Back to the 'root' of Incident Response

Boston Park Plaza Hotel | June 22-27, 2014

First Step Guide for Building Cyber Threat Intelligence Team

Hitoshi ENDOH (NTT-CERT)

Natsuko INUI (CDI-CIRT)

Agenda

- About Us
  - CDI-CIRT
  - NTT-CERT
- Part 1 – Cyber Threat Intelligence Team Building Basics
- Part 2 – NTT-CERT's experience (case study)
- Part 3 – Comparison of 2 Different Teams
- Summary

Agenda

- About Us
  - CDI-CIRT
  - NTT-CERT
- Part 1 – Cyber Threat Intelligence Team Building Basics
- Part 2 – NTT-CERT's experience (case study)
- Part 3 – Comparison of 2 Different Teams
- Summary

About CDI-CIRT

- Cyber Defense Institute Cyber Incident Response Team
- Provides incident response services to clients and non-clients (private & public sector)
- Most activities are within Japan
- Cooperation with international organizations
- Intelligence, Computer Forensics, Network Forensics, Malware Analysis, Coordination and Handling (work collaboratively)

Contact us at cirt@cyberdefense.jp

For more details, please visit us below, thanks!

http://www.cirt.jp/

Who am I? What do I do?

- Natsuko Inui
- Chief Analyst @ Cyber Defense Institute
- Incident Response (Handling / Coordination)
- Cyber Exercises
- OSINT, Research
- Most work is with the Public Sector (Including Defense)

Hobbies, loves

- Ducati Monster 696
  - Aella Slip-on Silencer
- Flute
  - Started lessons again this year!
- Music (highly addicted)
  - Classical to R&B to Heavy Metal

About NTT-CERT

- NTT is the biggest telecommunication company in Japan. (946 subsidiaries, 240k employees)
- NTT Group provides a lot of public services.
- Our constituency is NTT Group.
- POC of security matters related NTT Group.

https://www.ntt-cert.org/index-en.html

Who am I? What do I do?

- Hitoshi Endoh
- Research Engineer @ NTT Secure Platform Labs.
- Cyber threat analysis
- OSINT, Research
- Community Activities（JNSA,NCA, etc.）

JNSA 特定非営利活動法人 日本ネットワークセキュリティ協会 Japan Network Security Association

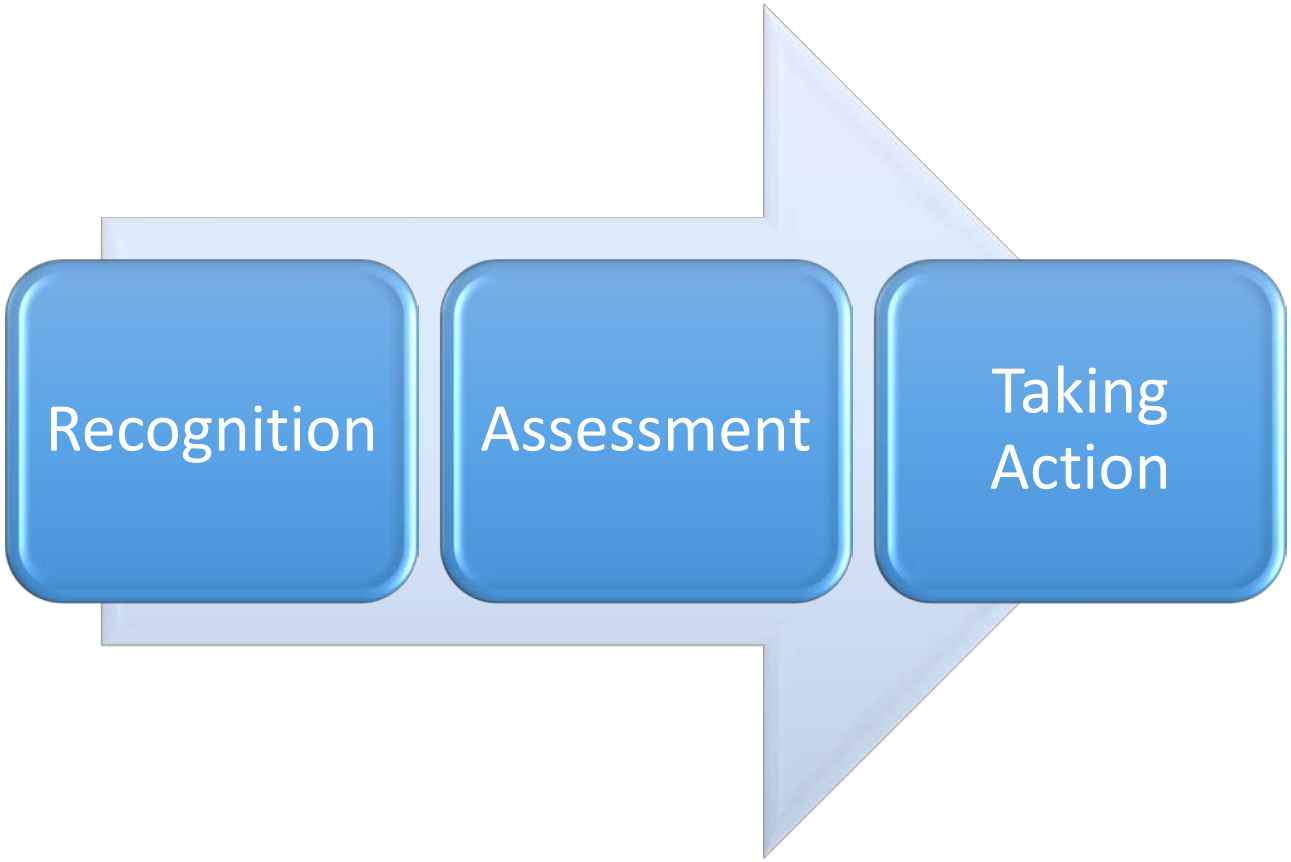
CSIRT 日本シーサート協議会 Nippon CSIRT Association

JNSA: NPO Japan Network Security Association
NCA: Nippon CSIRT Association

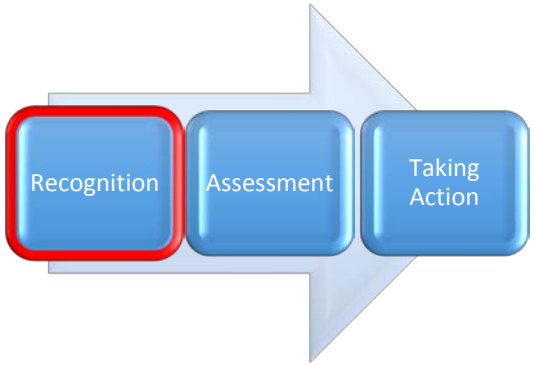
Agenda

- About Us
  - CDI-CIRT
  - NTT-CERT
- Part 1 – Cyber Threat Intelligence Team Building Basics
- Part 2 – NTT-CERT's experience (case study)
- Part 3 – Comparison of 2 Different Teams
- Summary

The 3 Steps – Back to the Basics

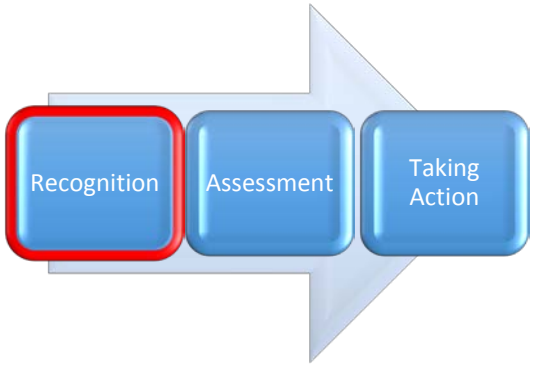


Step 1. Recognition



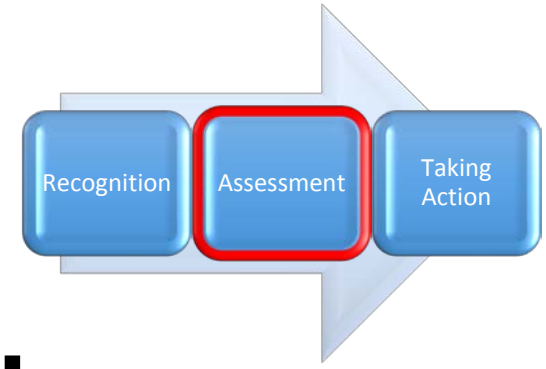
- Situational Awareness
  - “It is said that **if you know your enemies and know yourself, you will not be imperiled in a hundred battles**; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.（知彼知己,百戰不殆；不知彼而知己,一勝一負；不知彼,不知己,每戰必殆）”
    - Sun Tzu（孫氏）

Step 1. Recognition



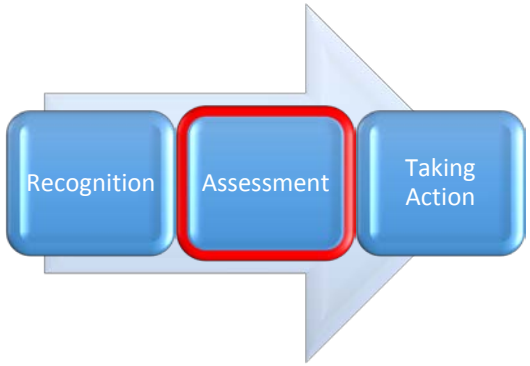
- Lesson Learned
  - No “off-the-shelf” solution
    - Think!! Don’t be lazy!!
  - Attackers “try” too
  - (Japan) Heavily reliant on outsourcing

Step 2. Assessment



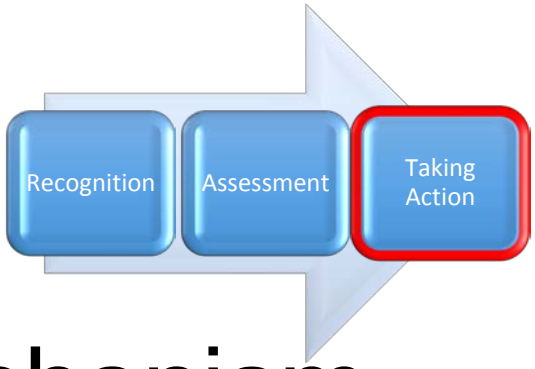
Don’t forget what you learned in the “recognition” phase

Step 2. Assessment



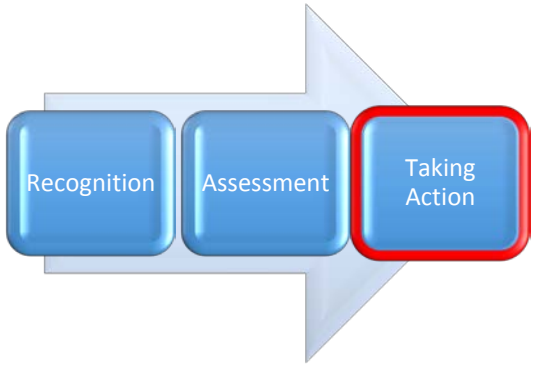
- Measure the risk(s)
  - Where should sensors be implemented?
  - Leveraging knowledge through discussions
    - **Bring all stakeholders to one table**

Step 3. Taking Action



- Building the entire mechanism
  - Framework (Procedures)
  - (Network & Computer) System
  - Human Resources
  - Operation

Step 3. Taking Action



- Lessons Learned
  - Relations among found evidence, reading patterns
  - Gathering information from FIRST members, latest blacklists, existing public reports
  - Assigning the roles of human resources

Agenda

- About Us
  - CDI-CIRT
  - NTT-CERT
- Part 1 – Cyber Threat Intelligence Team Building Basics
- Part 2 – NTT-CERT's experience (case study)
- Part 3 – Comparison of 2 Different Teams
- Summary

NTT-CERT's experience (case study)

- Introduce NTT-CERT's Activities based on CDI's 3 steps
  - Step 1. Recognition
    Step 2. Assessment
  - Step 3. Taking Action
- Sharing OSINT information
- Lessons Learned

Step 1. Recognition
Step 2. Assessment

- Proactive measures are very important. NTT Group provides national critical infrastructure of network communications.
- NTT-CERT needs Cyber Threat Intelligence Team.
- OSINT is suitable for us to collect information. Due to limitation of Japanese law, we can’t use subsidiaries’ log data.
- OSINT is very useful to share (no confidential information).

Step 3. Taking Action in 2013

Jan.	Feb.	Mar.	Apr.	May.	Jun.	Jul.	Aug.	Sep.	Oct.	Nov.	Dec.


Team building


Setting up, start daily work


Training(next slide)


Quarterly report(Apr.-Jun.)


Start sharing information


Quarterly report(Jul.-Sep.)


Conference Speaker

Training by Senior Analyst, outside the company

Benefit:

- Great skill up in the short term
- Valuable tools for collecting information and How to collect information safely
- Other useful tools and How to use them
- Methodology of making threat analysis, analyst report
- Improvement of expression ability
- Lessons Learned, Beneficial Know How

Daily Work

9:30	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00

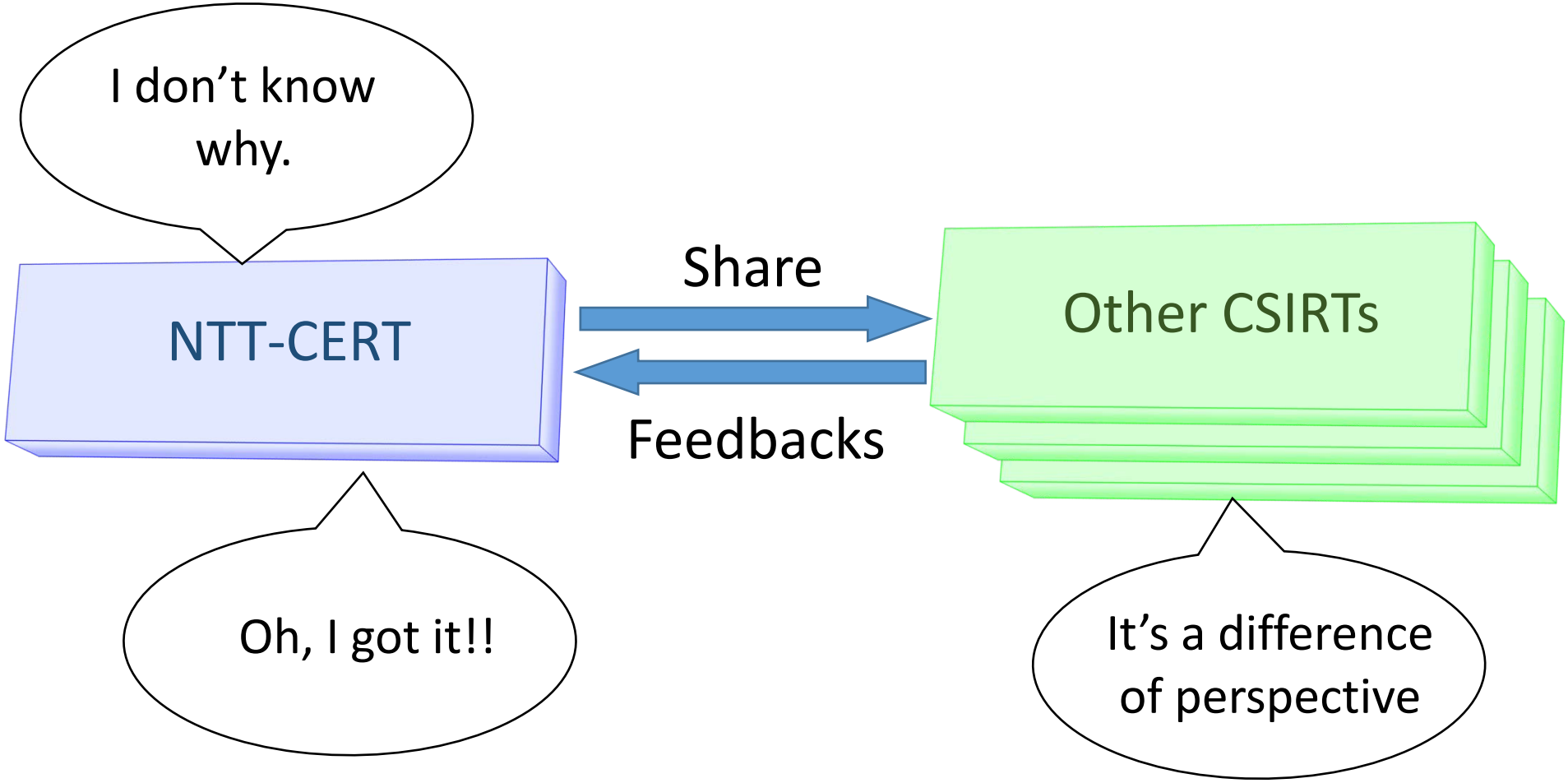

Collect articles


Read articles, Summarize


Sharing, discussion

- Detail analysis
- Tools evaluation
- Create reports
- etc.

Sharing OSINT information



L/L (1/4) OSINT Requirements

- Isolated Network from intranet
- Virtual PC and Resets every use
- Secure Browser with plug-ins
  (A lot of Japanese don’t use plug-ins)
- Research tools
  (ex. Keeping source IP secret.)

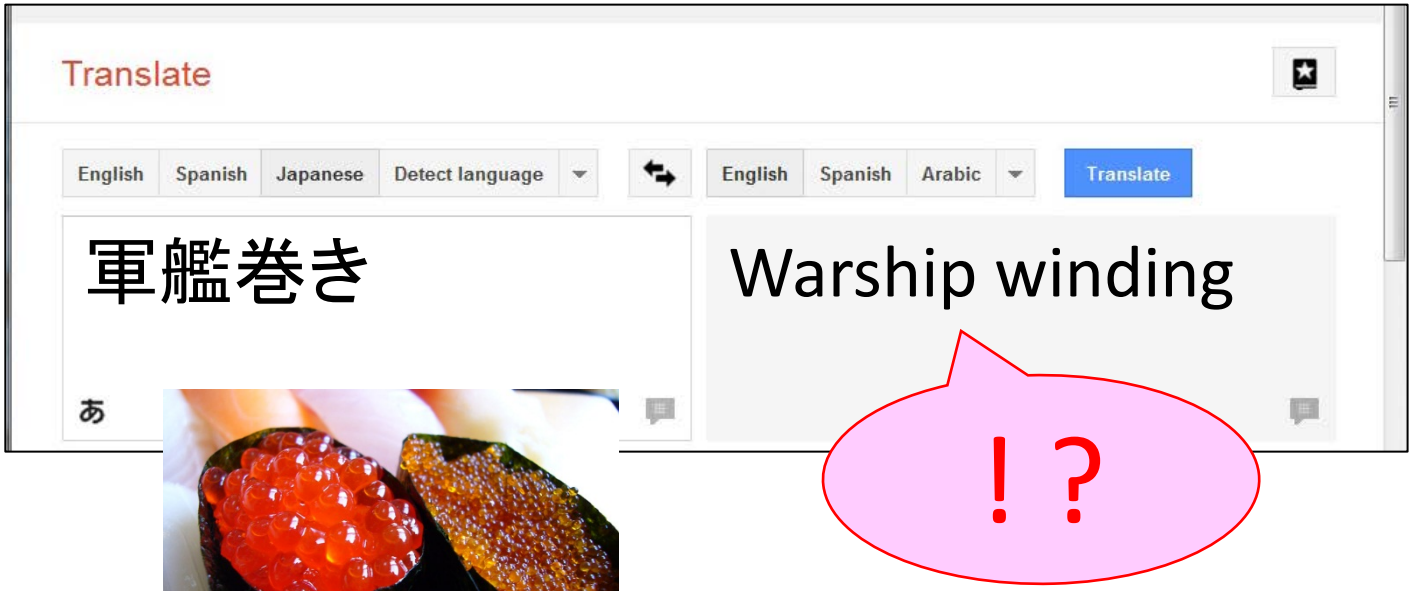
L/L (2/4) Local Languages are very important

- Most detail information from local language
- Slang (Not in Dictionary, Rapid change)

English	Cyber Attack
Japanese	サイバー攻撃
Chinese	网络攻击
Korean	사이버 공격
Russian	кибератака
Arabic	هجوم عبر الانترنت

L/L (3/4) Local languages are very important

- Machine Translation is not perfect.



“軍艦巻き” is a kind of Sushi !

L/L(4/4) Facility

- World news programs with large screen televisions
  → Notice a big news quickly
  → Get latest topics and key words

Future work

- Sharing and Collaborating widely, Extending our knowledge
- Social Media
- Useful Tools
- Multilingual
- Imaginations（ex. Media literacy）
  (There is no Media literacy curriculum in Japanese school.)

Agenda

- About Us
  - CDI-CIRT
  - NTT-CERT
- Part 1 – Cyber Threat Intelligence Team Building Basics
- Part 2 – NTT-CERT's experience (case study)
- Part 3 – Comparison of 2 Different Teams
- Summary

Comparison of 2 Different Teams

	CDI-CIRT	NTT-CERT
Category of Business	Security Service	Telecommunication
Important thing	Specialty	Teamwork
Position of the intelligence	Cutting edge	For proactive defense for NTT Group
Constituency	Client / Non Client (some exceptions, gov't and CI)	All Group Companies

Comparison of 2 Different Teams

	CDI-CIRT	NTT-CERT
Relationships with other specialists	By personal skill	By Team's activity
Situational Awareness	IR itself	OSINT Global Trends
Shortage	SOC	Fixed members

Agenda

- About Us
  - CDI-CIRT
  - NTT-CERT
- Part 1 – Cyber Threat Intelligence Team Building Basics
- Part 2 – NTT-CERT's experience (case study)
- Part 3 – Comparison of 2 Different Teams
- Summary

Summary

- No “off-the-shelf” solution for Cyber Threat Intelligence Team
  Think!! Don’t be lazy!!

- Own it. It’s yours, make it yours.

Thank you!

Special Thanks:
Mr. Kamiya Itaru
Mr. Ikuya Hayashi,
Mr. Yoshiki “Yo!” Sugiura
Mr. Masahito Yamaga,
Mr. Toshio Nawa