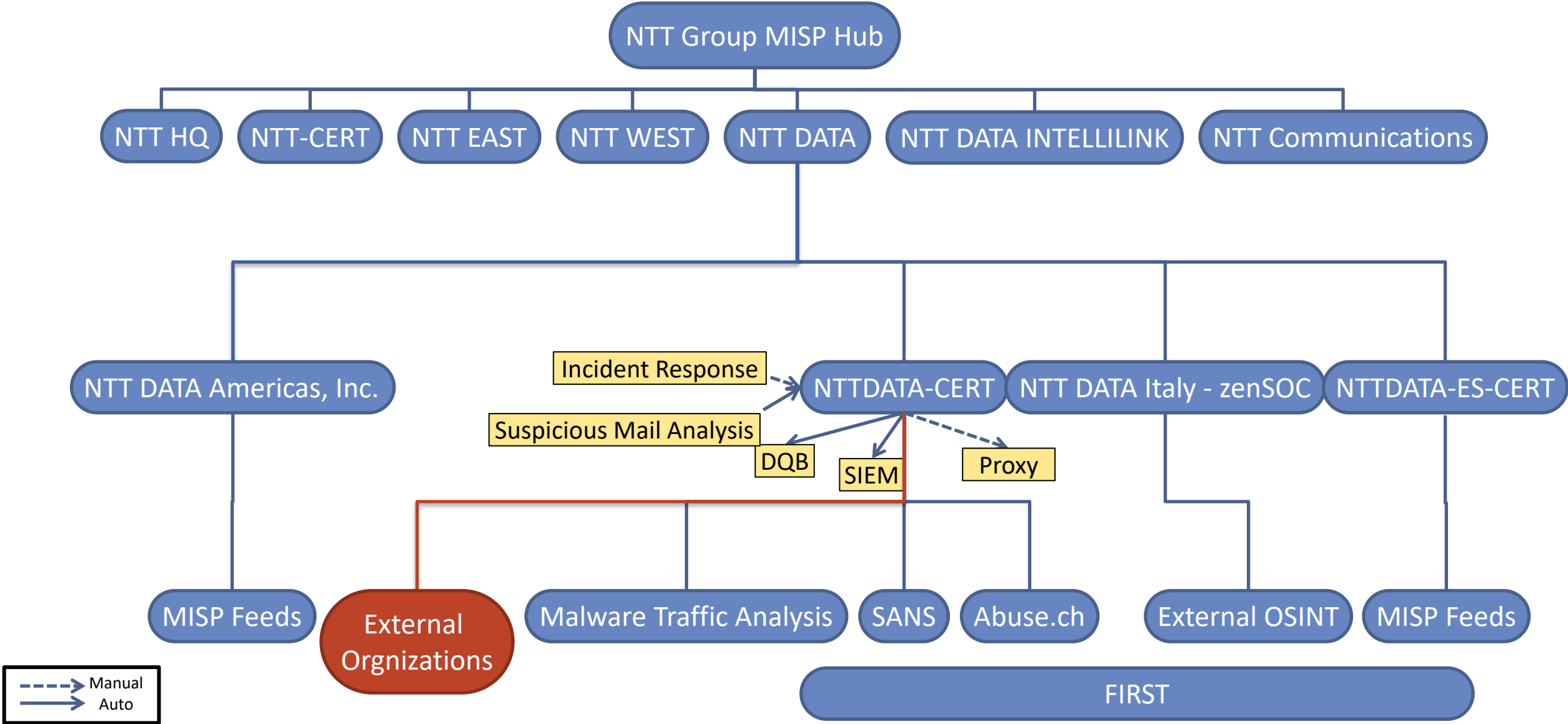
Jenkins jobs used for daily security operation of NTTDATA-CERT

S	名前 ↓	最新の成功ビルド	最新の失敗ビルド	ビルド所要時間
▶	⚠ MISP_Event_Extract_from_SOC_confirmed(PyMISP)	11 時間 #105	29 日 #76	19 秒
▶	✅ MISP_Event_Output(PyMISP)	22 時間 #452	8 日 0 時間 #446	24 秒
5. Integration with others				
▶	✅ MISP_Event_Republish_to_Outside(PyMISP) ▾	1 日 13 時間 #988	—	6 分 23 秒
4. Upload to MISP				
▶	✅ MISP_Event_Upload(PyMISP)	1 日 13 時間 #631	23 日 #620	17 秒
3. Enrichment with external services like SIEM				
▶	⚠ MISP_Exa_Enrichment_01(Common)	21 時間 #86	—	18 秒
▶	✅ MISP_HealthCheck	29 分 #16386	—	1.6 秒
▶	✅ MISP_Job_Input_02(CCI_mail)	1ヶ月 2 日 #58	—	3.8 秒
▶	✅ MISP_Job_Input_03(CCI_req)	13 時間 #842	—	25 秒
▶	✅ MISP_Job_Input_05(Other)	9 日 4 時間 #240	—	3.7 秒
1. Extract IoC from different sources				
▶	✅ MISP_Job_Input_06(Suspicious_mail)	21 時間 #505	29 日 #494	43 秒
▶	⚠ MISP_Meta_Enrichment_01(Common)	13 時間 #1508	—	16 秒
2. Process IoC with formatting for MISP				
▶	✅ MISP_Type_Classification_00(PyMISP)	13 時間 #1496	—	12 秒

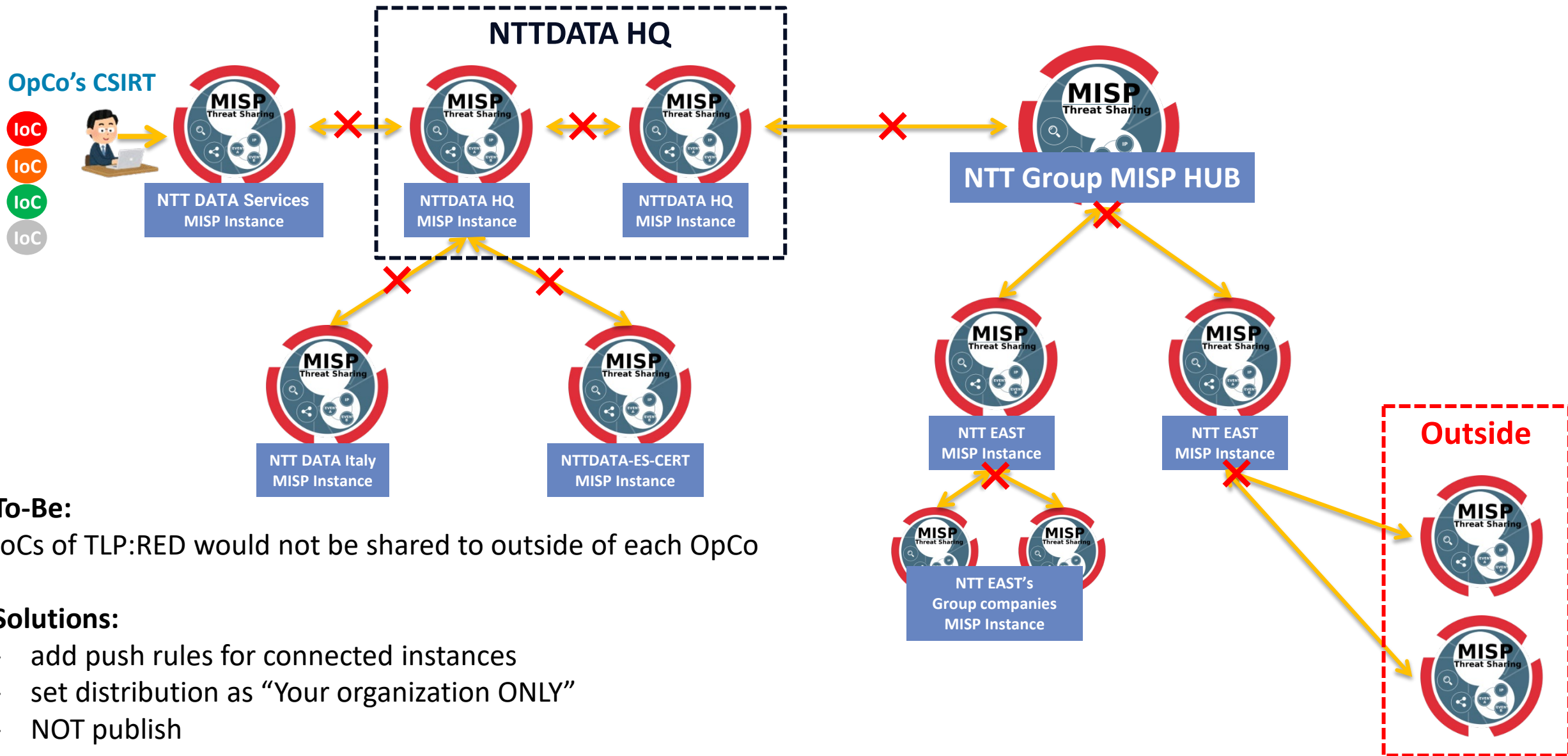
Integration with others



MISP Integration Architecture within NTT Group



Data flow on MISP (for TLP:RED)



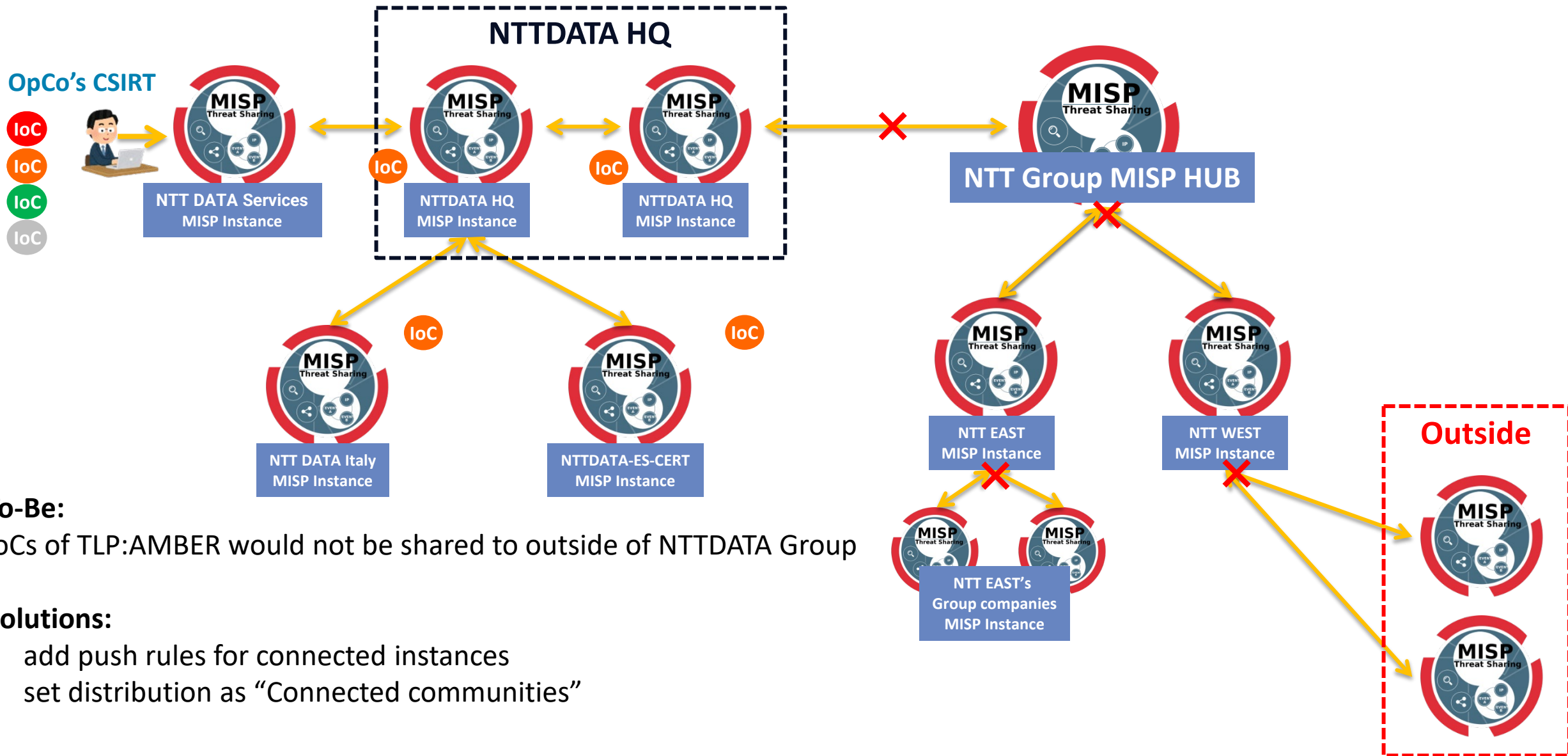
To-Be:

IoCs of TLP:RED would not be shared to outside of each OpCo

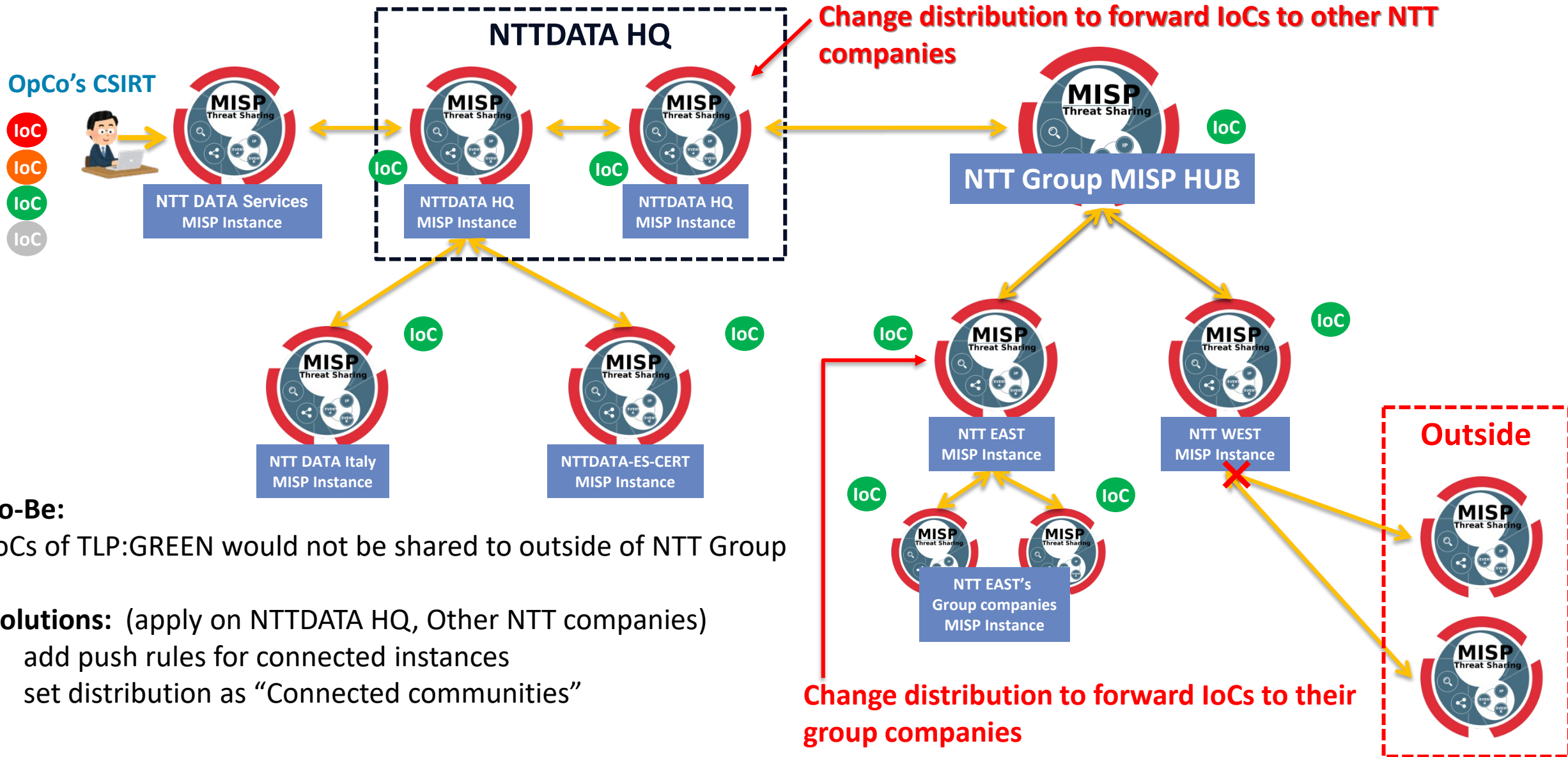
Solutions:

- add push rules for connected instances
- set distribution as "Your organization ONLY"
- NOT publish

Data flow on MISP (for TLP:AMBER)



Data flow on MISP (for TLP:GREEN)



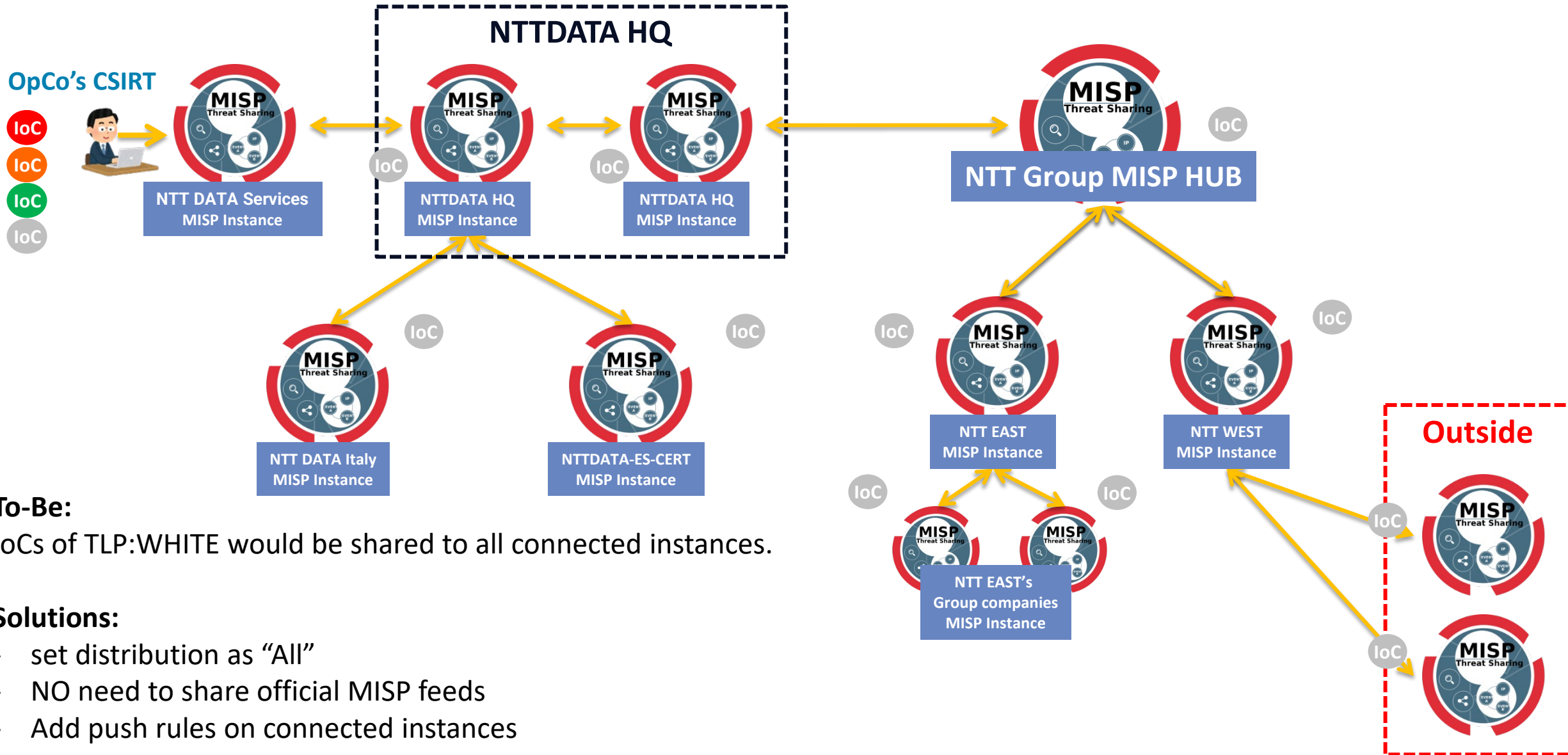
To-Be:

IoCs of TLP:GREEN would not be shared to outside of NTT Group

Solutions: (apply on NTTDATA HQ, Other NTT companies)

- add push rules for connected instances
- set distribution as "Connected communities"

Data flow on MISP (for TLP:WHITE)



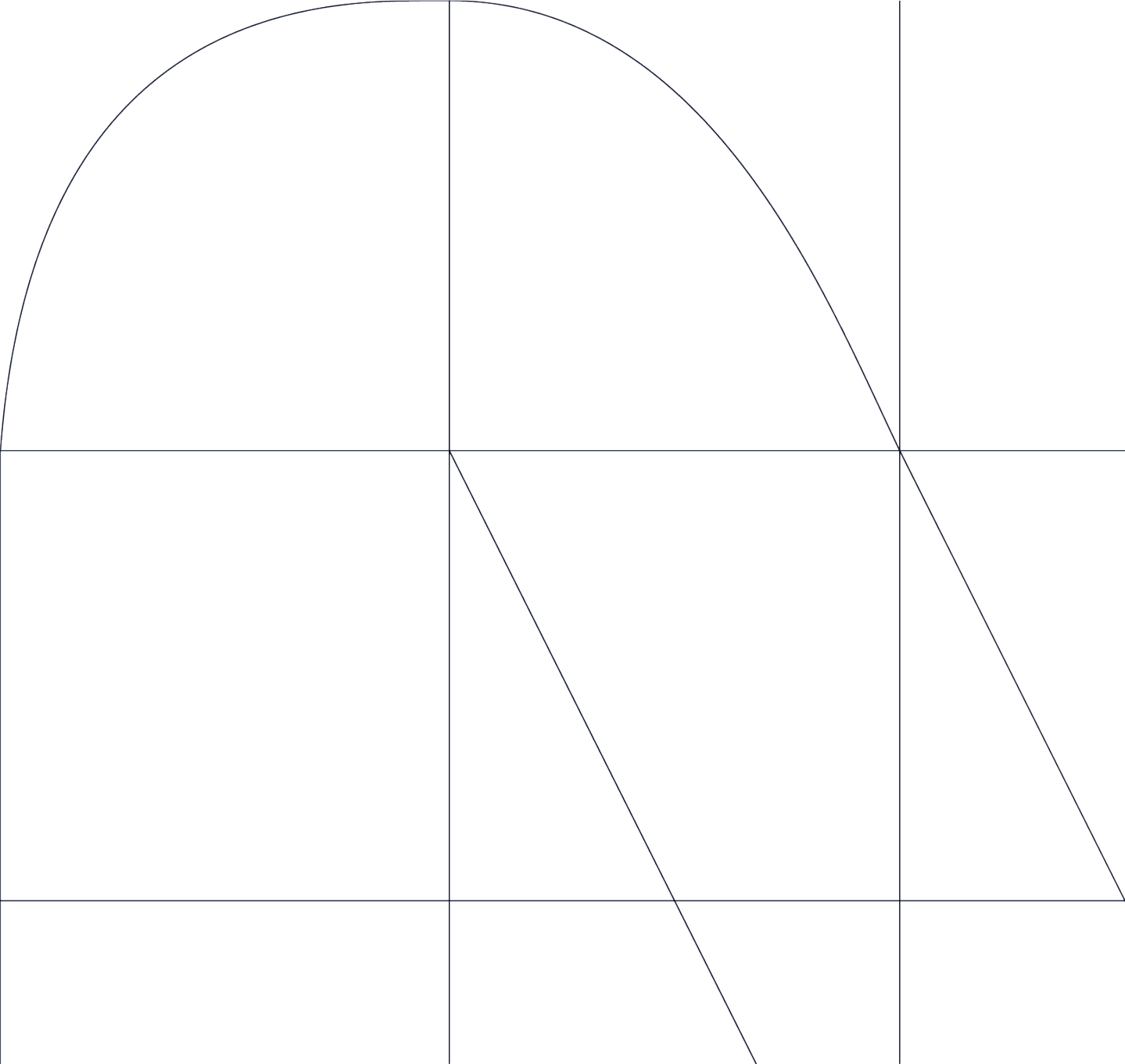
To-Be:

IoCs of TLP:WHITE would be shared to all connected instances.

Solutions:

- set distribution as "All"
- NO need to share official MISP feeds
- Add push rules on connected instances

Real threat response -- Emotet



Background

	News	Event	Sample	Opened	Note
2021					
Nov	Emotet restarted[1]				
Dec	Compromised case appeared @Japan [2]				
2022					
Feb	compromised case increased @Japan	Feb 2 1 st Suspicious mail received @NTTDATA-CERT	○		
		Feb 4 1 st Suspicious mail opened by Group company A	○	⚠	OA. No Malicious traffic
		Feb 8 Suspicious mail received @Group company A	○		Reported received.
Feb 10	1 st Awareness of JPCERT/CC[3]	Feb 10 2 nd Suspicious mail received @NTTDATA-CERT	○		
		Feb 22 Monitor & Block started			Import IoC from abuse.ch
		Feb 28 3 rd Suspicious mail received @NTTDATA-CERT	○		
Mar 3	2 nd Awareness of JPCERT/CC [3]	Mar 22 Suspicious mail opened by Group company B	○	⚠	OA. No Malicious traffic
		Mar 28 2 nd Suspicious mail opened by Group company A	×	⚠	Detected & blocked
Apr 26	3 rd Awareness of JPCERT/CC [3]				
		May 10 Monitor & Block finished			No events in April and May

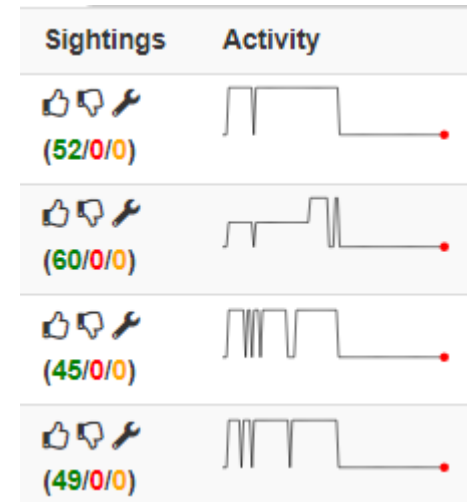
[1]. https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2021_3q_securityreport.pdf

[2]. <https://www.ipa.go.jp/security/announce/20191202.html>

[3]. <https://www.jpcert.or.jp/english/at/2022/at220006.html>

Review of HQ's Emotet IoC collection

- Import IoCs of Emotet from abuse.ch by script
 - FeodoTracker
 - URL Haus (tag:emotet)
- Difference from abuse.ch feed on MISP
 - Abuse.ch feed on MISP
 - Import each URL as an MISPEvent
 - Import tool (script)
 - Import URL/domain/IP into MISP
 - Segment all IoCs (Each MISPEvent has 1000 MISPAttributes)
 - Flexible for customization
 - Extract domain/IP/fqdn from URL for block-list
 - Add sighting to mark the status online/offline
 - Also can be used for visualization and evaluation



Review

(O) ... Collect IoCs before receive suspicious mail
 (X) ... Collect IoCs after receive suspicious mail

Date of mail received	Event	Count of Malicious traffic	Sources				
			ABUSE.CH	External Organization A	Malware Traffic Analysis	SANS Internet Storm Center	External Organization B
Feb 2	1 st Suspicious mail received @NTTDATA-CERT	5	5(O)	0	0	0	0
Feb 4	1 st Suspicious mail opened by Group company A	12	12(O)	12(X)	0	0	0
Feb 8	Suspicious mail received @Group company A	20	20(O)	0	0	0	0
Feb 10	2 nd Suspicious mail received @NTTDATA-CERT	14	14(O)	14(X)	0	0	0
Feb 28	Monitor & Block started	7	7(O)	2(X)	2(X)	0	0
Mar 22	3 rd Suspicious mail received @NTTDATA-CERT	8	8(O)	0	0	0	0

Have been collected before suspicious mail arrived.



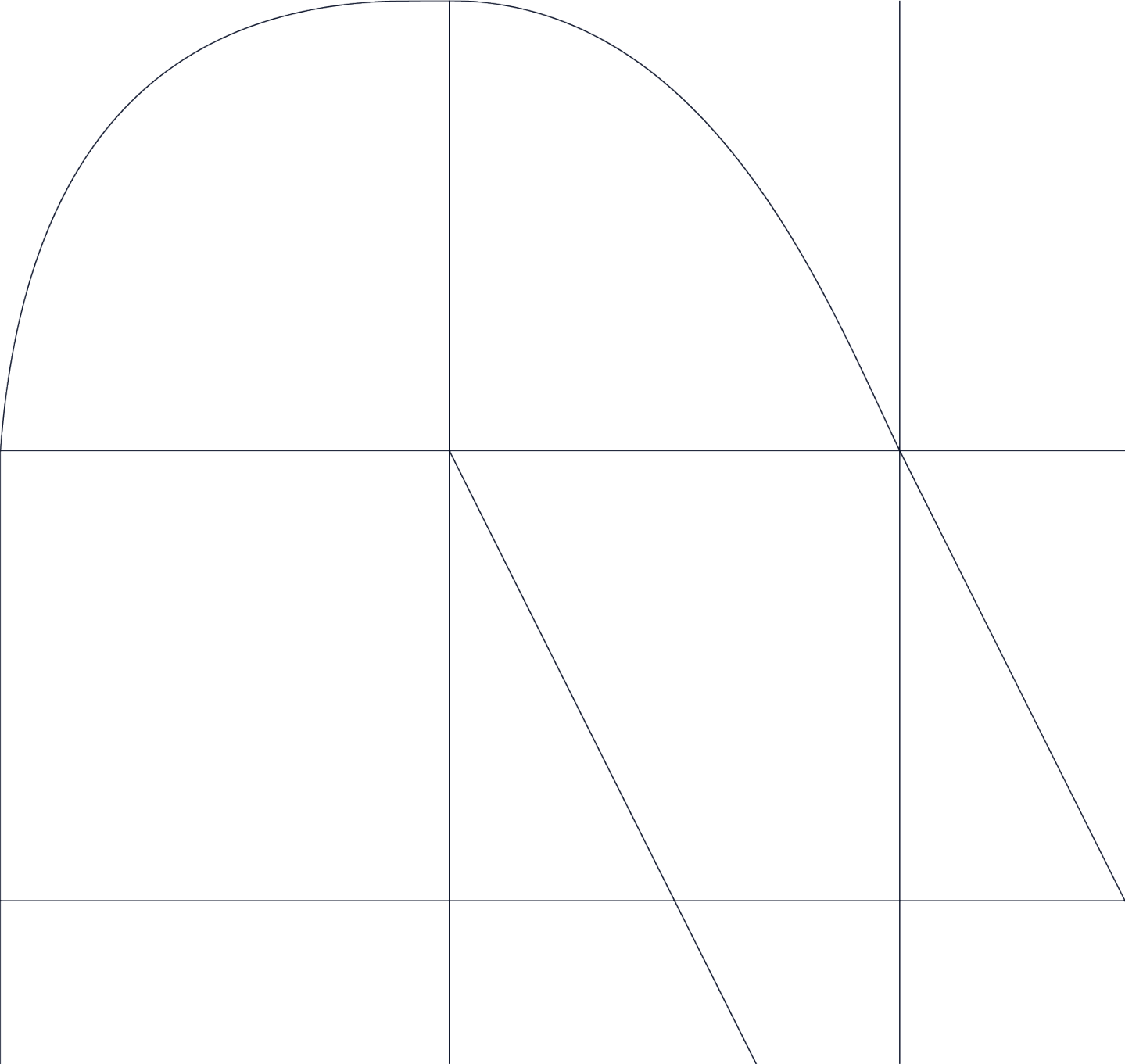
Delay from received



All malicious traffic can be blocked by collecting IoCs from abuse.ch

Not enough to block all malicious traffic

Future work



Standard intelligence management process



1. Planning
2. Collection
3. Processing
4. Analysis
5. Dissemination

Effectively manage intelligence with continuous feedback cycles

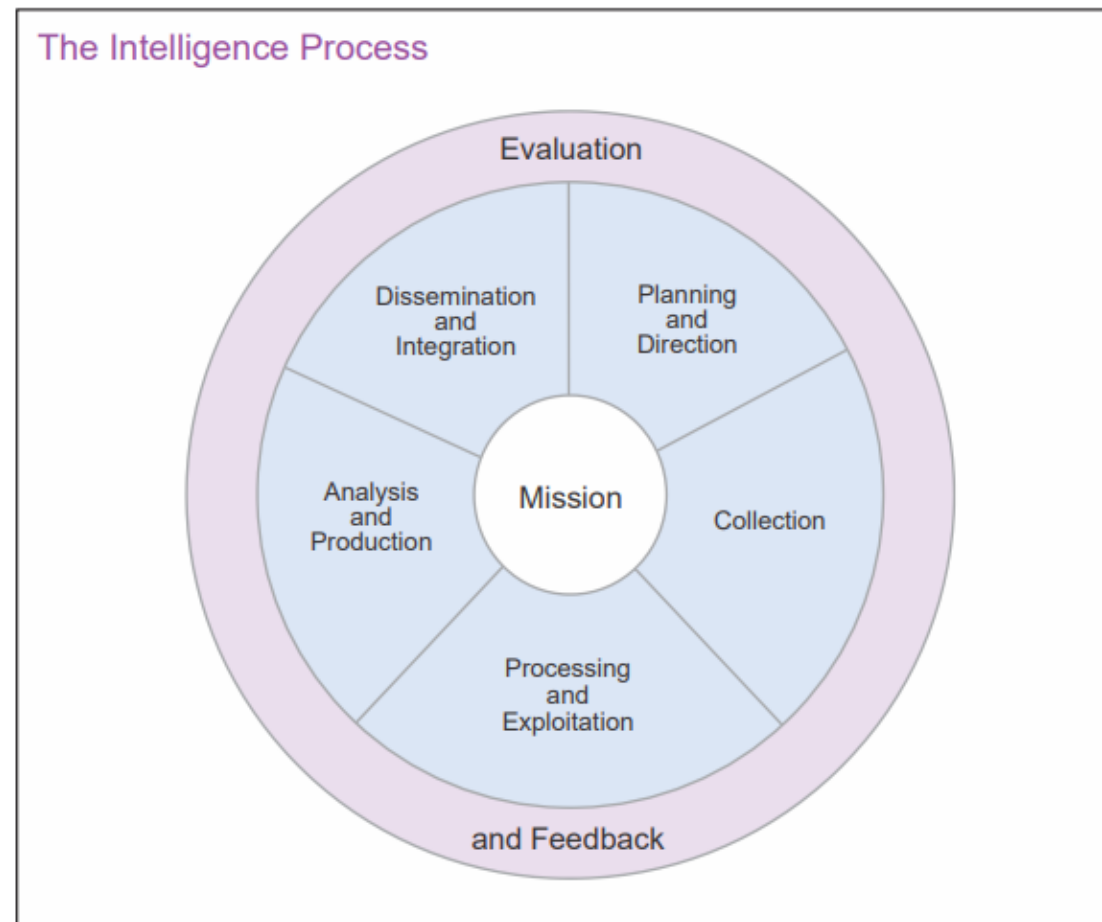


Figure I-3. The Intelligence Process

Joint Chiefs of Staff Document (JP2-0: Joint Intelligence)
https://irp.fas.org/doddir/dod/jp2_0.pdf

To be

NTT DATA-CERT focuses on IoC management and target to implement the process on daily security operation.

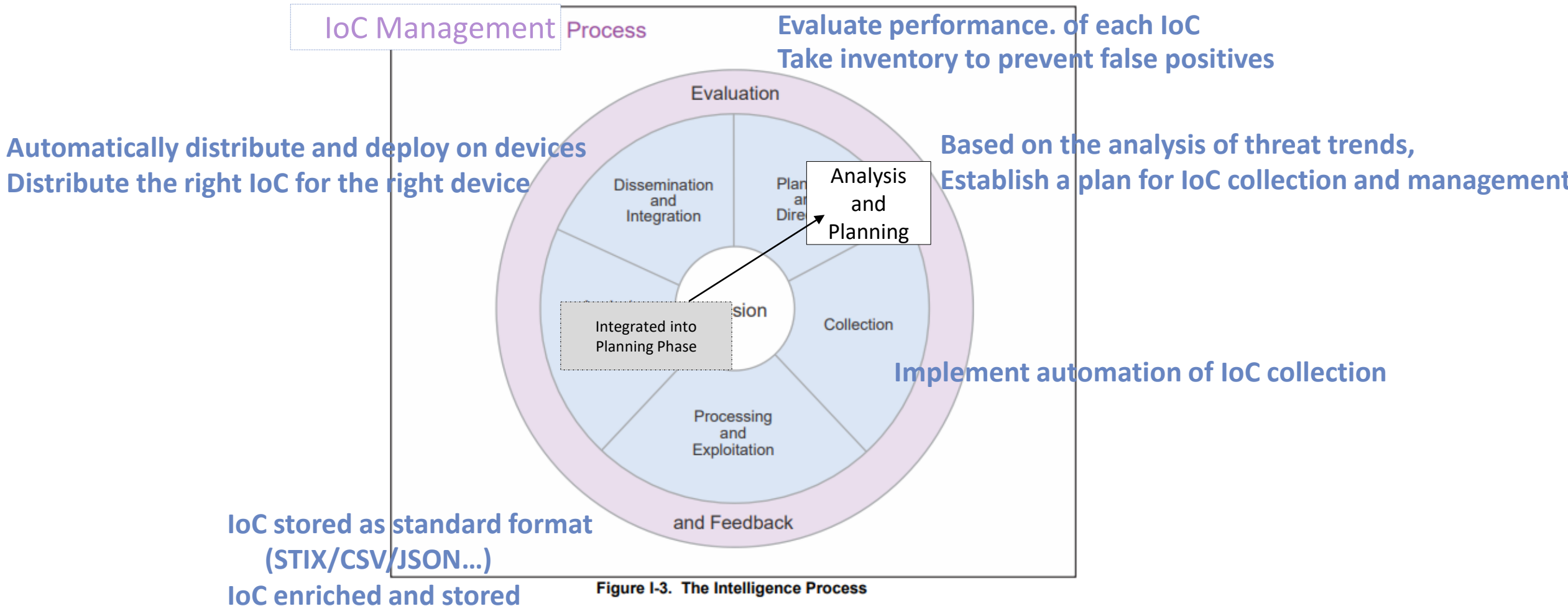


Figure I-3. The Intelligence Process

Address the gaps between To-be and As-is

NTT DATA-CERT plan to incorporate IoC Metabolism activation model

-> **Improve quality of IoCs and respond to threat trends better!**

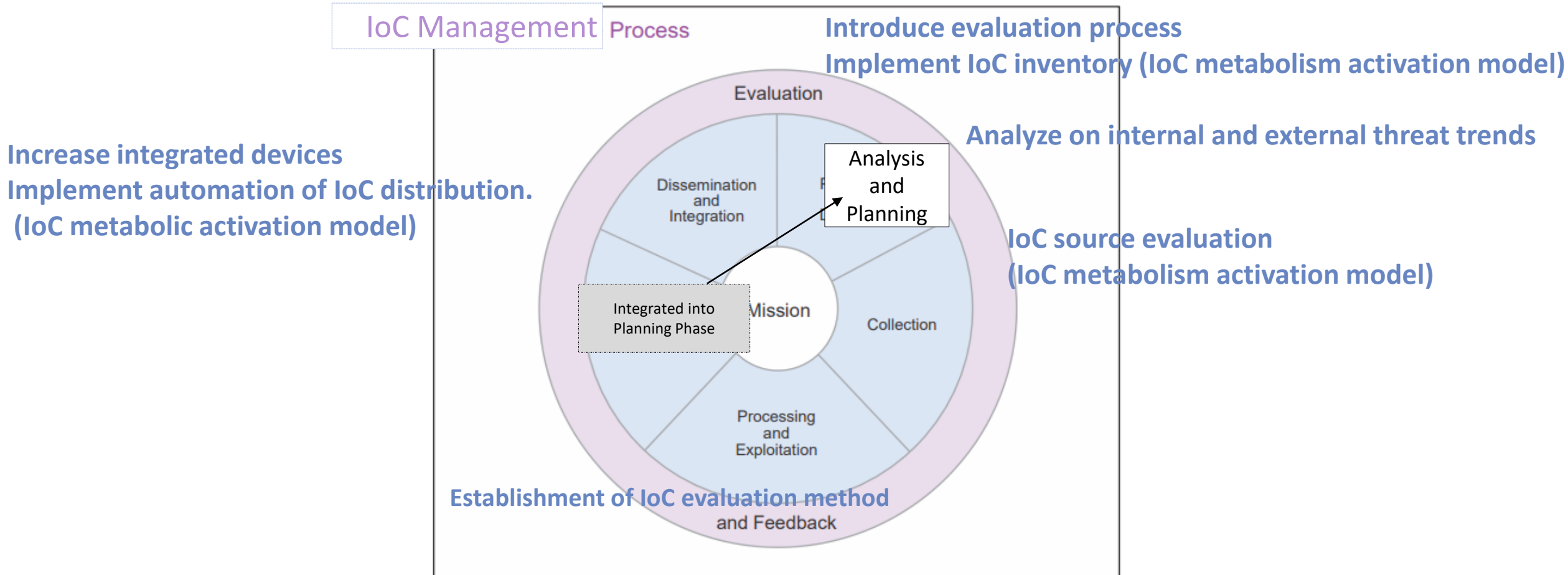
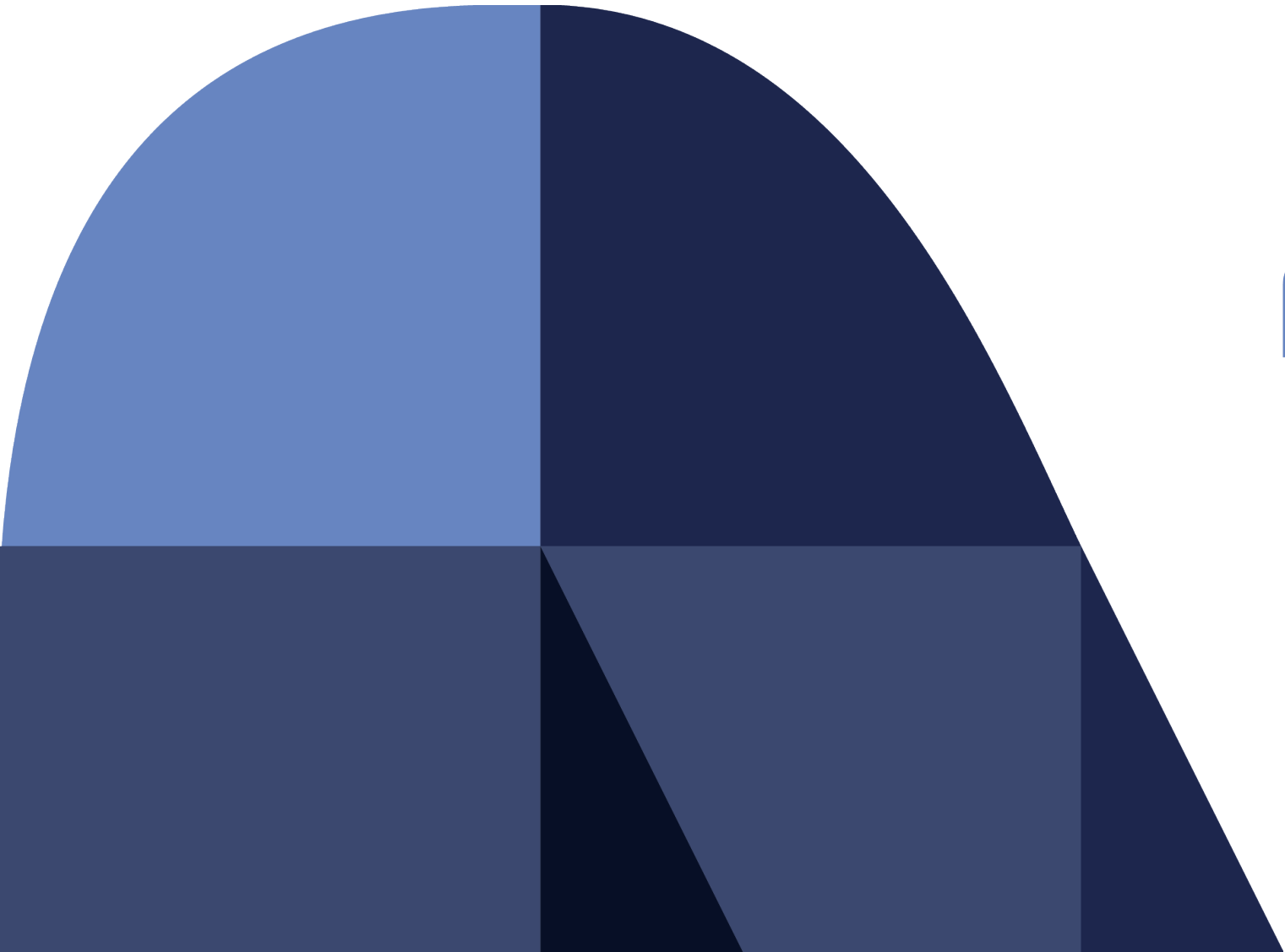


Figure I-3. The Intelligence Process



NTT DATA

Trusted Global Innovator

All other company or product names mentioned here in are trademarks or registered trademarks of their respective owners.