31ST ANNUAL FIRST CONFERENCE

EDINBURGH
JUNE 16-21
2019

Blue-team vs. Red-team Tabletop Exercise to Train the Process of Attack Investigation

Yoshihiro Masuda, Chiyuki Matsuda, Yusuke Kon, Keisuke Ito, Fumie Watanabe, Hajime Ishizuka, Toshiaki Ohta

Agenda

11:45-12:00 Introduction

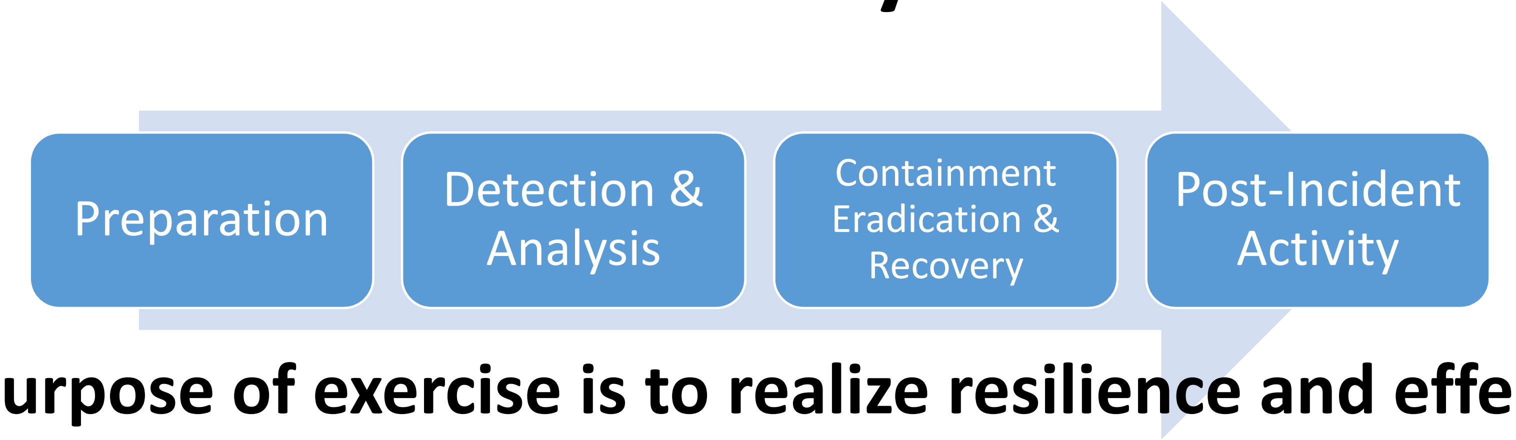
12:00-13:10 Hands-on: Tabletop Exercise

- ✓ Procedure explanation
- ✓ Role assignment (blue & red)
- ✓ Briefing on incident handling procedure(blue-team) & scenario selection (red-team)
- ✓ Exercise by tables
- ✓ Review

13:10-13:15 Closing

Introduction

Why Exercise is Necessary for CSIRTs?



The purpose of exercise is to realize resilience and effectiveness of Incident response.

- **Become to have mental readiness for cyber attacks and make familiar with incident handling procedure**
- **Extract issues and problems on current incident handling procedure and environment**

> *A CSIRT can most easily be described by analogy with a fire department.*
>
> *– Handbook of CSIRTs, CMU*

“But, there are some difficulties …”

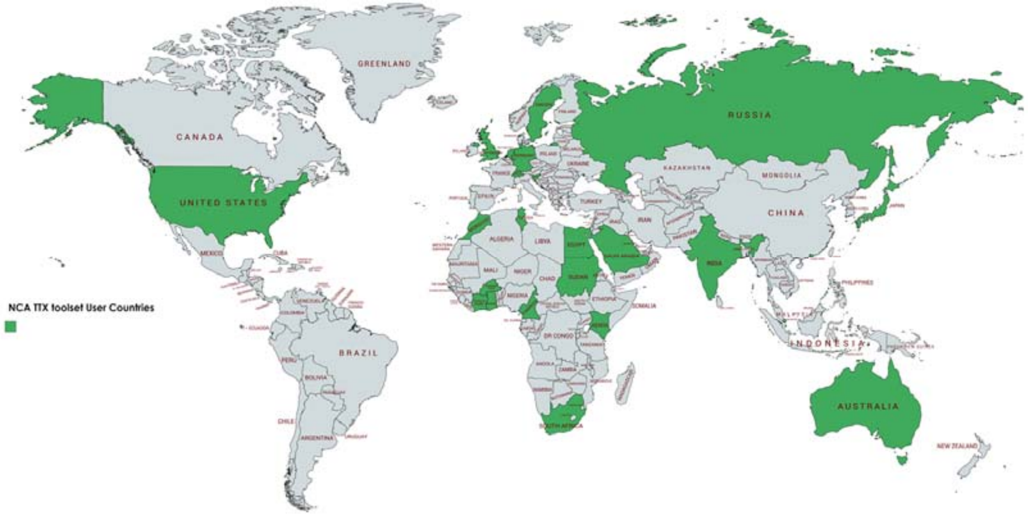
Lack of time to prepare

Lack of facilitation skills for conducting exercises

Difficulty of making effective exercise scenario

Workshop at FIRST Conference 2018

We developed a tabletop exercise method, and made a hands-on demonstration at FIRST Conference 2018.
The toolkit was shared with 25 workshop participants over 15 countries after the conference.



The countries our toolkit has been distributed

Developing the Method

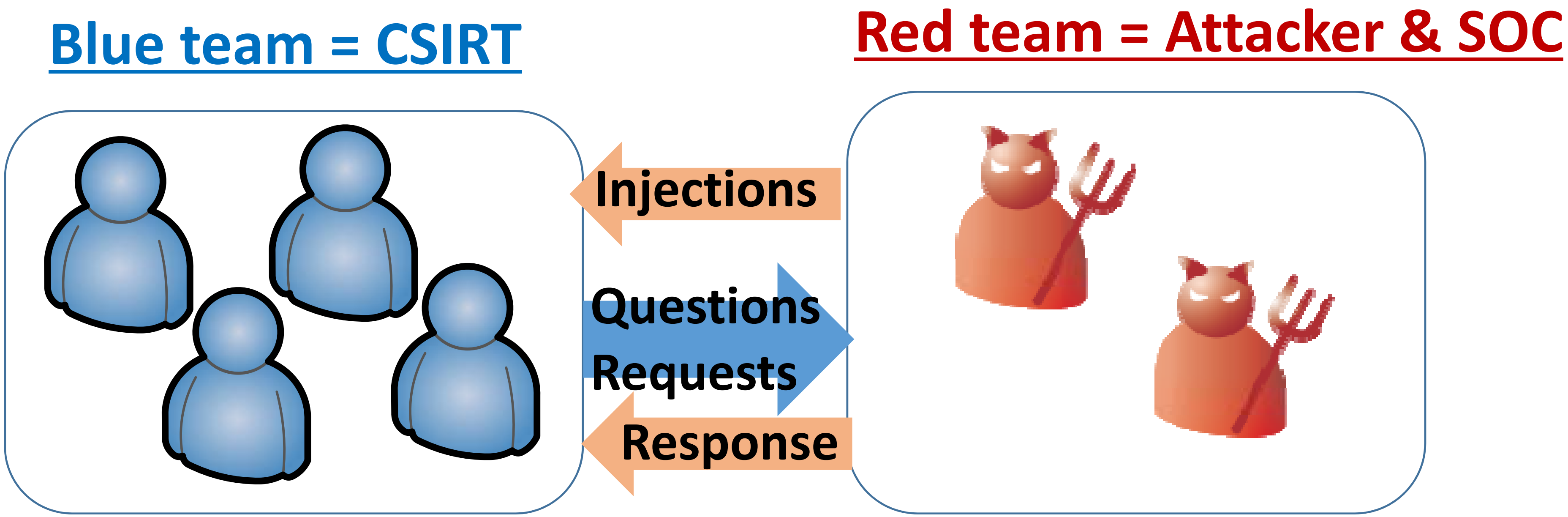
We developed a method which is focused on log analysis and containment.
Feasibility of the method has been verified through several trials at Incident Handling Exercise SIG of Nippon CSIRT Association (NCA), Japan.

Incident Handling Exercise SIG *of*
Nippon CSIRT Association, Japan

- SIG started on April 2016
- SIG members from 105 CSIRTs in Japan

Features of Our Tabletop Exercise Method

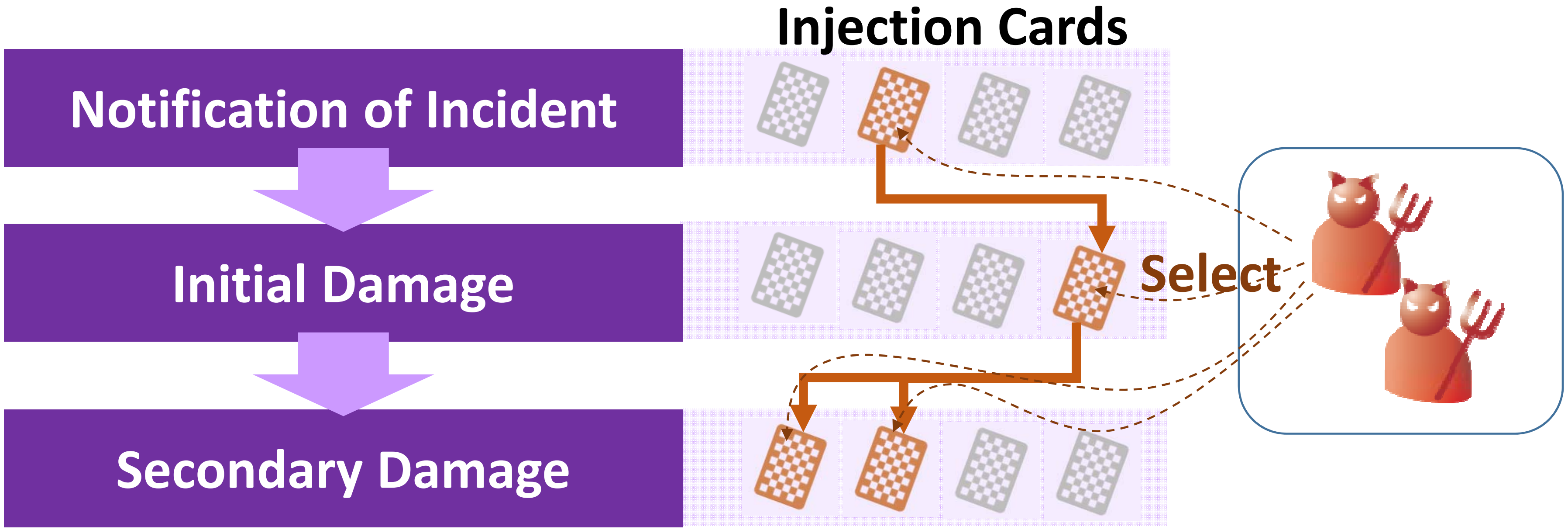
Feature 1: Blue team vs Red team Exercise



- Enforces red team members to think as an attacker
- Skilled facilitator is not required

Features of Our Tabletop Exercise Method

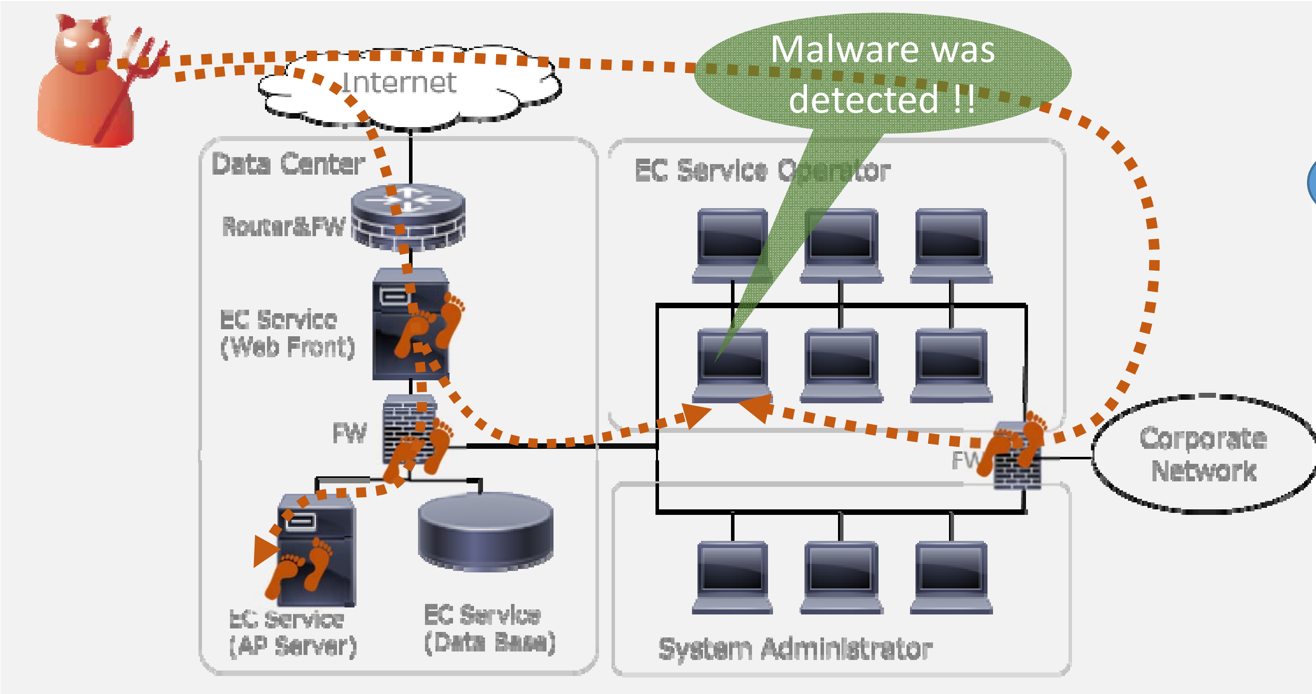
Feature 2: Random Scenario Making with Cards

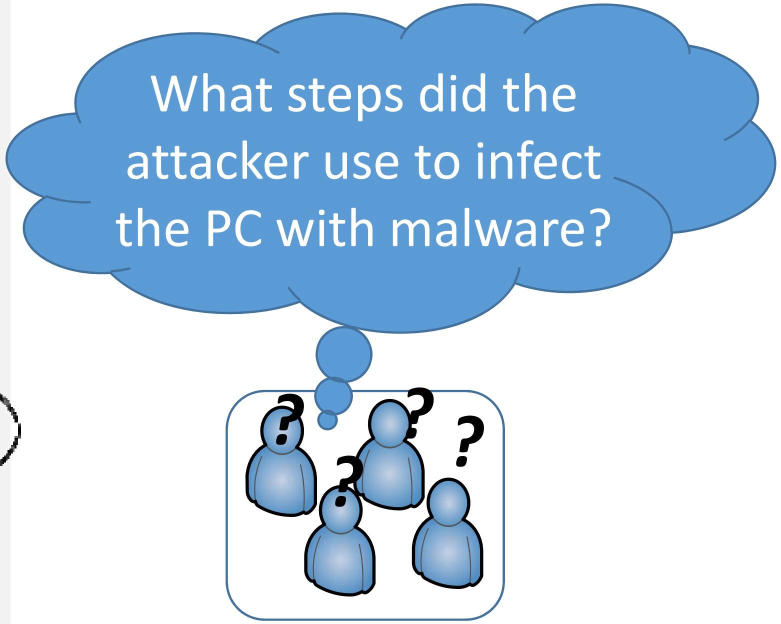


- Easy to develop an exercising scenario
- Enable to save time for developing an exercising scenario

Features of Our Tabletop Exercise Method

Feature 3: Focused on Containment and Investigation of Attack

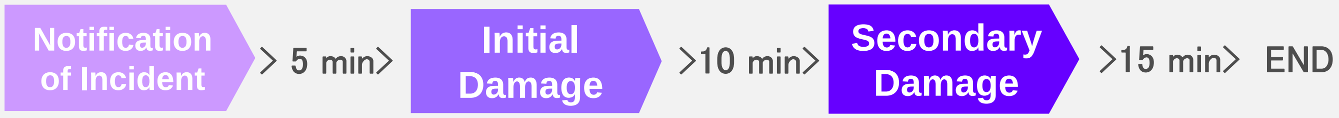



What steps did the attacker use to infect the PC with malware?
?
?
?
?

- **Improve the ability to discover attack process by analyzing log (as footprints) and decide suitable actions for minimizing the damage**

Hands-on:
Tabletop Exercise

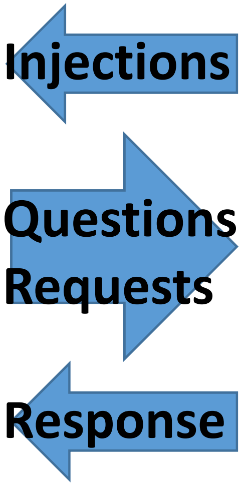
Schedule (12:00-13:10) 70 min

<table>
<tr><th></th><th>time</th><th colspan="2">items</th></tr>
<tr><td>Introduction</td><td>15</td><td colspan="2">• Overview of the tabletop exercise
• Self-introduction and role assignment at each table</td></tr>
<tr><td>Status Setting</td><td>5</td><td colspan="2">• Company profile and network architecture
• Threat Information</td></tr>
<tr><td rowspan="2">Preparation</td><td rowspan="2">10</td><td>Blue team</td><td>Red team</td></tr>
<tr><td>Discussion of Incident Response Procedure</td><td>Attack planning
- Chose a base scenario, and select condition cards</td></tr>
<tr><td>Exercise</td><td>30</td><td colspan="2">Blue team decides actions for injections given by red team.

Notification of Incident > 5 min> Initial Damage >10 min> Secondary Damage >15 min> END</td></tr>
<tr><td>Review</td><td>10</td><td colspan="2">Review the result by using a review sheet</td></tr>
</table>

Overview: What Blue & Red Team Do?

Blue team

- Discuss and present the countermeasures/actions to Red team, after receiving injection cards from Red team.
- Request log analysis to blue-team by using the request cards
- Note-taker write down the actions given by the commander on action recording sheet.


Injections

Questions
Requests

Response

Red team

- Present injection cards to Blue team
- Answer/respond to questions or requests from Blue team, based on your scenario
- Observe the blue-team actions for later review

Closing

How to Utilize Our Method

- Enhance reality by modifying the training kit reflect the actual system architecture and log file acquisition status in your own organization
- Improve capability by switching between red-team and blue-team
- Apply the training kit for integrated training with multiple system personnel involved

Thank you