Cybersecurity Talent Development in NTT Group

Takehiro Ozaki, NTT-CERT
Mitsuhiro Hatada, NTT Com-SIRT

About us

- Takehiro Ozaki
  - NTT Secure Platform Laboratories
    - Senior Research Engineer of NTT-CERT
  - NTT Group Certified Security Professional

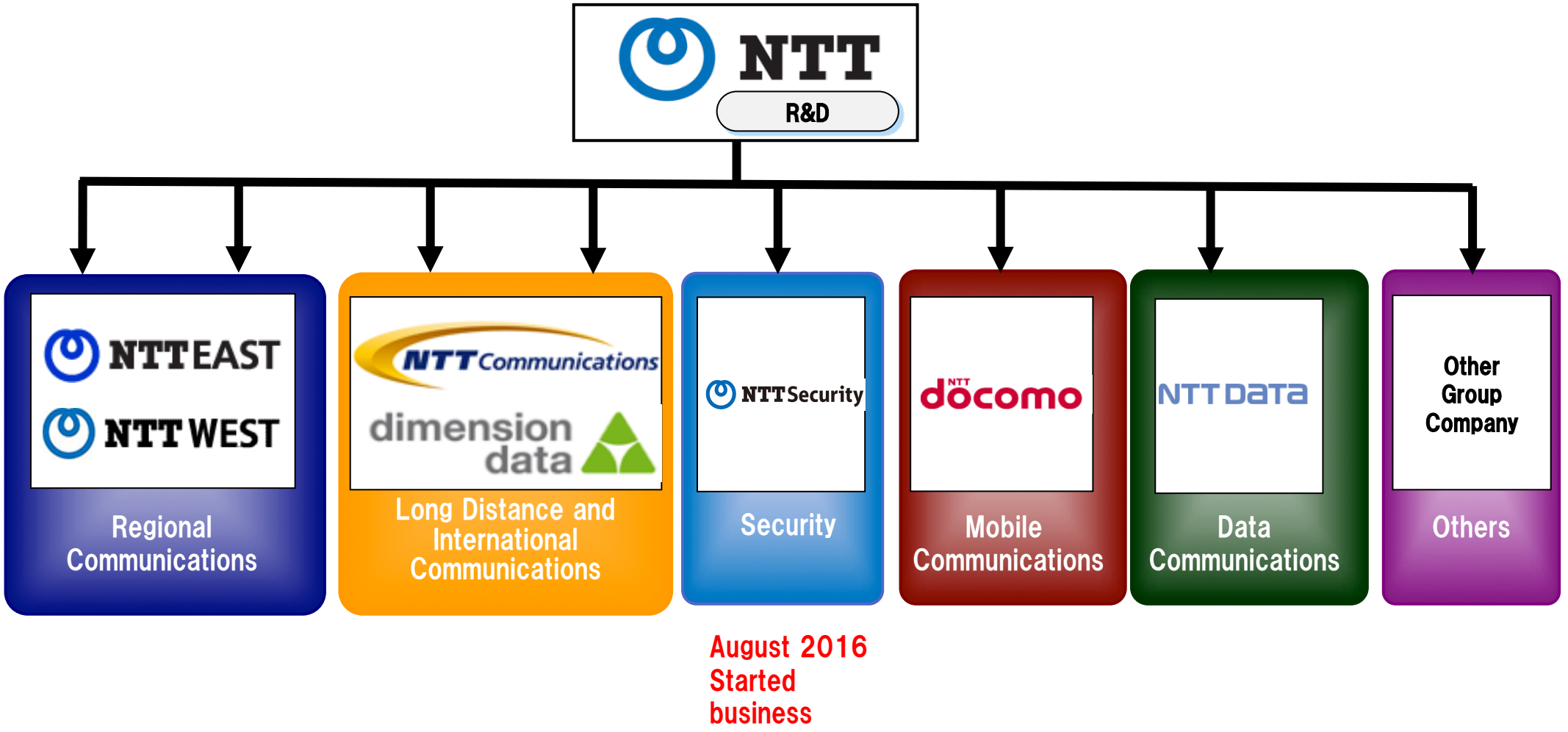
- Mitsuhiro Hatada
  - NTT Communications Corporation
    - Cybersecurity, Technology Development Department
    - & Tokyo 2020 Taskforce
    - & NTT Com-SIRT
  - NTT Group Certified Security Principal
  - Ph.D. student
  - MWS organizer
    - http://www.iwsec.org/mws/2017/

Agenda

- Security Certification Program in NTT Group
  - Overview of NTT Group
  - Security certification program
  - Technical activity
  - Keys to success
- NTT Com Cyber Range
  - Overview
  - Scenario Development
  - Training cases
  - Lessons learned

SECURITY CERTIFICATION PROGRAM IN NTT GROUP

Diagram of NTT Affiliate Groups

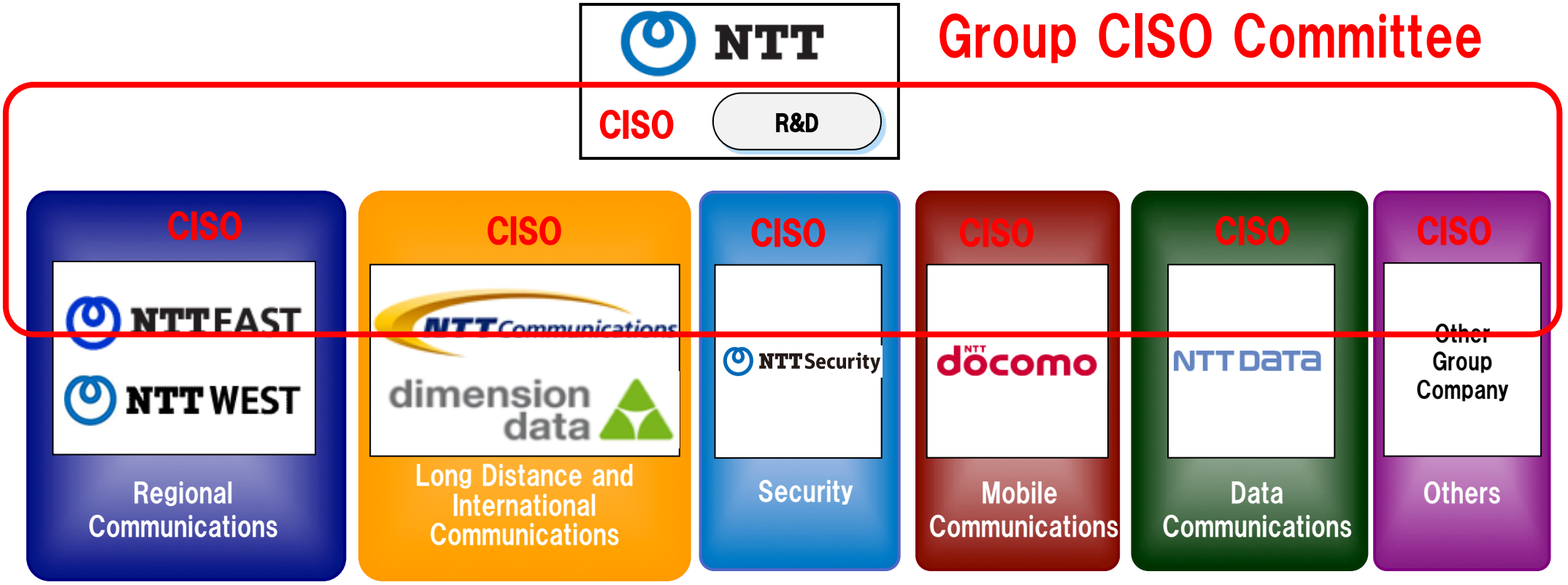


August 2016
Started
business

http://www.ntt.co.jp/gnavi_e/index.html

CISO and CISO Committee

- **Appointed CISO each group company and established the Group CISO Committee in 2015.**
  - **Promote security information sharing among group companies.**
  - **Strengthen security operation and cybersecurity talent development.**



Situation of Cybersecurity

A Few Years Ago …

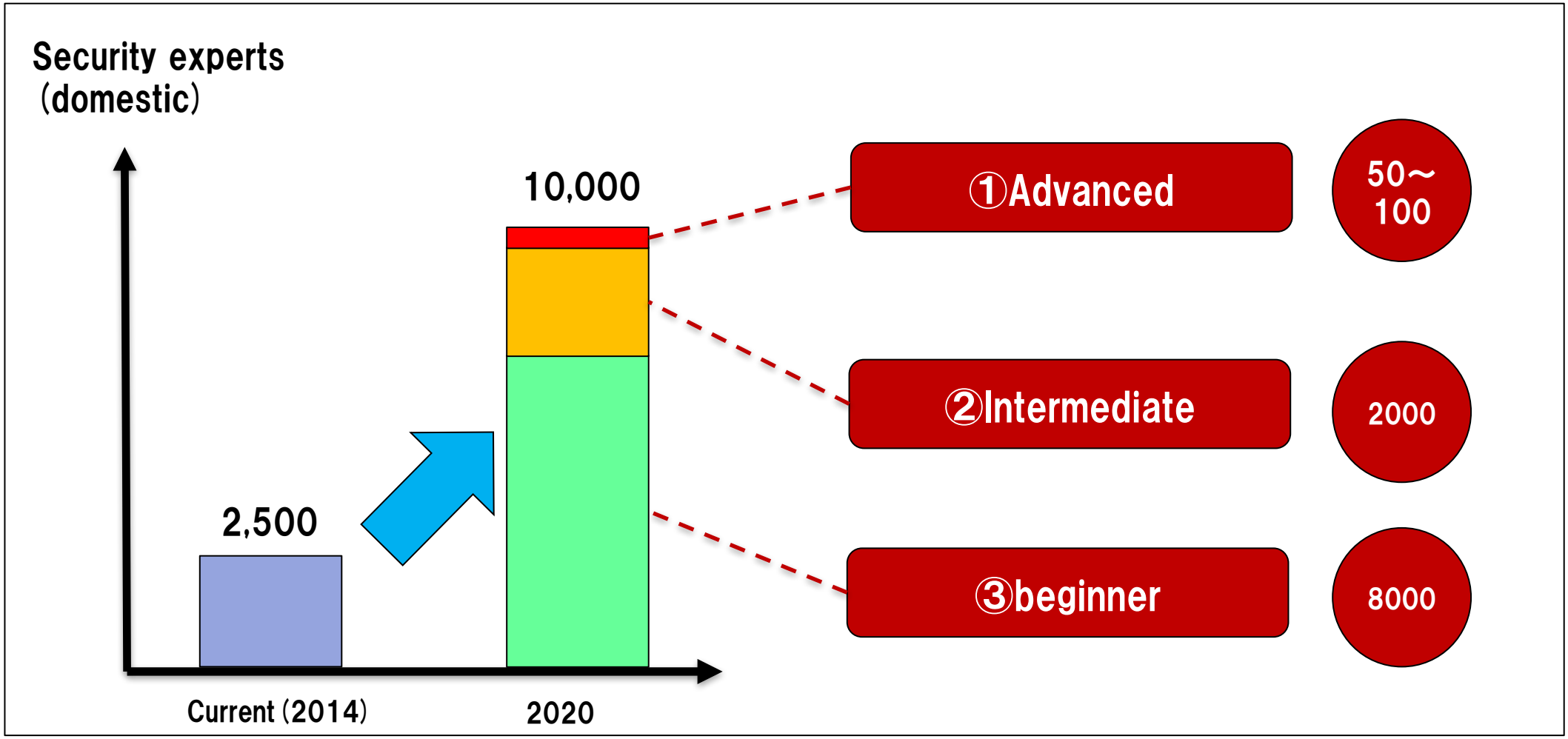
- In the world:
  - Cyber threats became more sophisticated and diversification.
  - Cyber attacks and data breaches became social issues.

- In Japan:
  - Cyber talent shortage has been a serious problem.
  - A Japanese government organization estimated in 2014 that Japanese companies need an additional 80,000 information security engineers.

- NTT Group:
  - Several cyber attacks and data breaches…

Increased demand for Security expert

- **Develop 10,000 security experts by 2020.**



Security Certification Program

- **Original Security Certification Program started in 2015**

☐ Why certification?

- **Define Classes, Titles, Levels of security experts.**
- **Encourage engineers to get more motivated in security field.**
- **Take the stats of security experts.**

For security experts to be motivated and to be active

Security expert Type/Level Map

Level	Title	Job Classification		
		Security management consulting	Security operations	Security development
Advanced	Security Master	Develop first-rate experts capable of delivering the best performance in the industry		
	Security Principal			
Intermediate	Security Professional	Reinforce the pool of specialists who have a wealth of experience and exceptional judgment		
Beginner	Security Expert	Raise the level of workers who are able to carry out their work with the required knowledge		

Definitions of Each Class

- **Security management consulting**
  - **Security supervisor**
  - **Auditor and Assessment**
- **Security operations**
  - **Monitoring operator**
  - **Operation supporter**
- **Security development**
  - **Architect**
  - **Engineer and researcher**

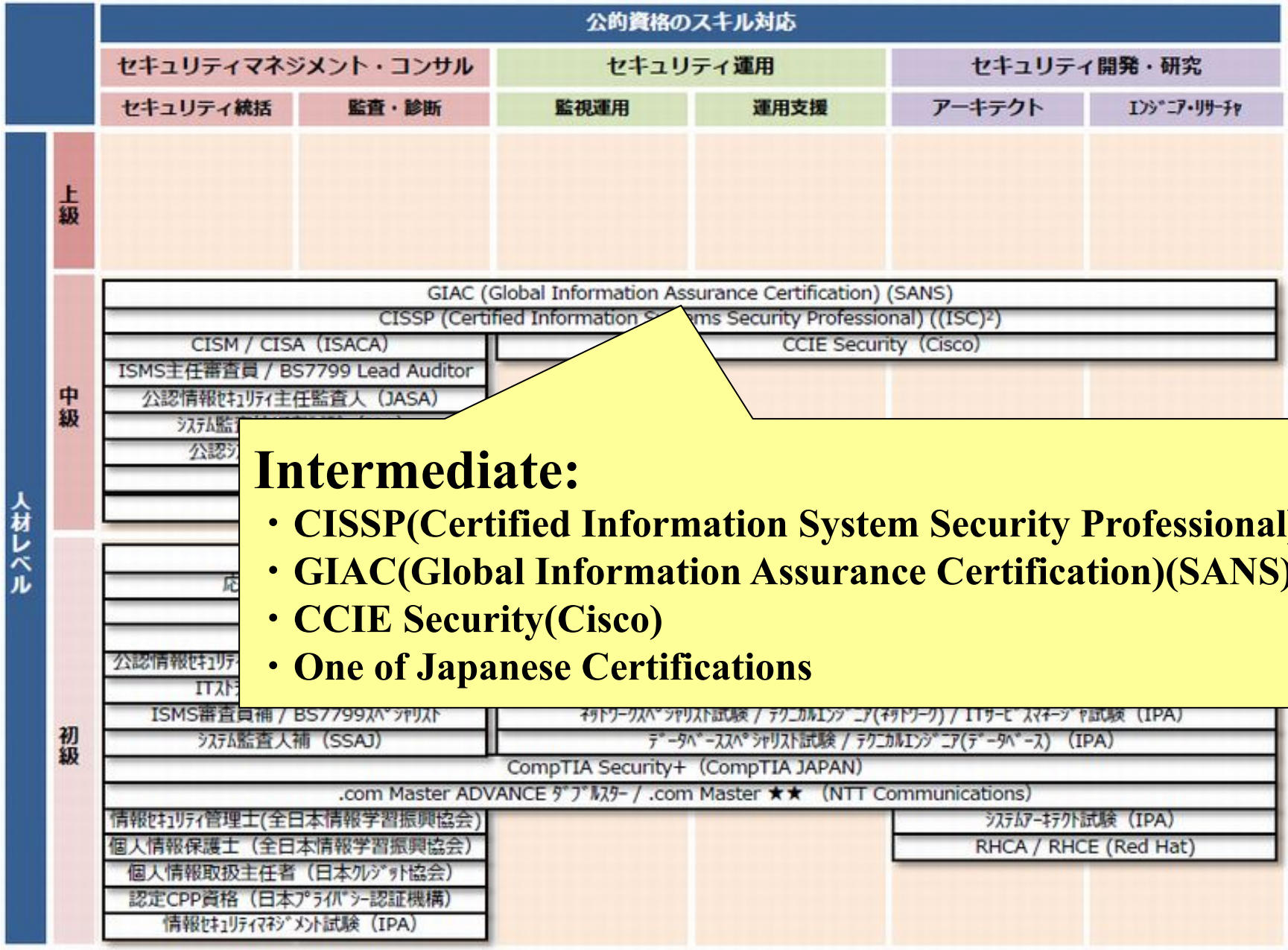
Level Qualification

- **Advanced:**
  - **Approval examination formed by group CISO committee member, current advanced members and university professors.**

- **Intermediate:**
  - **Work experience**
  - **Public/In-House qualifications**
  - **Pass an exam using Cyber Range (operations)**

- **Beginner:**
  - **Public/In-House qualifications**
  - **Take a training by the online lecture system (Gacco)**

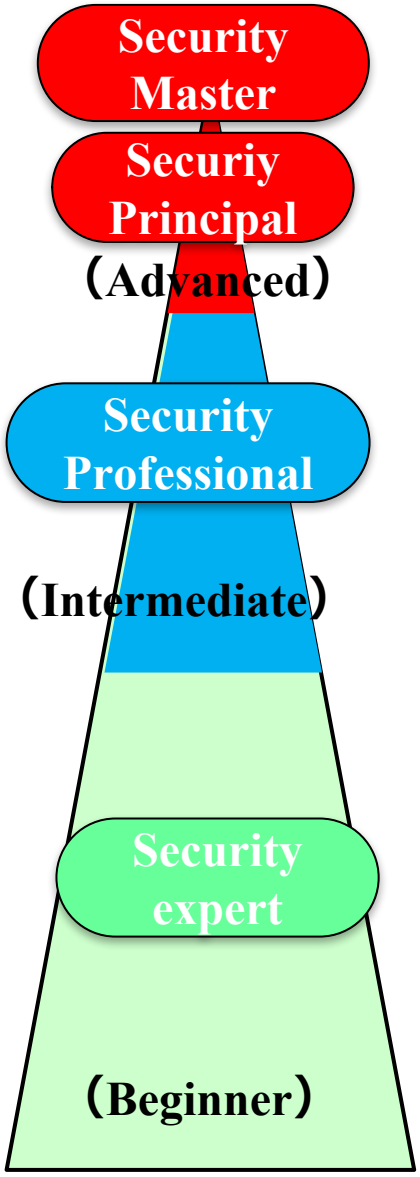
Public Qualifications



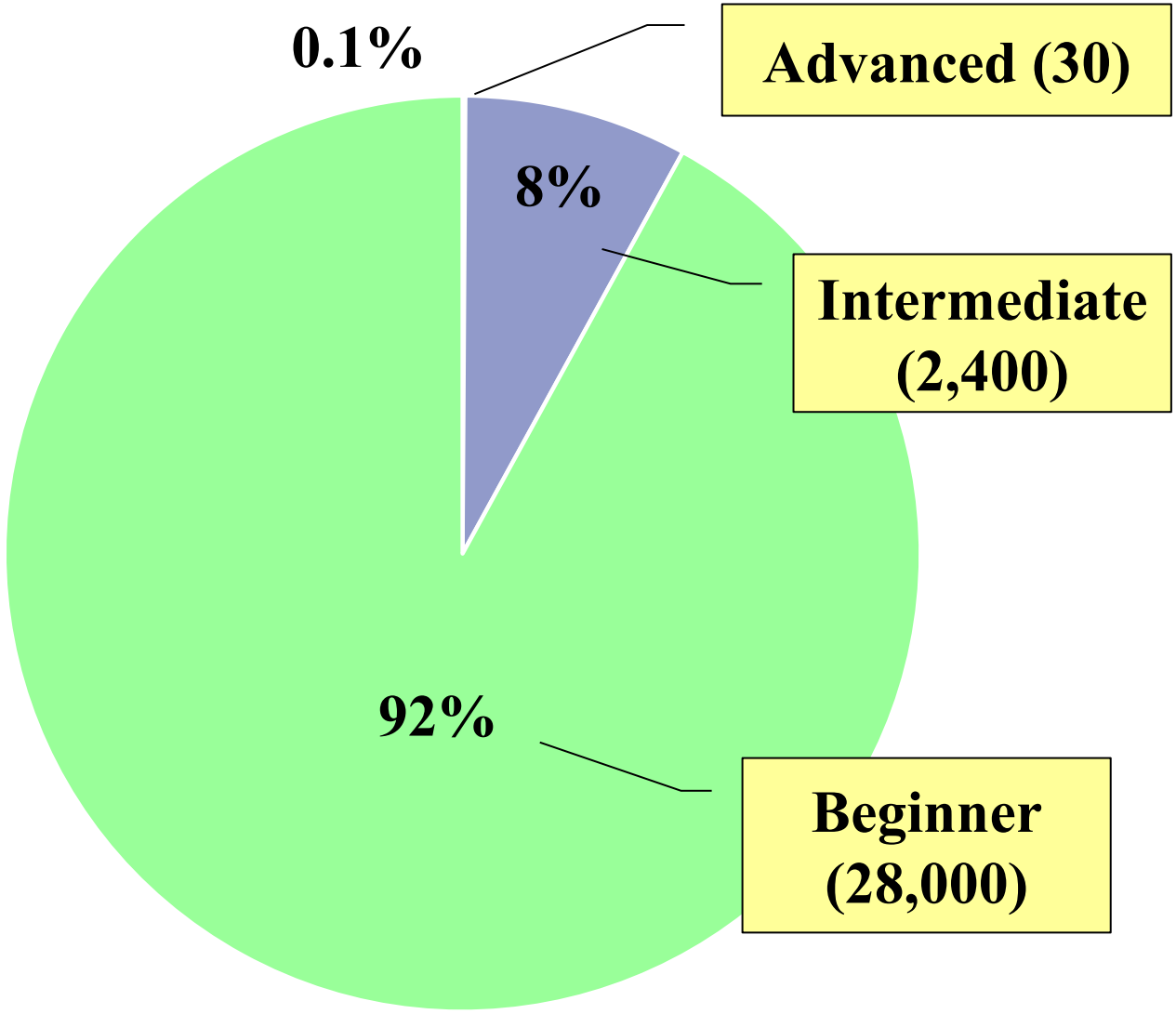
Intermediate:

- **CISSP(Certified Information System Security Professional)**
- **GIAC(Global Information Assurance Certification)(SANS)**
- **CCIE Security(Cisco)**
- **One of Japanese Certifications**

Current Security experts



Certified



Group Security Logo / License Card

● Logo

◆Derive

Since owls do not miss any small ones, they are said to be "guardian guards and guards of the forest" from ancient times, expressing the image of security that they are always watching

● License Card

Advanced

Intermediate

Beginner

Online Security Training

- **Produced by University Professors and Lab members.**
- **Online training for non-security personnel.**
- **Platform is provided by a NTT group company.**

Learning style by Gacco

Online

10 minutes
Video contents

Outside 、Free time

SmartPhone,
Tablet

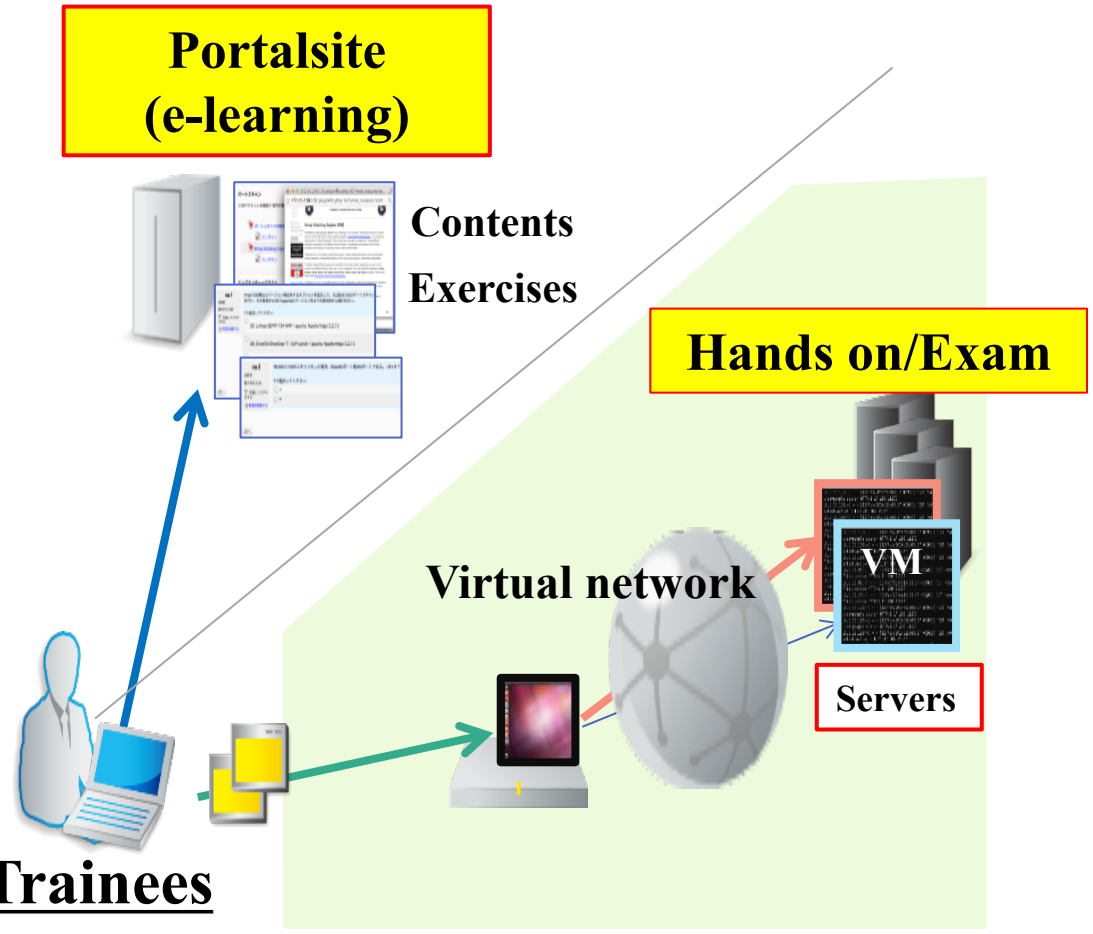
Gacco security program overview

Course name	Start date	trainer
情報セキュリティ『超』入門	2015/July	Institute of Information Security ‘s Professors
情報セキュリティ初級	2015/October	

Cyber Range Training

- **Technical Hands-On Training**
- **Trainee can get a certification of intermediate level of security-operation by passing an exam.**

●Cyber Range tarining

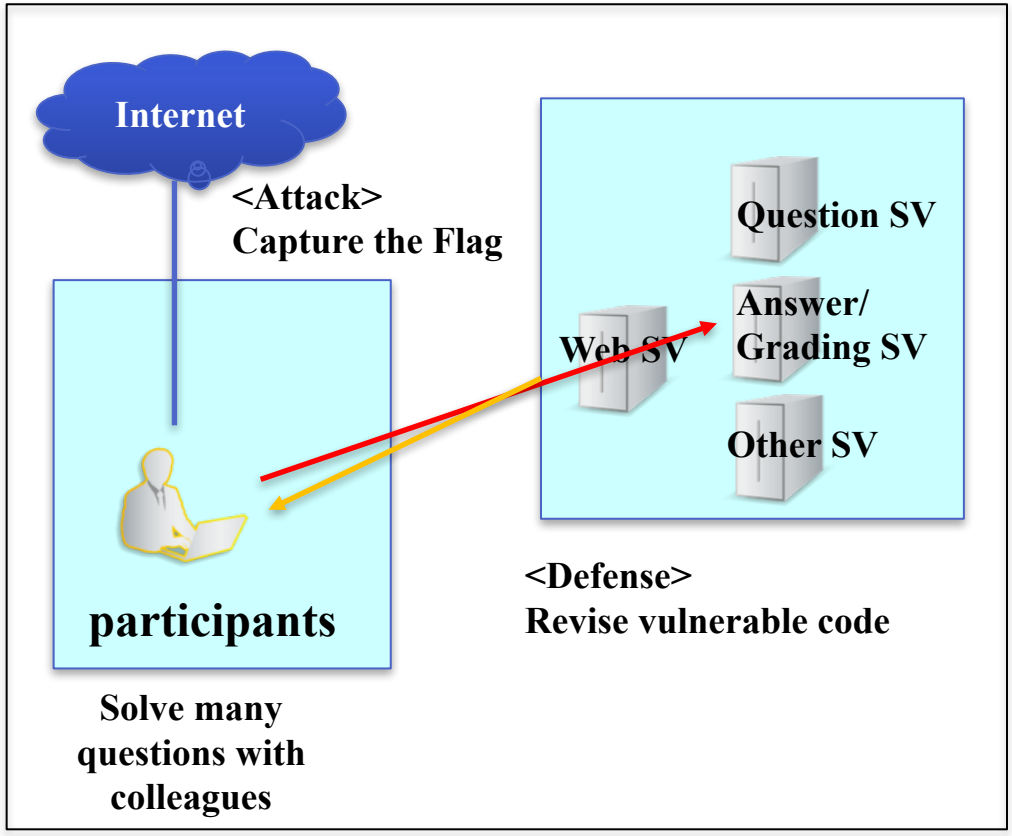


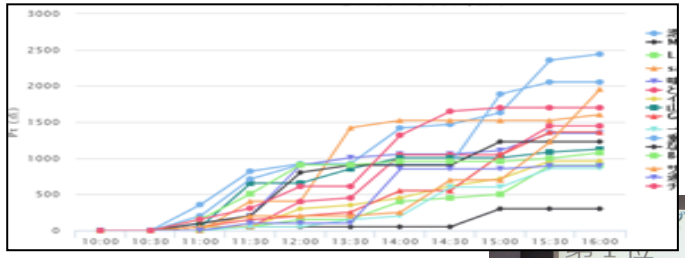
	Contents
Day 1	Web site compromise
Day 2	Data breach
	Spear Phishing
Day 3	DDoS
Day 4	Training and review
	Exam Test

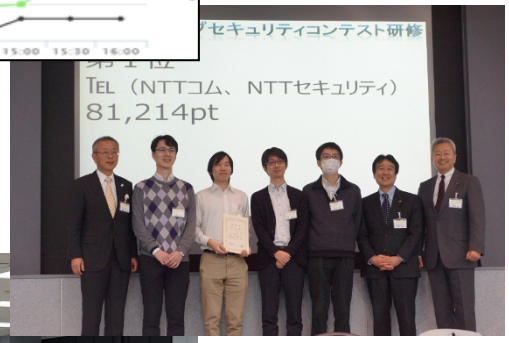
Security Contest

- NTT Group tournament for intermediate & beginner level experts.
- Communicate with each participants.
- Panel discussion and support by Advanced members.

Overview of contest







Winner

Atmosphere of the venue

Keys to Successful

- How to define specific security tasks and skill sets
  - Very complicated real tasks, required skills
  - Original definition of security experts ourselves
- How to expand this program to many group companies
  - Many group companies (departments) and several business conditions

Goal

Improvement of the environment and be active with motivation for security experts through Security Certification Program.

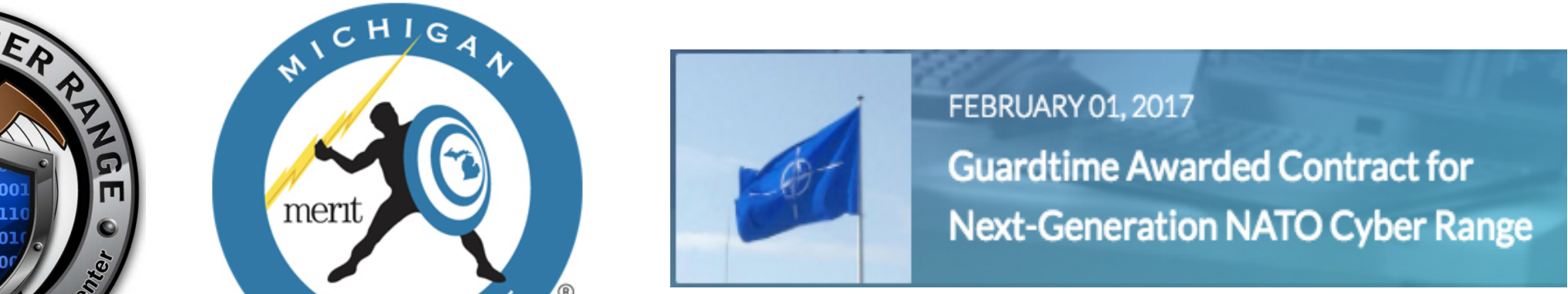
Further activities

- **Shifting aim to raise the beginner level engineers up to the intermediate level.**
- **Broadening this NTT Group's qualification method to overseas subsidiaries.**

NTT COM CYBER RANGE

Overview

- Cyber Range
  - Virtual and/or physical environment
  - Cyber warfare training and testing



Motivation of own development in 2014

- Flexibility
  - Architecture
  - Topology
  - Virtual and/or Physical
  - Privilege
  - Threat changes
- Reusable experience
  - Incident
- Principle
  - Avoid vendor specific feature
- Target people
  - From beginners to professionals
  - Various job categories as ISP, MSSP, and CSIRT.
    - Pre-sales engineers
    - Network operators
    - System developers
    - Analyst

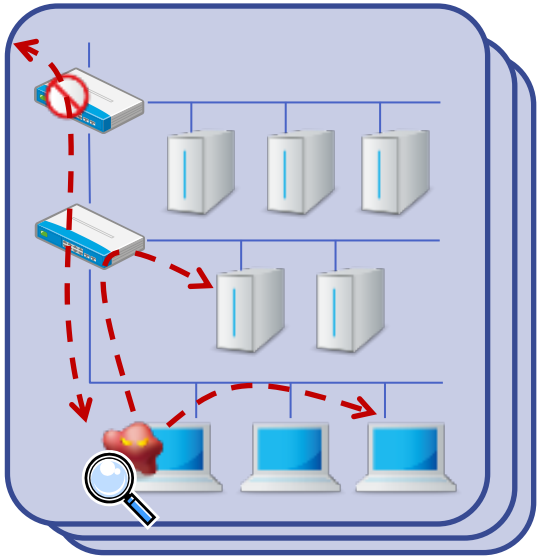
The farthest way about is the nearest way home.

People surrounding our cyber range

Developer

COTS Tester

Infrastructure engineer



Testing

Training

Scenario developer

Trainer

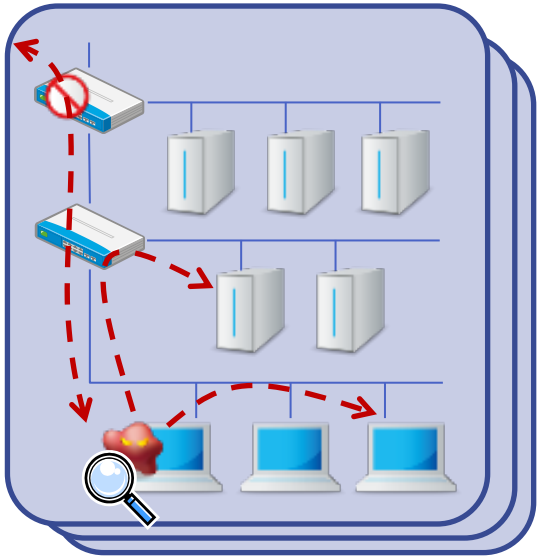
Trainee

Testing example

Developer

COTS Tester

Infrastructure engineer



Testing

- Developer
  - Threat hunting tool
  - Controller
- COTS Tester
  - Sandbox
  - EDR
- Infrastructure engineer
  - OpenStack
  - vSphere

Training example

- Basic course
  - Crypto
  - Authentication
  - Packet analysis/crafting
  - Web vulnerability
  - Reverse engineering
  - Exploit
- Advanced course
  - Web site compromise
  - Multiple types of DDoS
  - Spear Phishing
  - Data breach

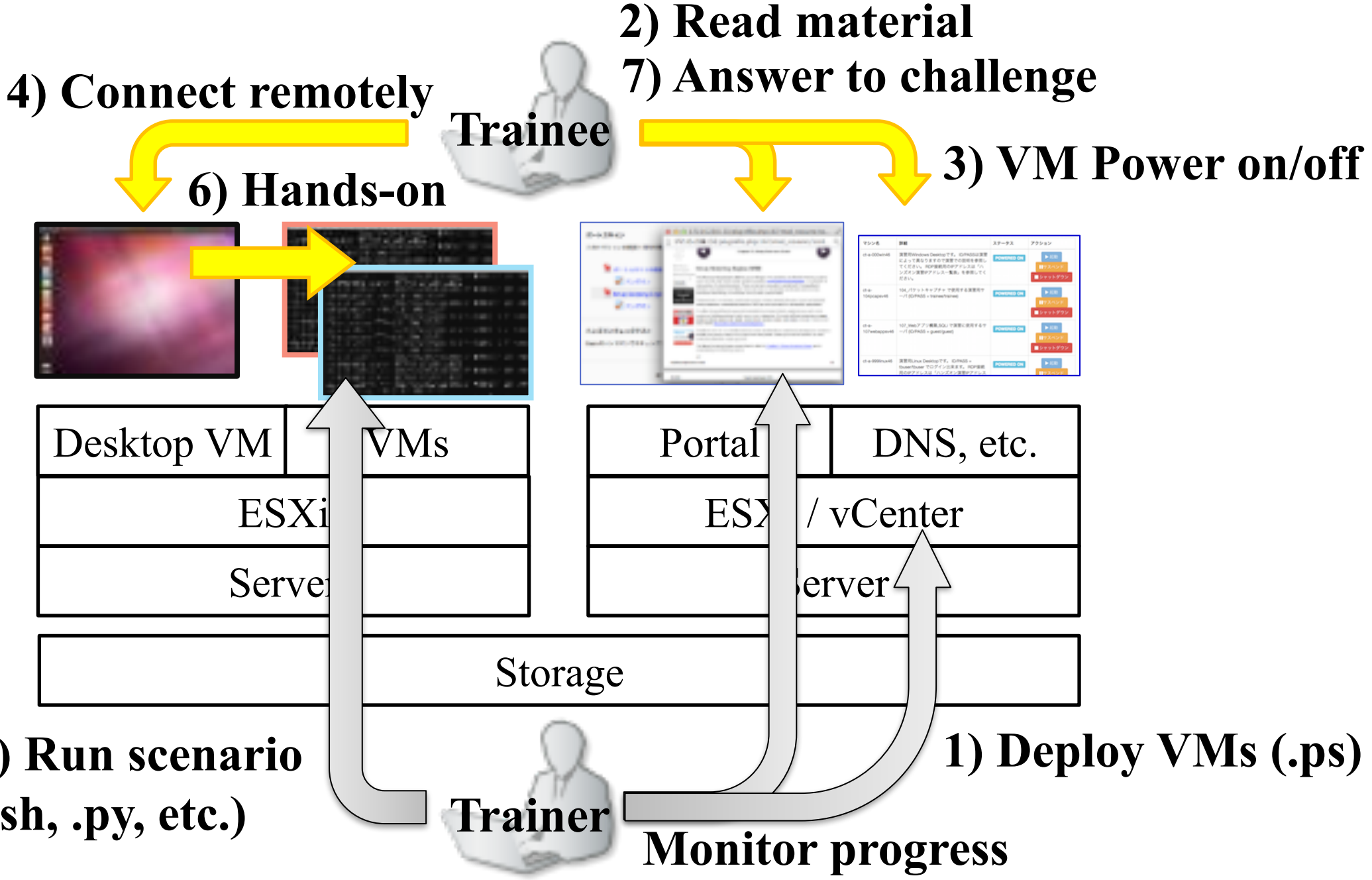
Training

Scenario developer

Trainer

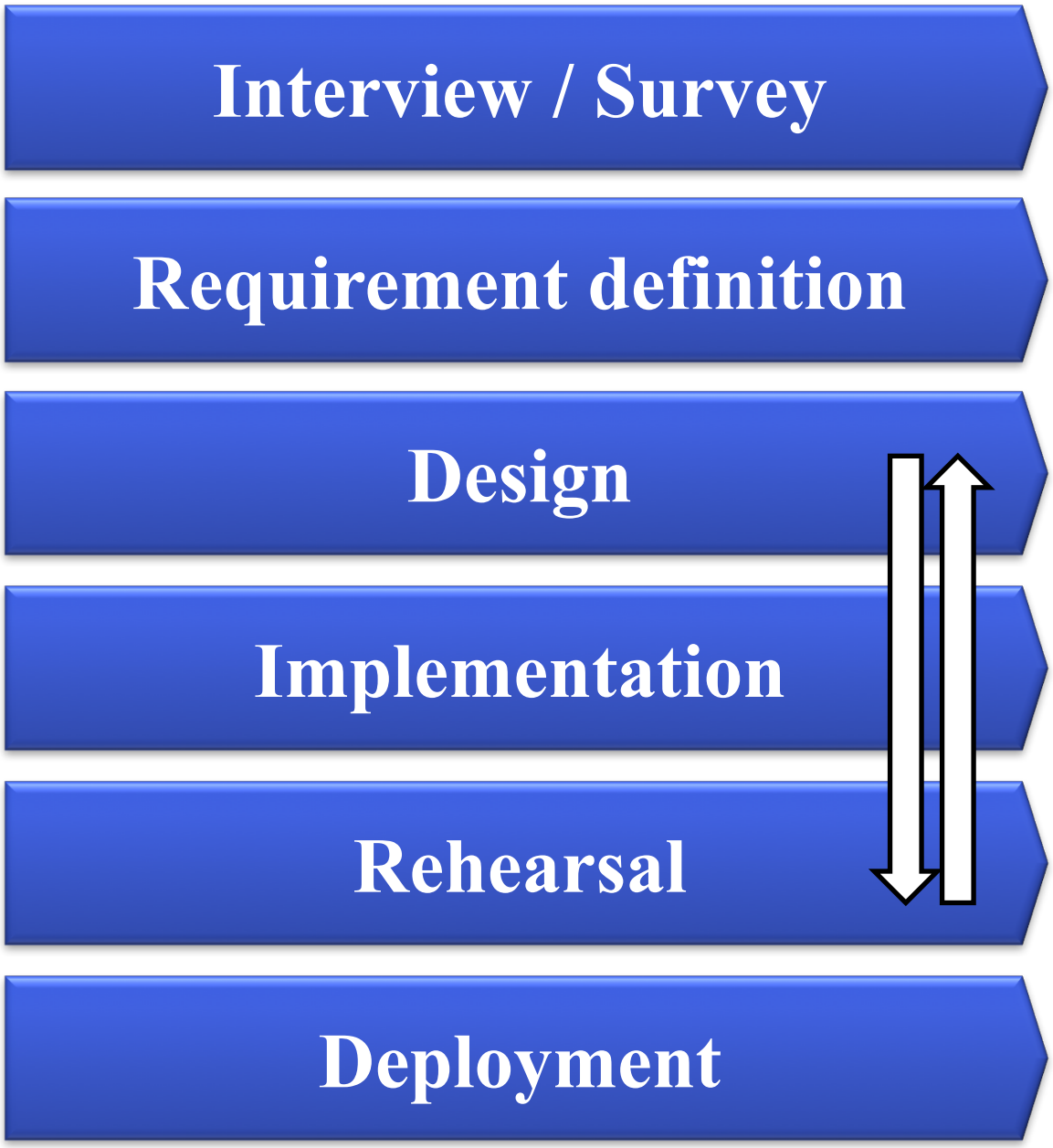
Trainee

Component and Operation



DEMO

Scenario development



- Incident detail
- Problems / Struggles

- Skills you can earn

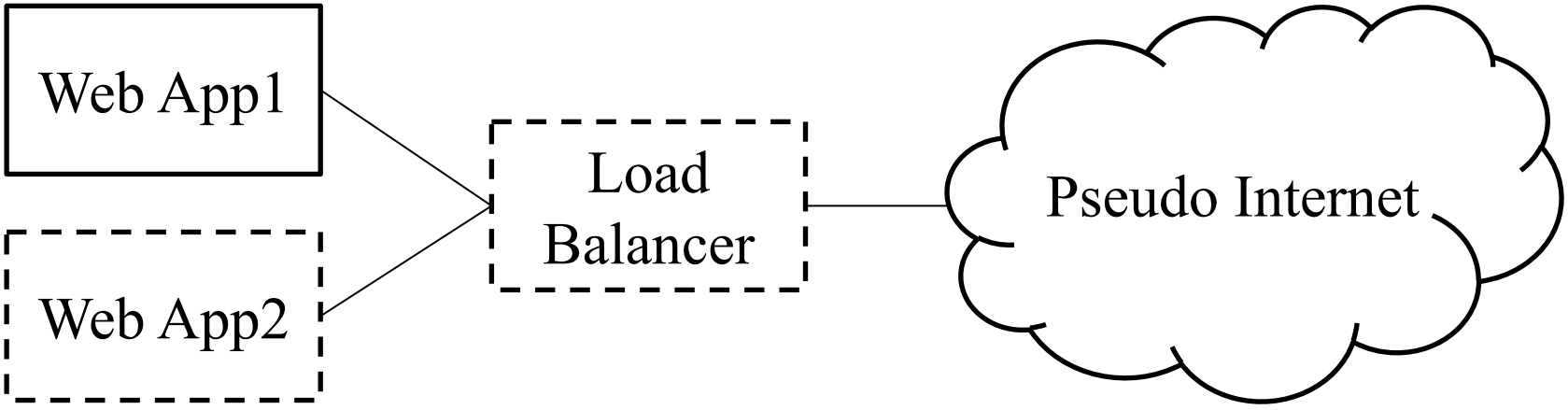
- Host and Network
- Attack and Defense
- Legitimate action
- Common or individual
- Test
- Reading material & challenges

- Walk-through

- Master images creation
- Copy and change setting

Web site compromise

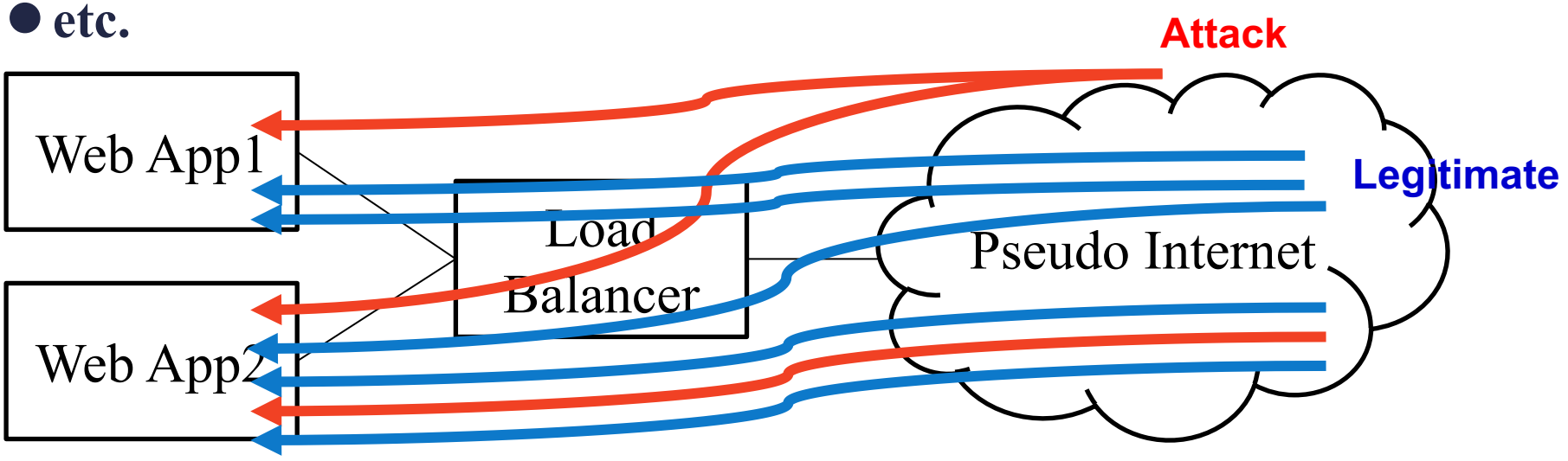
- Section 1
  - Vulnerability (Struts2) and incident cases
  - Setup
    - Install and configure apache, tomcat, and struts with sample application on Web App2
    - Install and configure mod_proxy on Load Balancer
    - Customize logging



Understand the environment.

Web site compromise

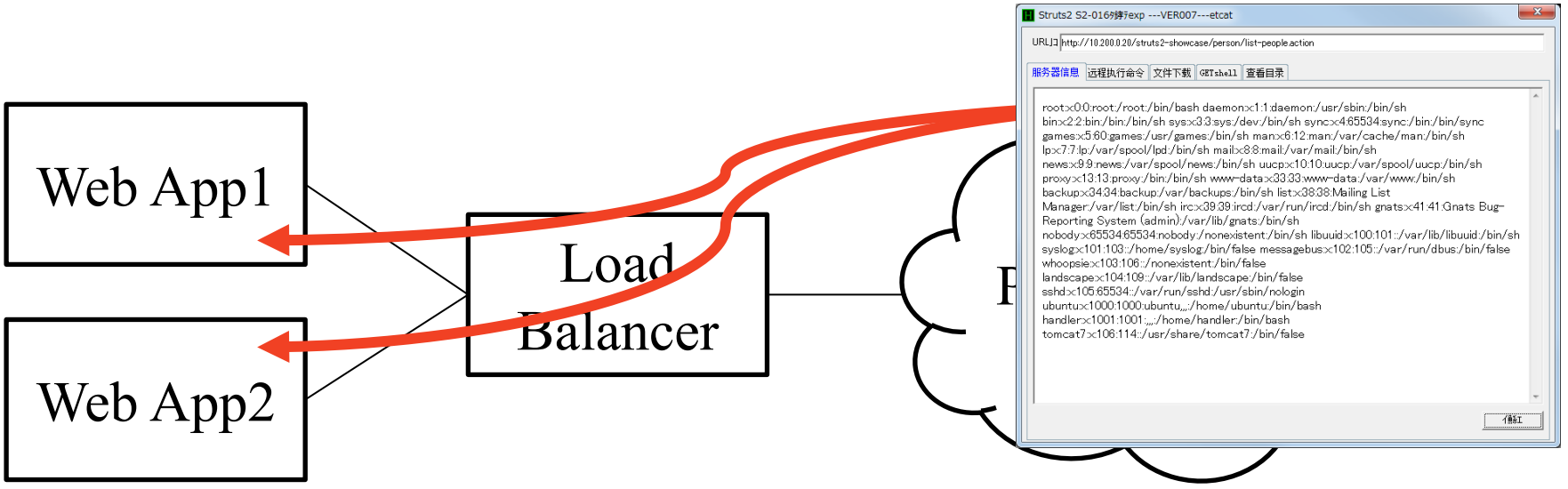
- Section 2
  - Detect attacks
  - Investigate incidents
    - Attack sources
    - Uploaded file
    - Webshell
    - etc.



Analyze logs and files w/o overlooking.

Web site compromise

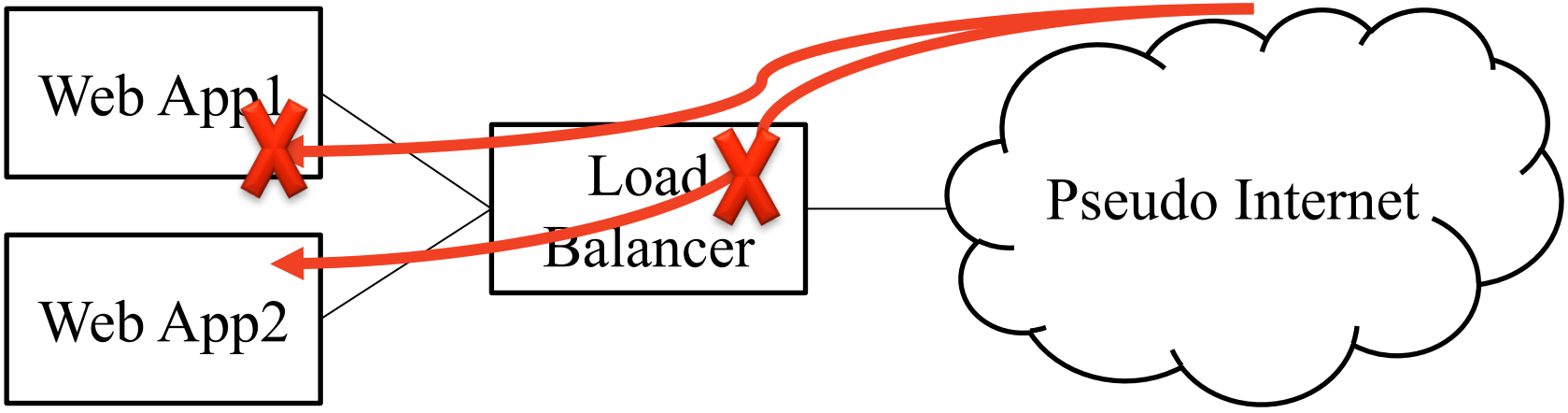
- Section 3
  - Try PoC
  - Utilize attack tool
  - Verify logs, files and packets



Know your enemy.

Web site compromise

- Section 4
  - Apply interim measure
    - mod_rewrite, mod_security, and Servlet filter
  - Test
  - Identify limitations
  - Apply permanent measure
    - Fixed version



Defend by better choice.

Certification training and exam.

- Curriculum
  - Day 1 – 3
    - Advanced (4 scenarios)
  - Day 4
    - Review
    - exam. (modified 4 scenario)
- Style
  - Lecture and hands-on
  - Individual
- Kit
  - Laptop and display
  - Wifi
  - Internet connection
- Size
  - 8 - 10 trainees from multiple companies / a term

Security Bootcamp for NTT Group

- Curriculum
  - 1st month
    - Basic
  - 2nd month
    - Advanced (4 scenarios)
- Style
  - Self-learning
  - Individual
  - Biweekly review meeting
  - Wrap-up meeting w/ trainee's boss
- Kit
  - Laptop and display
  - Wifi
  - Internet connection
- Size
  - 4 - 8 trainees from multiple companies / a term

Wrap-up meeting

enPiT Security “SecCap”

- Curriculum
  - Advanced (2 scenarios)
  - Short version
- Style
  - Lecture and hands-on
  - 3 – 4 students / group
  - Tutor / group
- Kit
  - Laptop
  - 1 display / group
  - Wifi
  - Internet connection

- Size
  - 20 - 30 students from multiple universities / a term

https://www.seccap.jp/gs/index.html

Lessons learned

- Keep away from regular work.
- Make trainees compete with each other.
- Deal with actual incident to enhance reality of scenario.
- Practice makes perfect.
- Essential things to learn are immutable even in exercises targeting old vulnerabilities.
- Briefing and debriefing are crucial.
  - Avoid misunderstanding the situation and the role.
  - Feedback to each other leads to the next action.
- Clarify what level of talent you want to raise.


Thank you!