Real-time Log Analysis Tool with STIX 2.0

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

The University of Tokyo

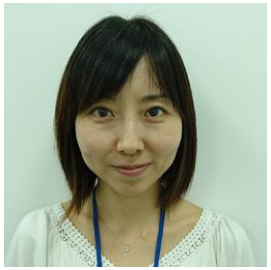
Wataru Matsuda, Mariko Fujimoto, Takuho Mitsunaga

Profile

Wataru Matsuda, Mariko Fujimoto, Takuho Mitsunaga

- Project researcher, Secure Information Society Research Group, the University of Tokyo (SiSOC)
- Job description:
  - Analysis and publication on cyber security
  - Education for human resources for cyber security
  - Presentations and lectures in seminars/universities etc.
- Publication/Works :
  - CSIRT – from building to running – (coauthor)
  - Tracking mimikatz by Sysmon and Elasticsearch

https://hitcon.org/2017/CMT/slide-files/d2_s1_r1.pdf


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
- Challenges
- Solution
- Demonstration
- Conclusion

BACKGROUND

Background

- Cyber attacks become more sophisticated
- To detect cyber attacks, shared indicators such as C&C server **domain** and **IP address** can be useful
- Information sharing scheme has been developed globally, and indicator formats such as STIX are standardized during the past years
- As indicator exchange increases, however, there are new challenges to handle indicators, comparing **increasing number of shared indicators** against **a large amount of logs**
- In this presentation, we will present how our tool works for effective detection to take advantage of STIX

Indicator

- Indicators are information indicating the features of attacks
  - Host name, IP address and URL of C2 servers, etc.

Example 1

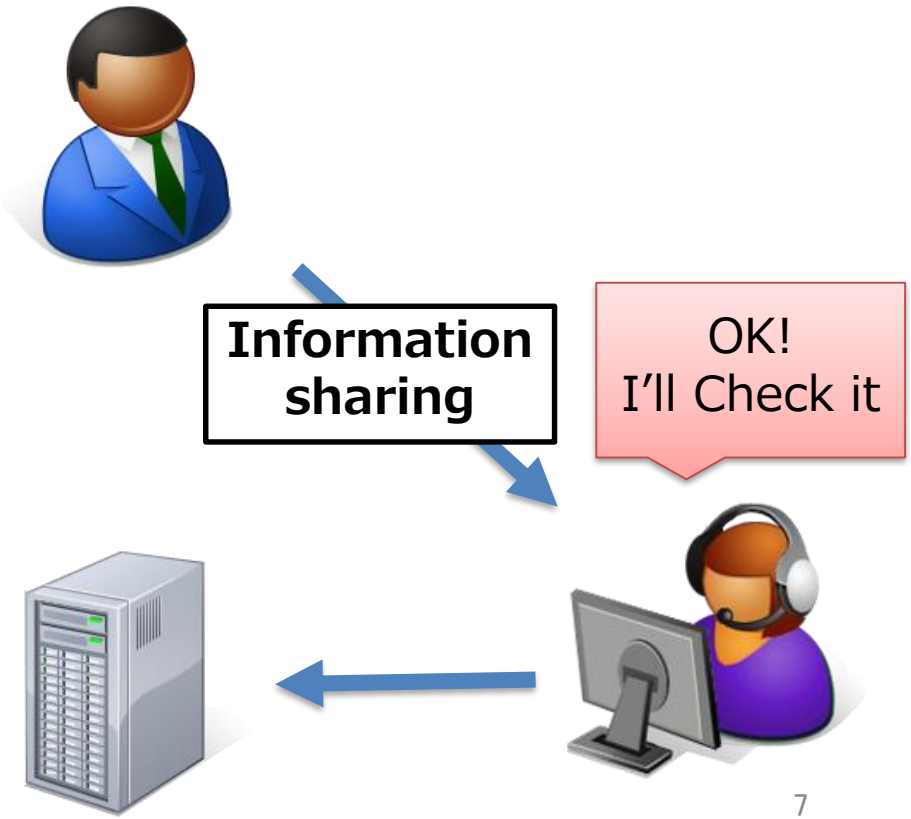
Malware's C&C server

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

Example 2

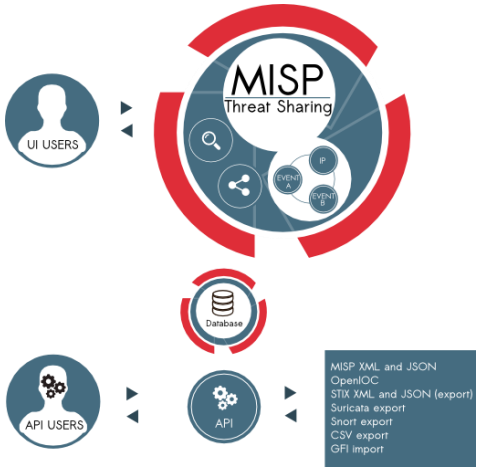
Source of DDoS attack

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

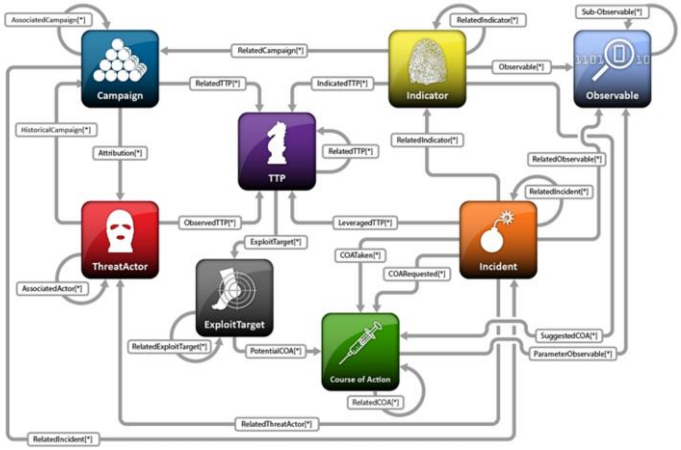


Trends of information sharing

- Information sharing schemes have been developed globally in recent years
  - DHS has been operating AIS (Automated Indicator Sharing) since 2016
  - CIRCL (The Computer Incident Response Center Luxembourg) shares malware information through MISP
- STIX(The Structured Threat Information eXpression) was introduced by MITRE



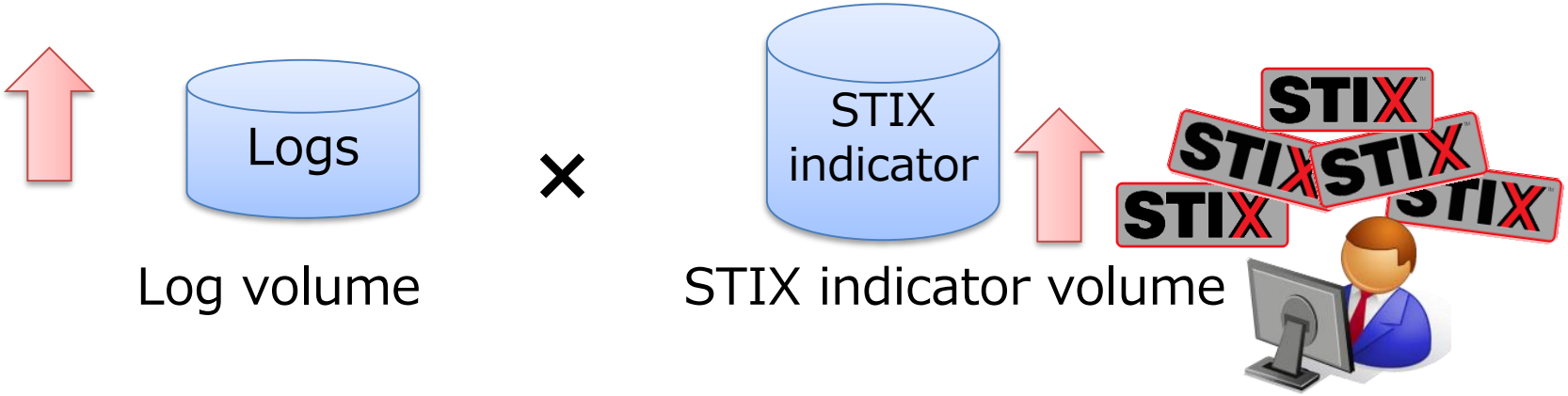
(from https://www.circl.lu)



(from http://stixproject.github.io/getting-started/whitepaper)

Challenges

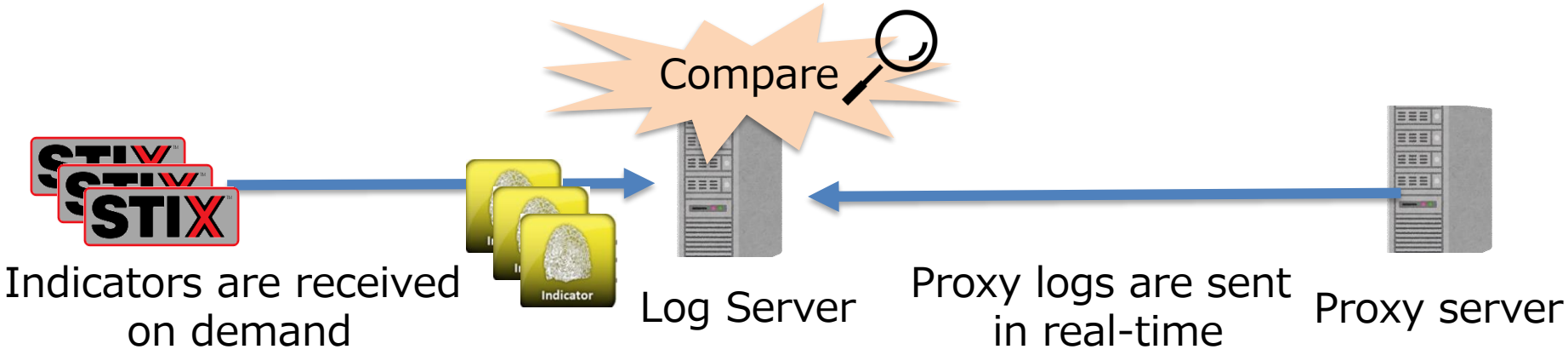
- STIX is becoming more popular, and shared information is increasing through the STIX format
- We need to compare a large amount of logs with a number of STIX indicators
- We need appropriate tools which can extract indicators from STIX and compare with the logs



CHALLENGES

Challenges of the detection trigger

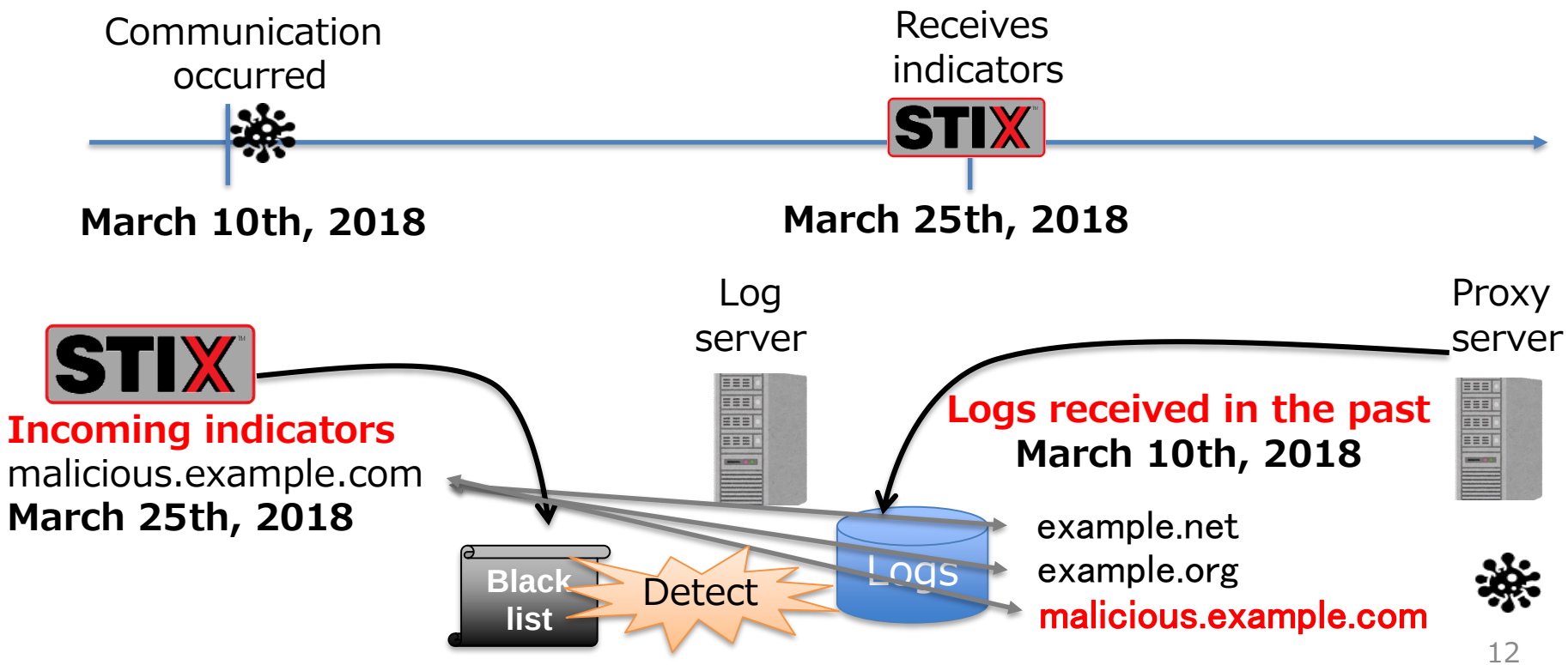
- There are challenges in automated detection
  - It is important to detect attacks immediately, also we have to detect potential infected computers
  - There is a time lag between the observation of an attack and the release of the indicator
- We need to compare indicators with logs **in a timely manner**



Challenges of the detection trigger

Detection trigger 1: when we receive indicators

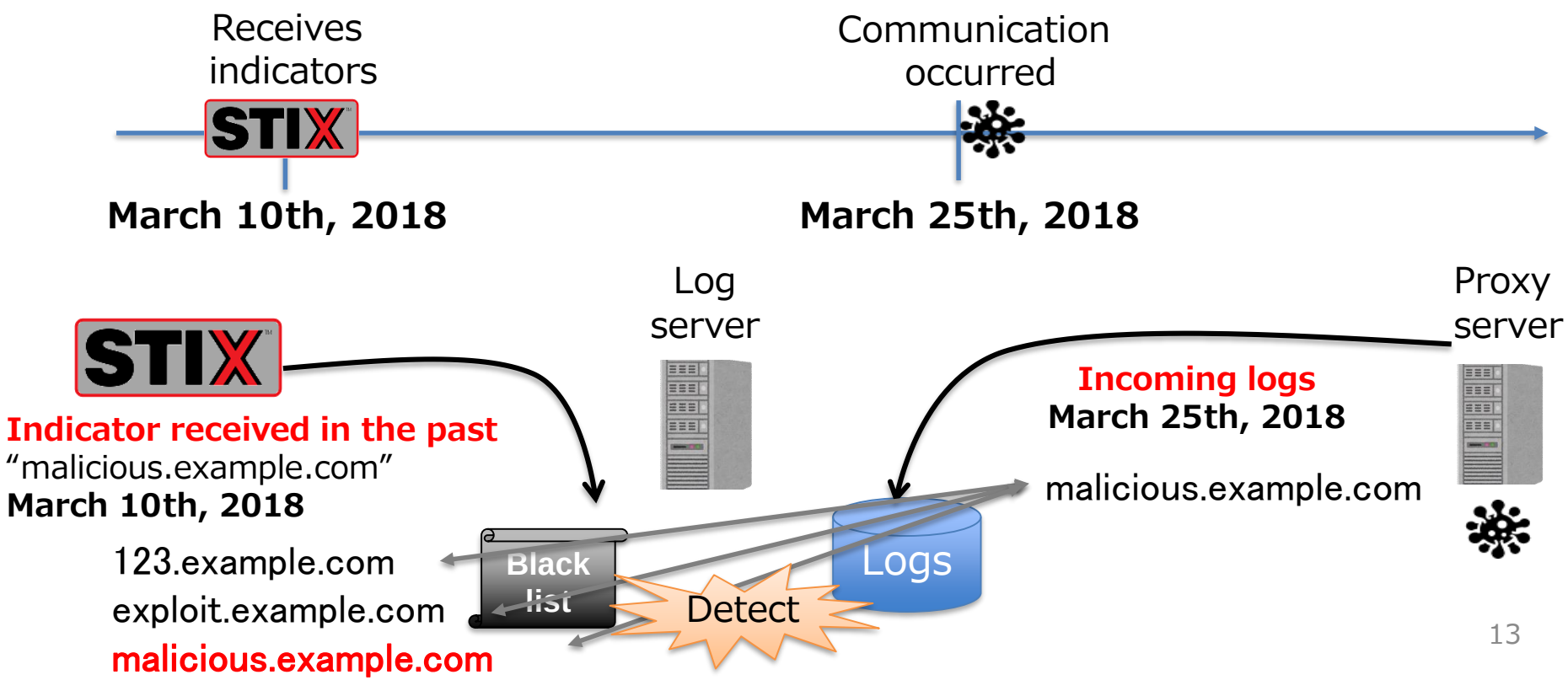
- When we receive STIX indicators, we have to compare them with past logs to find potential infected computers
- Many organizations may adopt this detection approach



Challenges of the detection trigger

Detection trigger 2: when communications to the Internet are performed

- When communications to the Internet are performed, we have to compare them with all indicators to detect attacks immediately



Considerations for blocking domains

The reason why we focus on **Detecting** malicious domains rather than **Blocking** them by Firewall or URL filtering:

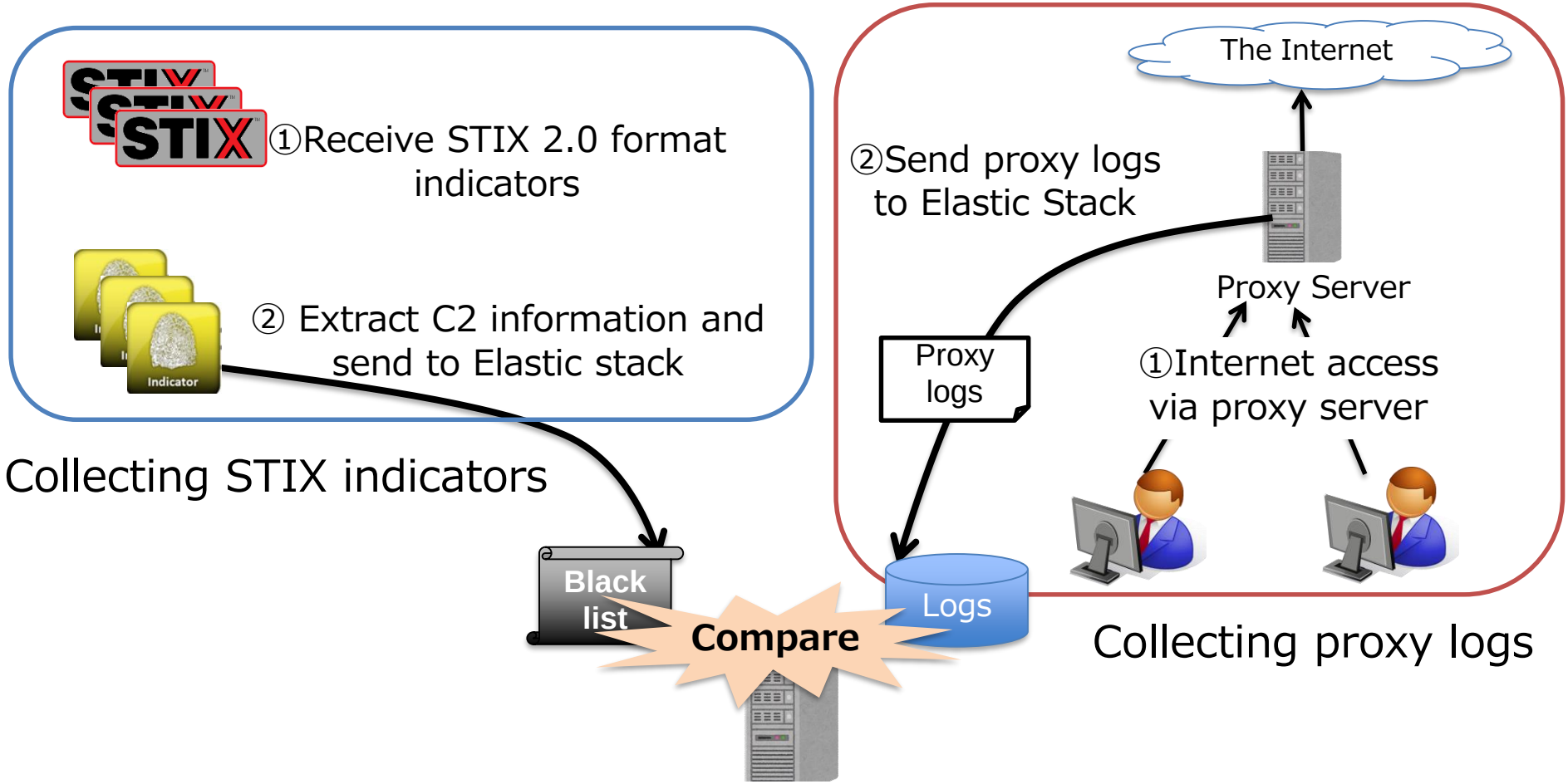
- We should consider the valid period of the C2 server
  - Some indicators have the information of the valid period
  - Sometimes legitimate websites are used as C2 servers (Keep blocking the domains are difficult when they are used in business operations)
- We should consider the reliability of indicators
- There are maximum number of URLs in filtering functions

Blocking specific domains for a long period is difficult.

SOLUTION

Summary of the proposed method

- We propose a method which compares logs with STIX 2.0 indicators automatically using Elastic Stack



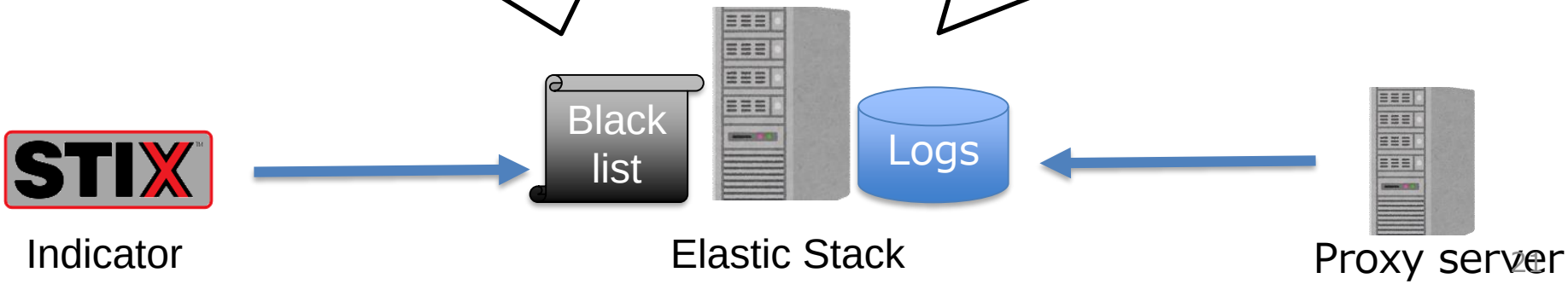
Elastic Stack(Elasticsearch, Logstash, Kibana, Filebeat)

Summary of the proposed method

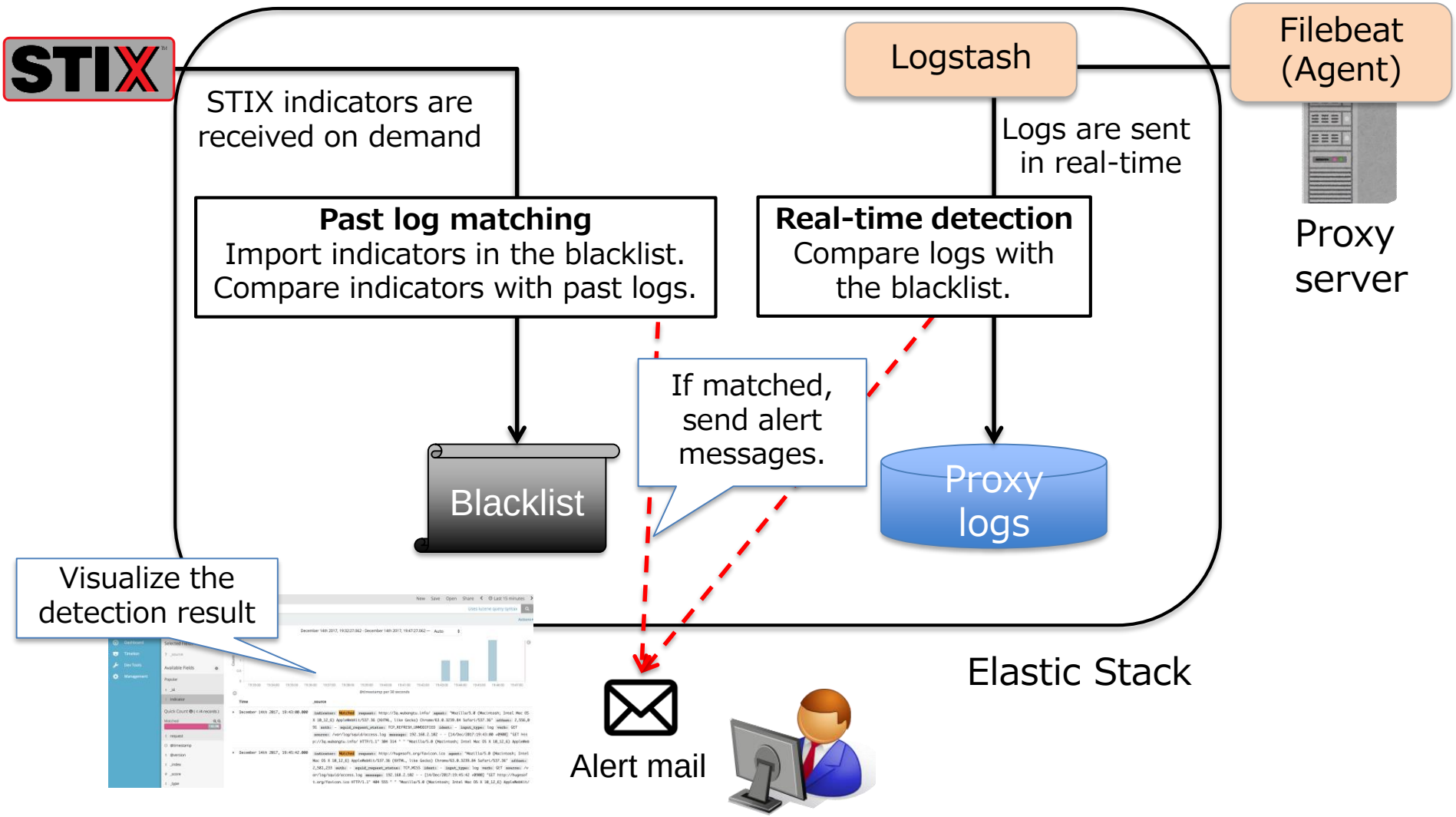
- Our method solves issues mentioned in previous slides
  (1)Effective log analysis and automated detection using Elastic Stack
  (2)Compare indicators with logs in a timely manner

Past log detection
When STIX indicators are imported into Elastic Stack, the tool compares indicators with past logs.

Real-time detection
When proxy logs are transferred into Elastic Stack, the tool compares proxy logs with indicators in the blacklist.



Structure of the proposed method



← Flow of detection

← - - Flow when a log matches the blacklist

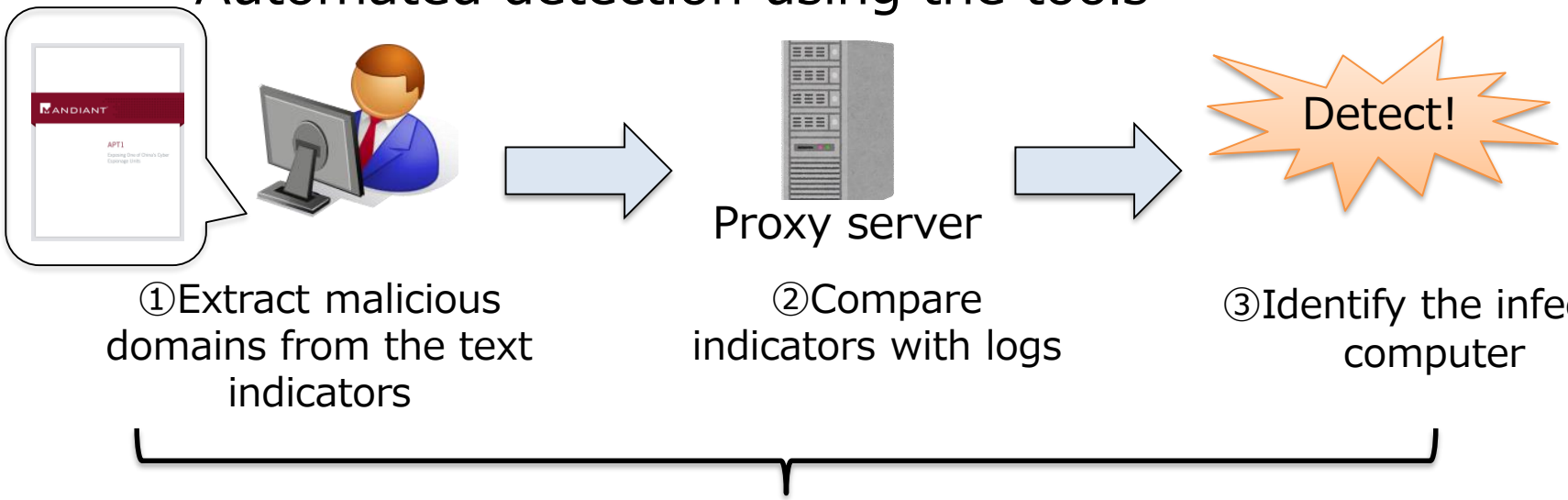
Time saving by using the system

Incident response flow

The system uses automated detection to reduce the incident response time.

Time saving by using the system

- Compare total amount of time needed to identify the compromised computer
  - Manual operation
    - Extract malicious domains from the text format indicators
    - Search malicious domains from proxy logs using “grep” command
  - Automated detection using the tools



The tool utilizes automated detection process.

Time saving by using the system

The incident response time has been successfully reduced by 84% using the system.

Manual operation

Operations	The time required
Extract indicators from APT1 report	About 3.5 minutes
Search indicators from proxy logs	About 6 minutes
Total	About 9.5 minutes

Automated detection using the tools

Operations	The time required
Launch the detection tool	About 1.5 minutes

DEMONSTRATION

Demonstration

東京大学 情報学環

SiSOC TOKYO

stix2.0_ELK 〉 apt1.json 〉

input_report

Project

stix2.0_ELK ~/PycharmProjects/stix2.0_ELK

- old
- apt1.json
- filebeat.yml.squid
- imddos.json
- input_report.py
- logstash.conf
- poisonivy.json
- poll_create_file.py
- search_blacklist.py
- send_alert.py
- taxiidata.json

External Libraries

search_blacklist.py | send_alert.py | logstash.conf | input_report.py | apt1.json

```
303        "valid_from": "2015-05-15T09:00:00.000Z",
304        "kill_chain_phases": [
305          {
306            "kill_chain_name": "mandiant-attack-lifecycle-model",
307            "phase_name": "establish-foothold"
308          }
309        ]
310      },
311      {
312        "type": "indicator",
313        "id": "indicator--3f3ff9f1-bb4e-4392-89e5-1991179042ba",
314        "created": "2015-05-15T09:00:00.000Z",
315        "modified": "2015-05-15T09:00:00.000Z",
316        "object_marking_refs": [
317          "marking-definition--3444e29e-2aa6-46f7-a01c-1c174820fa67"
318        ],
319        "name": "FQDN hugesoft.org",
320        "pattern": "[domain-name:value = 'hugesoft.org']",
321        "labels": [
322          "malicious-activity"
323        ],
324        "valid_from": "2015-05-15T09:00:00.000Z"
325      },
326      {
327        "type": "indicator",
328        "id": "indicator--8390fd29-24ed-45d4-84d7-c5e5feaf195d",
329        "created": "2015-05-15T09:00:00.000Z",
330        "modified": "2015-05-15T09:00:00.000Z",
331        "object_marking_refs": [
332          "marking-definition--3444e29e-2aa6-46f7-a01c-1c174820fa67"
333        ],
```

objects 〉 pattern

Run input_report

CONCLUSION

Conclusion

- Indicators can be useful to detect targeted attacks effectively
- Tools for automation and recognizing STIX are necessary for effective detection
- We introduce a Real-time Log Analysis tool for practical use of STIX
- We can reduce the incident response time by using the system
- As a result, damage from attacks can be minimized by immediate detection

Future works

- Comparison using valid period of the indicators
- Supporting more STIX indicator patterns
- Real-time importing of STIX indicators using TAXII (Trusted Automated eXchange of Indicator Information)

※TAXII is a technical specification to securely share and exchange threat information

REFERENCE

Evaluation of the system

- Summary of evaluation
  - Import the following STIX 2.0 indicators to Elastic Stack
    - Indicators of APT1:

      https://oasis-open.github.io/cti-documentation/examples/example_json/apt1.json
    - Indicators of poisonivy:

      https://oasis-open.github.io/cti-documentation/examples/example_json/poisonivy.json
  - Conduct normal business operations including Internet browsing via the proxy server
    - Access malicious URL on the blacklist several times
  - Transfer proxy logs to Elastic Stack
  - Evaluate whether the system can detect malicious communications correctly

Evaluation result

- Total amount of URL access: 15,790
- Total amount of C2 server access: 34

- False positive rate: 0%
- False negative rate: 0%

We published the source code of our tool.
https://github.com/sisoc-tokyo/STIX2_ES_detection

Thank you for your attention!
coe@ml.sisoc.tokyo