SDN Control System Based on Threat Level of Shared Information

June 12, 2017

Interfaculty Initiative in Information Studies Graduate School of Interdisciplinary Information Studies,

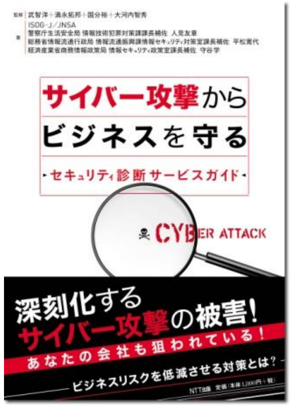
The University of Tokyo

Takuho Mitsunaga

Profile

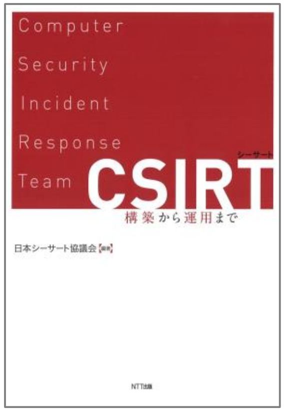
東京大学 情報学環
SiSOC TOKYO

- Name: Takuho Mitsunaga
- Position/Affiliation: Project Associate Professor, Secure Information Society Research Group, the University of Tokyo
- Job description:
  ・Analysis and publication on cyber security
  ・Collaboration with, top management and system administrative divisions.
  ・Presentations and lectures in seminars/universities etc.
  ・Writing papers and reports about analysis of security


サイバー攻撃から
ビジネスを守る
・セキュリティ診断サービスガイド・
CYBER ATTACK
深刻化する
サイバー攻撃の被害!
あなたの会社も狙われている!
ビジネスリスクを低減させる対策とは?

「Protect your business from cyber attacks」
Co-auther/ Supervising editor

「Information Security White Paper 2013」
Co-auther



「CSIRT」
Co-auther

About Secure Information Society Research Group, the University of Tokyo

- SISOC-TOKYO researches on Internet security through collaboration with industry, academia and government.
  - SISOC-TOKYO gathers human resources through collaboration among industries, academia and government to research on social and international issues and widely reports on the analysis results.
  - SISOC-TOKYO promotes interdisciplinary research, human resource education and policy recommendation against issues on cyber space and security from a macro and long-term perspective.

Agenda

- Background
  - Information Sharing Scheme and its Challenges
- Challenges
- Solution
- Demonstration
- Conclusion

Background

Background

- Cyber attacks becoming more sophisticated – complete protection from intrusion is difficult
- Early detection = minimum damage
  →Sharing threat information is a key

- Threat information sharing in Japan
  Security Early Warning Service (JPCERT/CC)
  J-CSIP (IPA)
  C4TAP (NISC)
  Counter Cyber Intelligence (National Police Agency)

- Indicators helps detecting attacks effectively and identifying affected areas in the network

Issues around Threat Info Sharing

- Currently, mostly done manually

- Senders:
  1. Takes time to prepare information to share

- Recipients:
  2. Hard to examine large amount of information
  3. Triage is complicated and needs a set of skill
     ・Threat level (Targeted attacks or large-scale malspam)

Security personnel need to check every piece of indicator information to judge if there is a need to block communication to the hosts

Challenge 1: Info Sharing

- Mostly done in text format
- Needs manual processing

Example 1

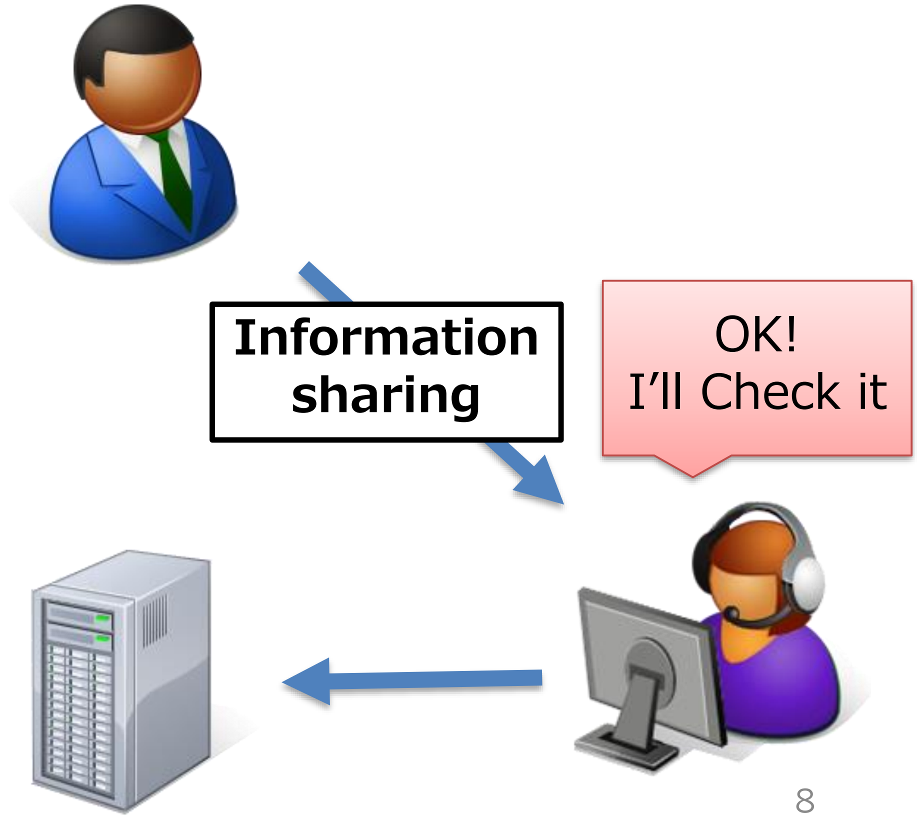
Malware’s C&C server

- Duration
- IP address (Outbound)
- Characteristics in communication
- Action (Detect, Block in Proxy log)

Example 2

Source of DDoS attack

- Duration
- IP address (Inbound)
- Characteristics in communication
- Action(Detect, Block in Apache log)

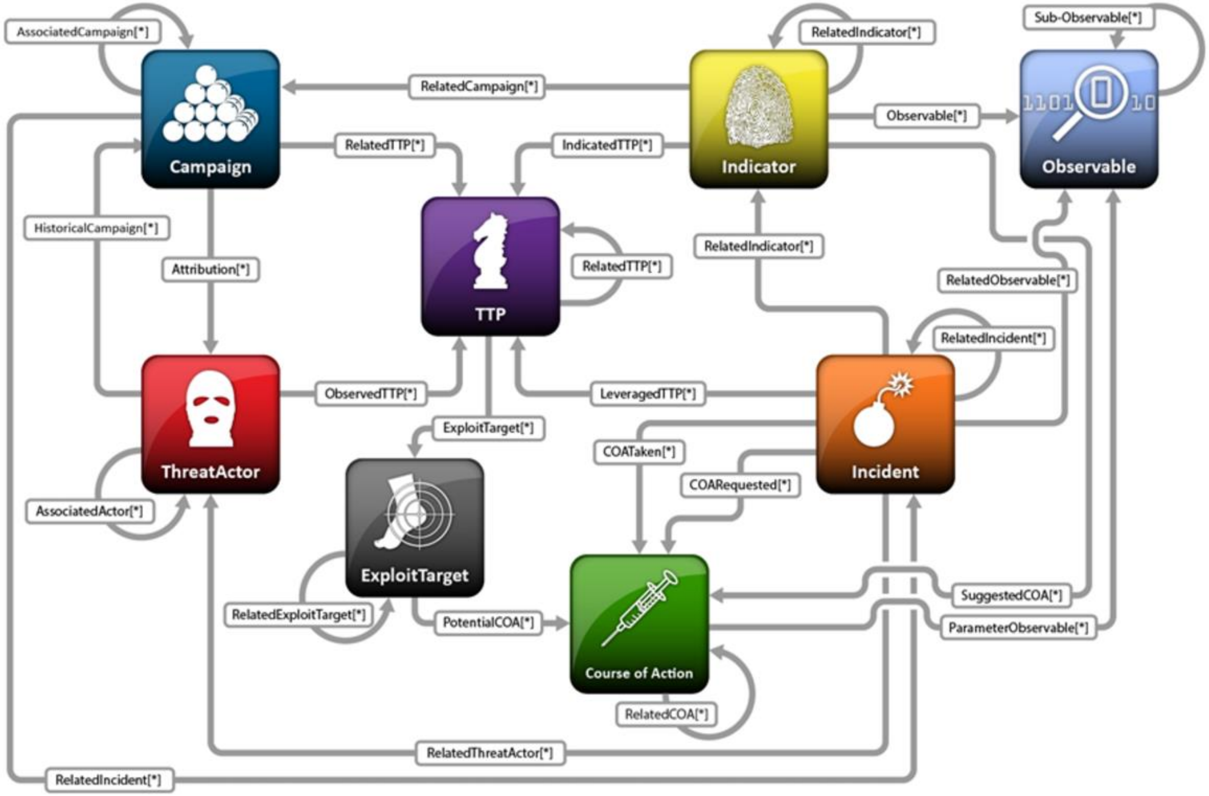


Information sharing

OK!
I’ll Check it

STIX

- “The Structured Threat Information eXpression (STIX™) is a quickly evolving, collaborative community-driven effort to define and develop a language to represent structured threat information”
(from http://stixproject.github.io/getting-started/whitepaper)

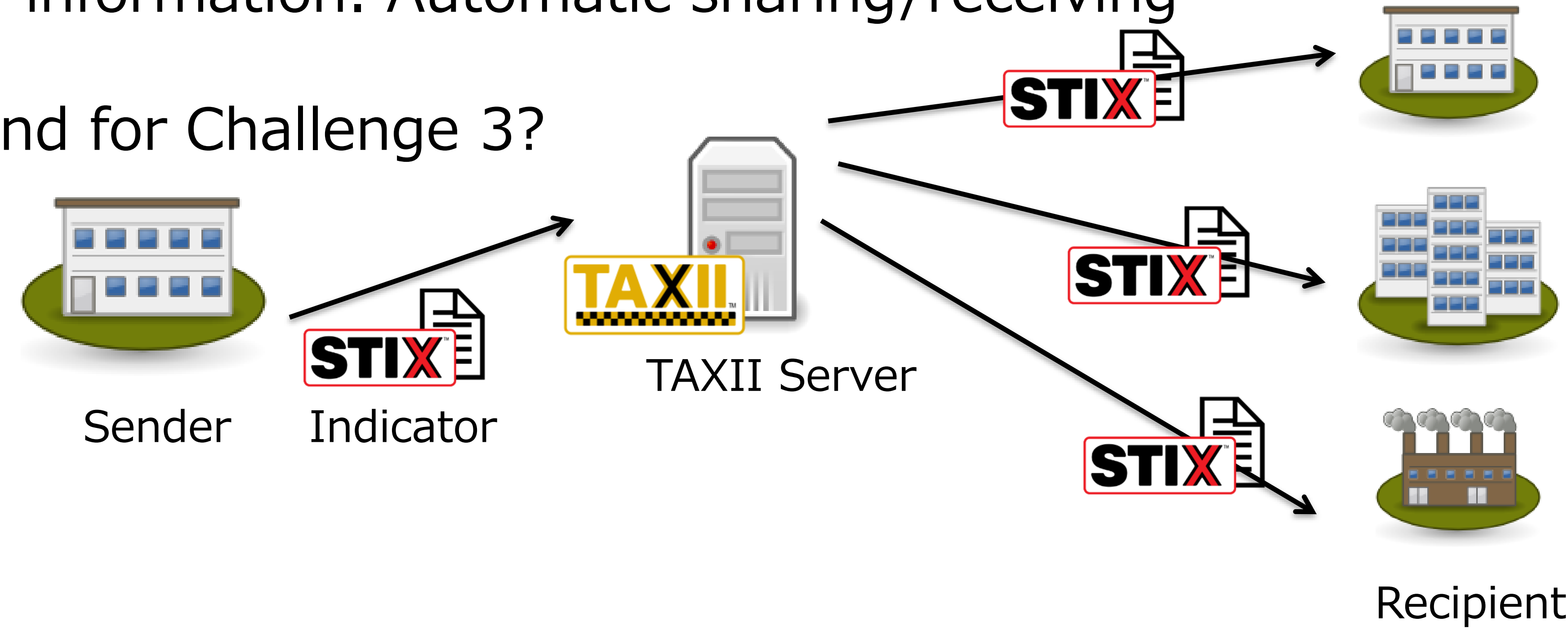


Solution

Measure for Challenge 1 & 2: Follow the standardized scheme

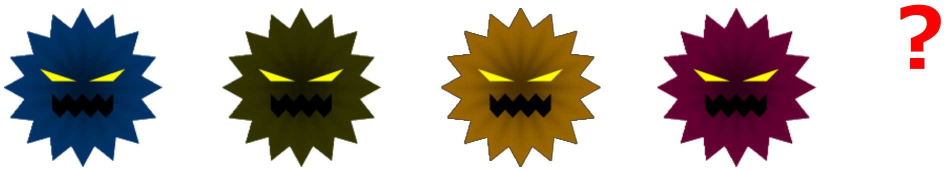
- STIX: Standardized format for describing threat information. Helps common understanding and machine process
- TAXII: Standardized protocol for exchanging threat information. Automatic sharing/receiving

And for Challenge 3?



Solution

- Measure for Challenge 3: Automatically judge threat level and provide counter action
- What type of attacks are considered “severer”?
  - Adware
  - Ransomware
  - Banking Trojan
  - Malware by APT attackers



Unfortunate case in Japan

- 1.2 Million PII leakage
  - The victim organization detected the malware infection and asked the AV vendors about the malware, then they answered,

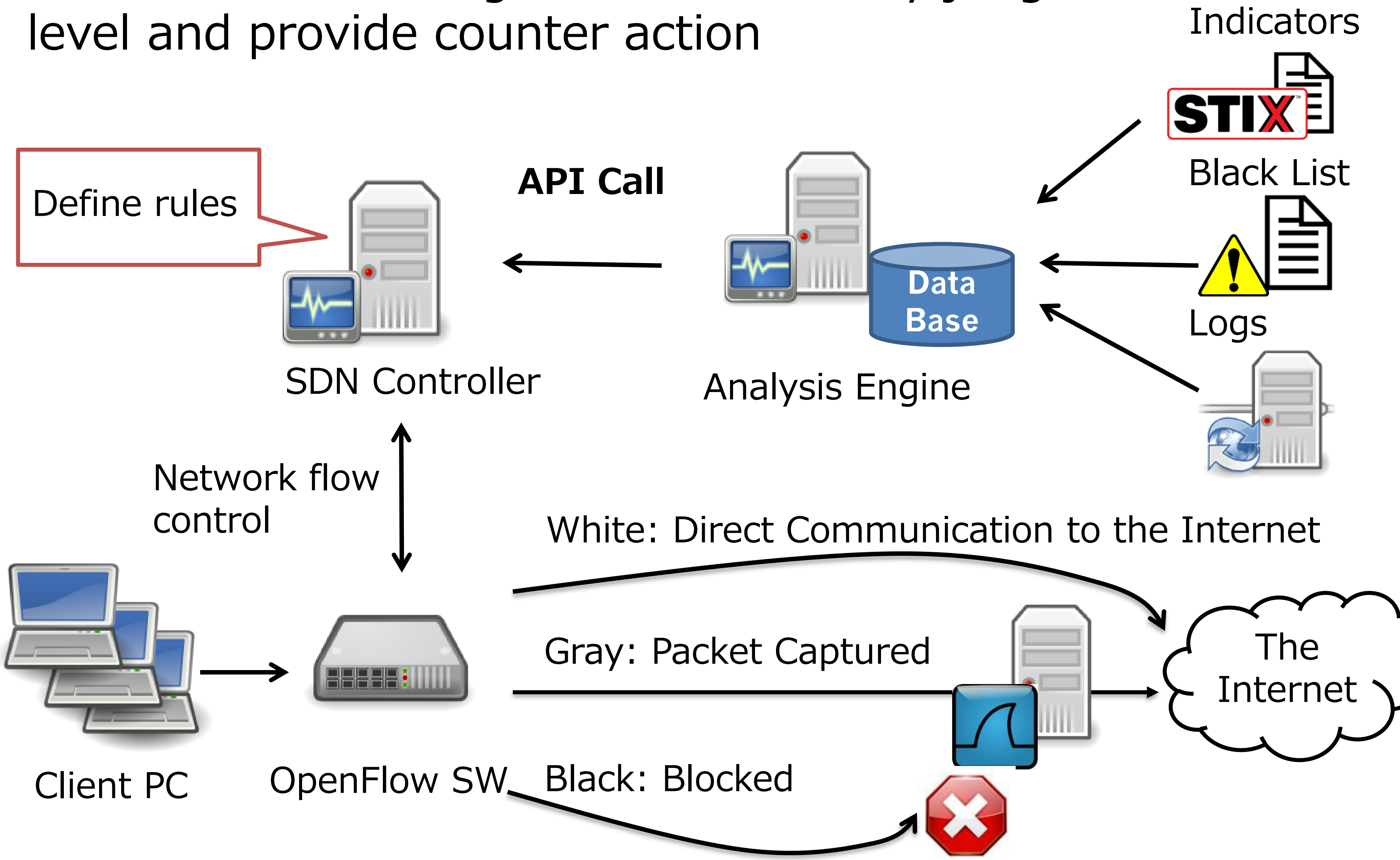
“The malware does not the type of malware to exfiltrate information”

… and the response was delayed.

Importance of Triage
For incident response with limited resources,
defining “priority” based on the threat level is important

Solution

Measure for Challenge 3: Automatically judge threat level and provide counter action



Indicators

STIX

Black List

Logs

Define rules

API Call

Data Base

SDN Controller

Analysis Engine

Network flow control

White: Direct Communication to the Internet

Gray: Packet Captured

Black: Blocked

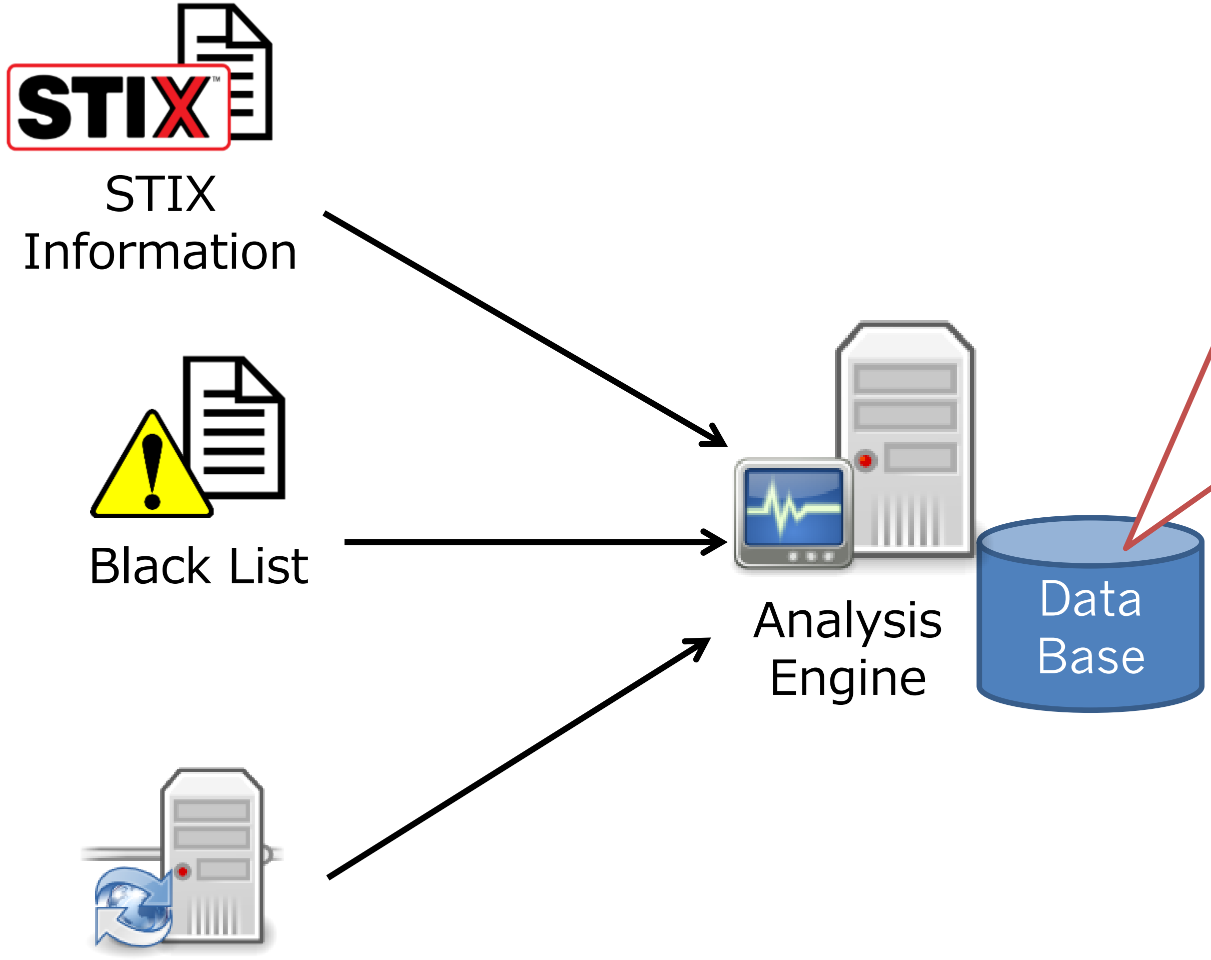
Client PC

OpenFlow SW

The Internet

Solution

Step 1: Create database and visualize indicator information



Indicator

- Date
- IP address
- Domain
- File name / Path
- Registry…

Demonstration

Solution

Step2: Analyze threat level

1. Pattern matching
2. OSINT (ex. Register name)
3. Similarity

Step2: Analyze threat level

1. Pattern matching

- **Black Lists/Indicators**

Data name	Attribute	Date	Type	Indicator
Malware A	APT	2017/4/1	Domain	example.com
DDoS A	Ransom	2017/4/28	IP	172.xx.xx.xx
DDoS B	Hactivist	2017/6/1	IP	172.xx.xx.xx
Malware B	Ransom	2017/6/28	File	system32¥bad.exe

- **Logs**

Data name	Date	Type	Indicator
Proxy log	2017/x/x	Domain	example.com
Proxy log	2017/x/xx	Domain	safe.example.jp

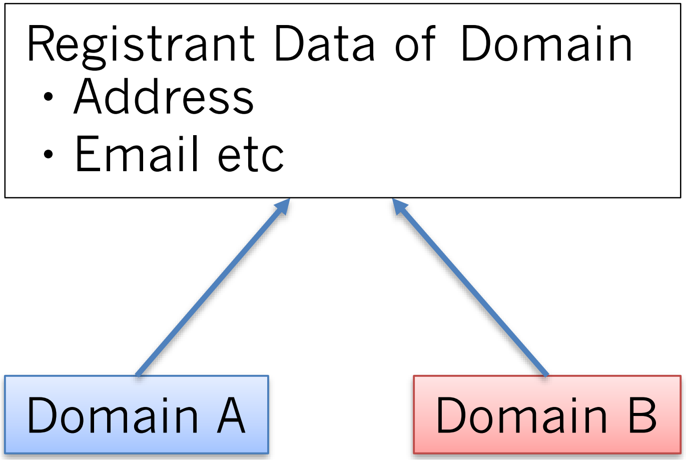
Data name	Date	Type	Indicator
Local Data	2017/x/x	File	system32¥bad.exe
Local Data	2017/x/xx	File	system32¥safe.exe

Step2: Analyze threat level

2. OSINT (ex. Registrant name)

Domain correlation:

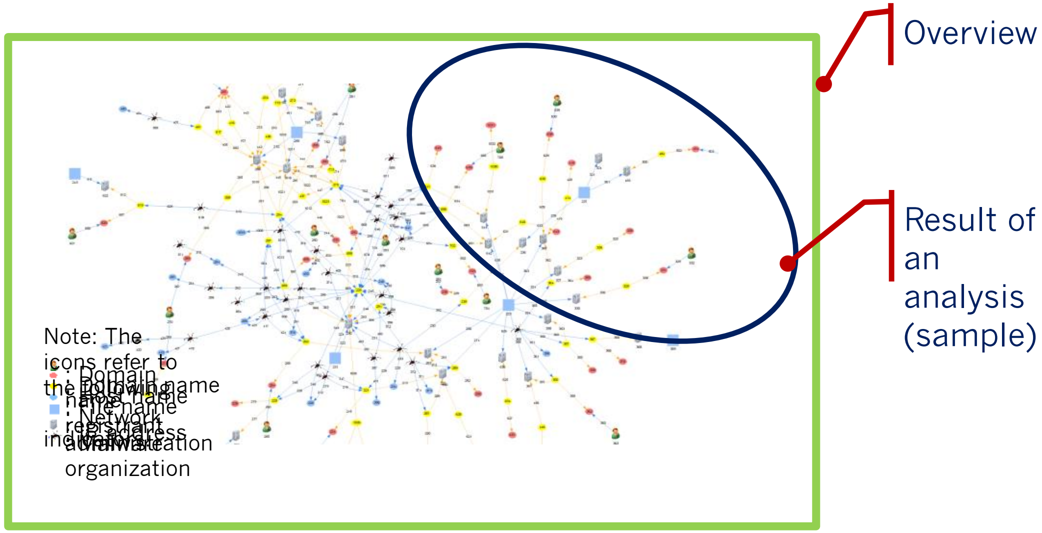
If the domain registrant is identical to other malicious hosts, it is considered that there is a correlation



Registrant Data of Domain
・Address
・Email etc

Domain A

Domain B



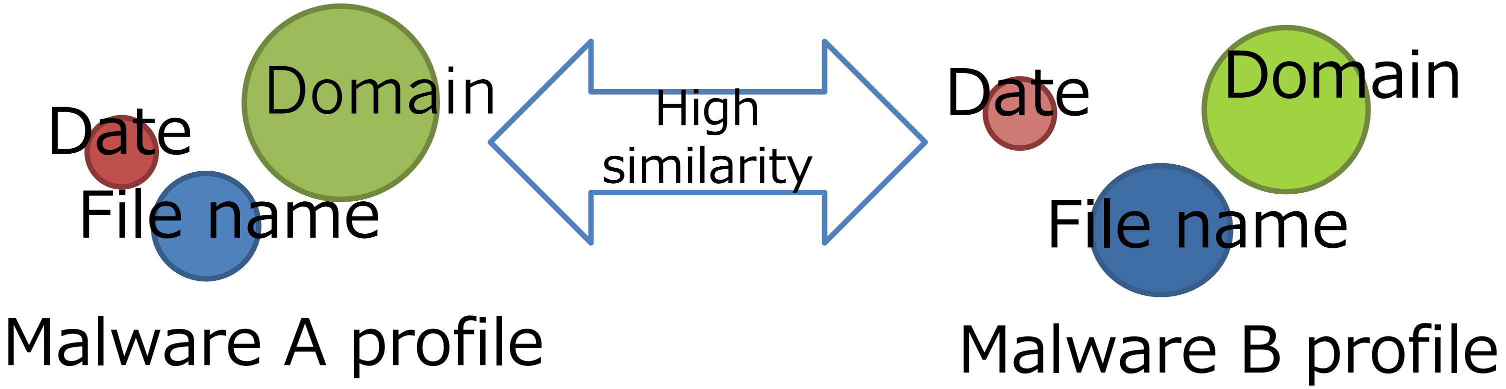
JPCERT/CC Cases:
Emdivi and the Rise of Targeted Attacks in Japan
http://blog.jpcert.or.jp/2015/11/emdivi-and-the-rise-of-targeted-attacks-in-japan.html

Solution

Step2: Analyze threat level

3. Similarity

Malware name	Family	Date	Domain	Generated file
MalwareA	FamilyA	2017/4/1	example.com	system32¥evil.exe
MalwareB	FamilyB	2017/4/28	example.org	system32¥bad.exe



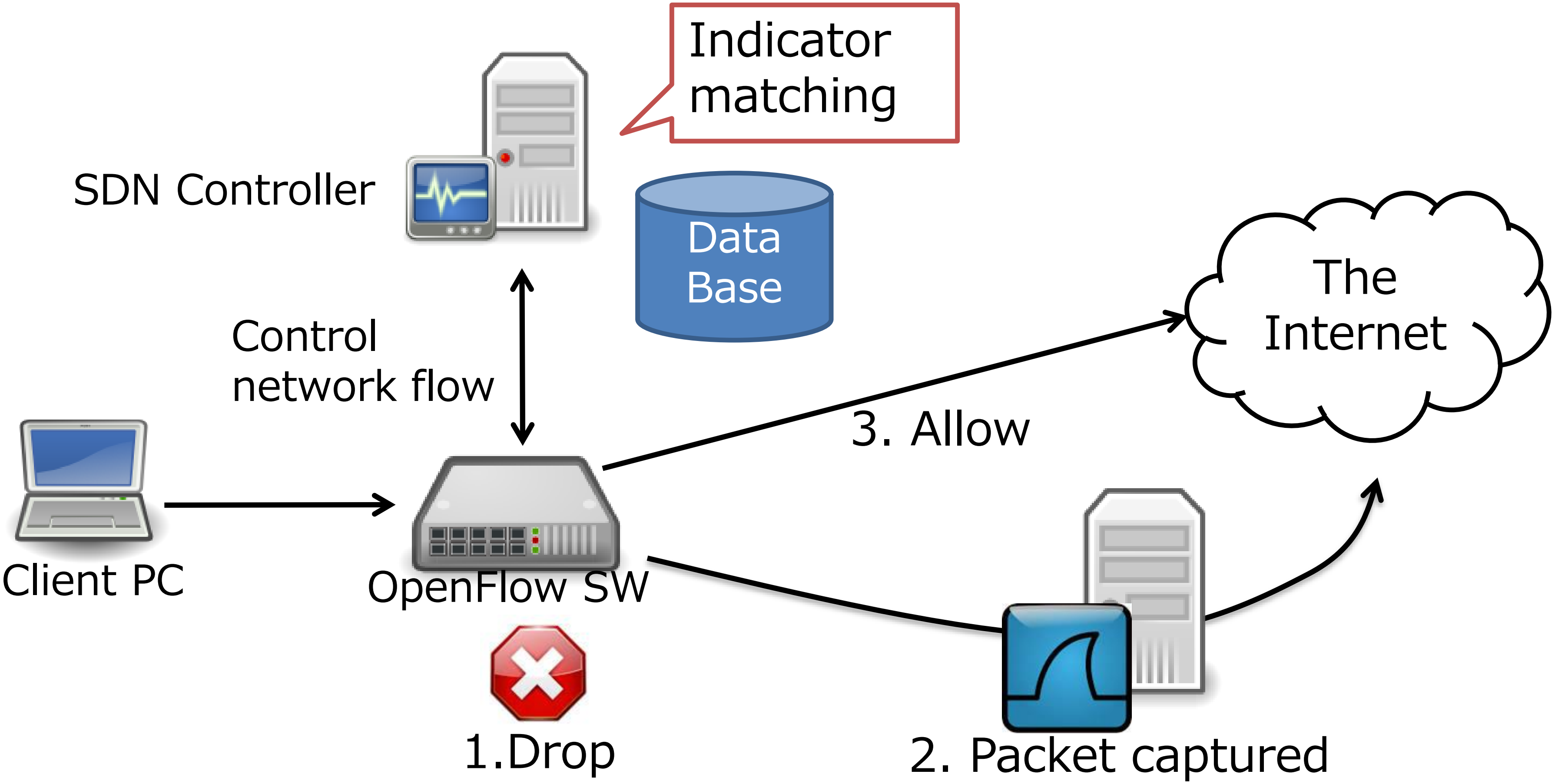
Malware A profile

Malware B profile

Step3:Control network flow based on threat level

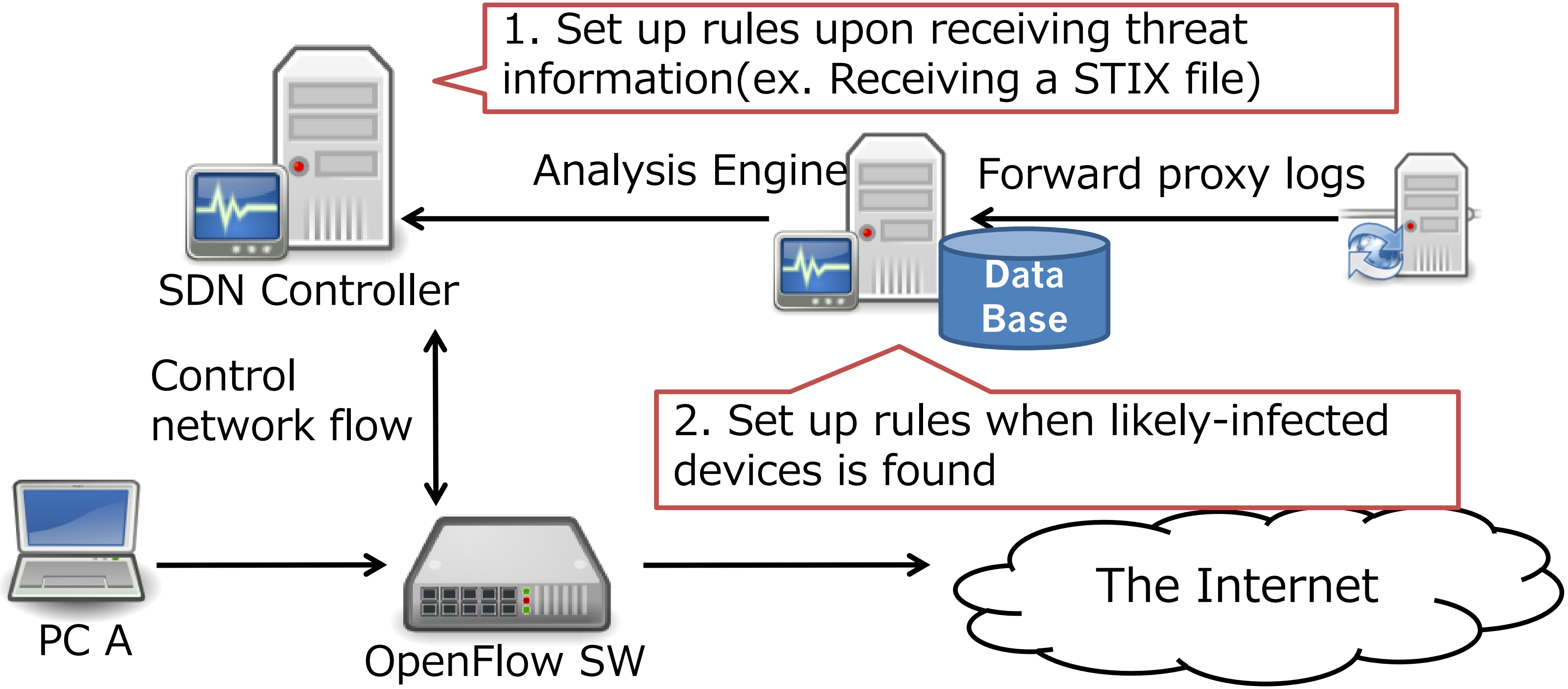
Severity

1. Black: Blocked immediately
2. Gray: Packet captured
3. White: Communication allowed



Challenges in the solution 1

Timing for implementing the defined rules



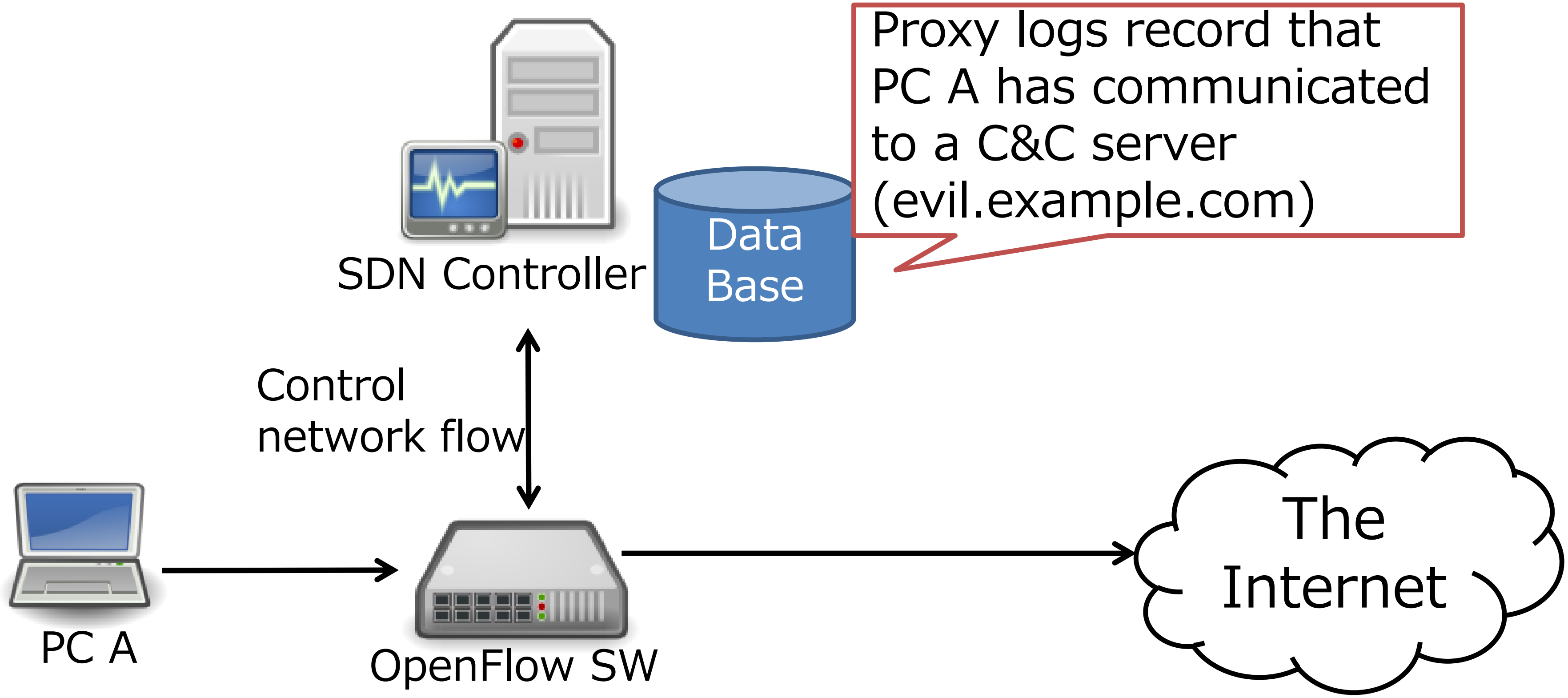
1. Set up rules upon receiving threat information(ex. Receiving a STIX file)

2. Set up rules when likely-infected devices is found

Rule	Advantage	Disadvantage
1	Less load on SDN controller	Increases rules on SDN controller IP addresses may not be up to date
2	Less rules on SDN controller Actual IP addresses are listed	Much load on SDN controller

Challenges in the solution 2

Areas where the rules are applied

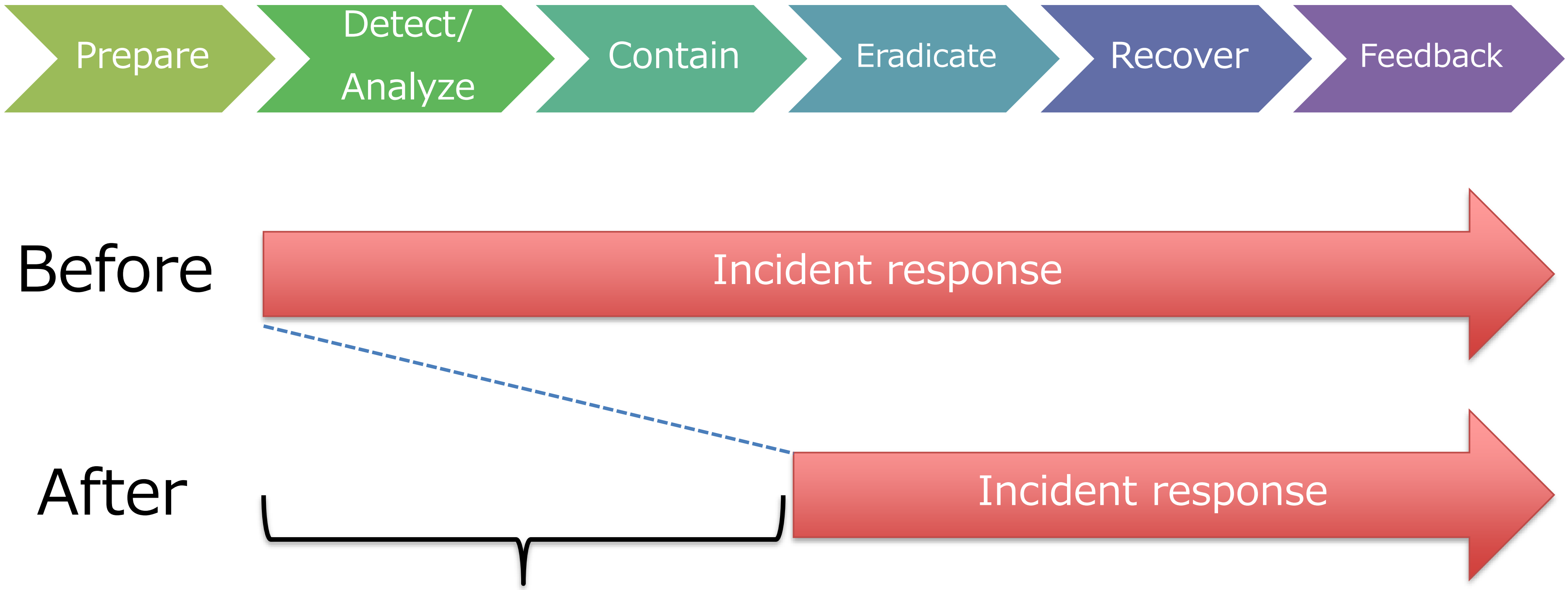


Proxy logs record that PC A has communicated to a C&C server (evil.example.com)

From	To	Access
Any	evli.example.com	Drop
PC A	Any	Drop

Likely-infected devices should not be allowed to communicate to any hosts?

Incident response flow



Reduce time by automated information sharing
and communication control

Conclusion

- Information sharing is effective in dealing with cyber attacks – however, certain skills required both for senders and recipients
- Automated threat information sharing schemes are available (STIX/TAXII)
- By combining them with SDN, automatic triage of threat information and blocking of communication is possible
- Needs further consideration on when and how far the rules are implemented