From Learners to Leaders: A "Train the Trainer" Model for Self-Sufficient Cyber Resilience in Southeast Asia

Armoris Inc
kamata@armoris.jp

2025/Sep/10
@**APNIC** / **FIRST**

Me: Keisuke Kamata

- 24 years in cybersecurity (started at JPCERT/CC in 2002)
- Start working with JICA's cybersecurity project since 2008
- Founding member of Financials ISAC Japan (2014)
- Advisor to Japan Financial Services Agency since 2016
- Cybersecurity Advisor to Ibaraki Police since 2021
- CTO of Armoris Inc Japan since 2019

Context & Challenge

- Rising cyber threats worldwide (same in 20+ years)
- Limited local resources and reliance on external experts
- Need for *sustainable, self-sufficient* resilience capability

Project overview

- Cyber Range & Table top hybrid exercise train the trainer
  - As a part of Japan International Cooperation Agency (JICA) project for cybersecurity enhancement in AP region
- **Main goal:**
  - Build local leaders
- **Target countries:**
  - Indonesia: University of Indonesia ++
  - Cambodia: Ministry of ICT
  - Philippines: Department of ICT
- **Duration:**
  - 2024/Oct - 2025/Apr

CR&TT hybrid exercise overview

203.0.113.0/24

Redteam (you)

Attacker

bluetam

DMZ (10.0.16.0/24)

dns(10)

web(11)

SERVER (10.0.32.0/24)

proxy(10)

file(11)

CLIENT (10.0.64.0/24)

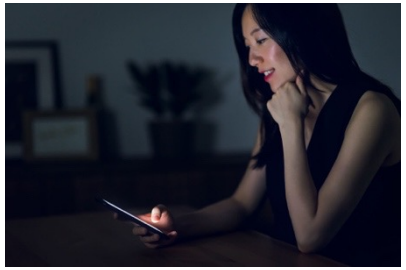
win10(10)

fwids
(254)

Tech

Mgmt

Top management (or CISO)



customer

regulator

police

Project Steps

1. Pre training (2 months)
2. T3 session : Part I (8 days)
   - Let candidates to build exercise environment
   - Conduct attack and defense (log analysis)
   - Understand exercise planning method
3. T3 Session : Part II (2 days)
   - Half of them become red team and conduct exercise
     - Another half blue
   - Swap red/blue and conduct exercise again
4. Actual Training session :
   - Conduct actual exercises in each countries (4 days)

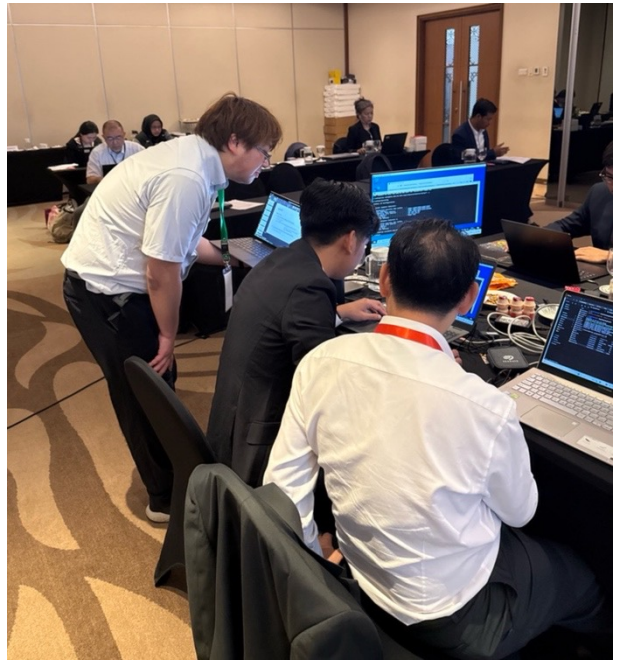
1. Pre training

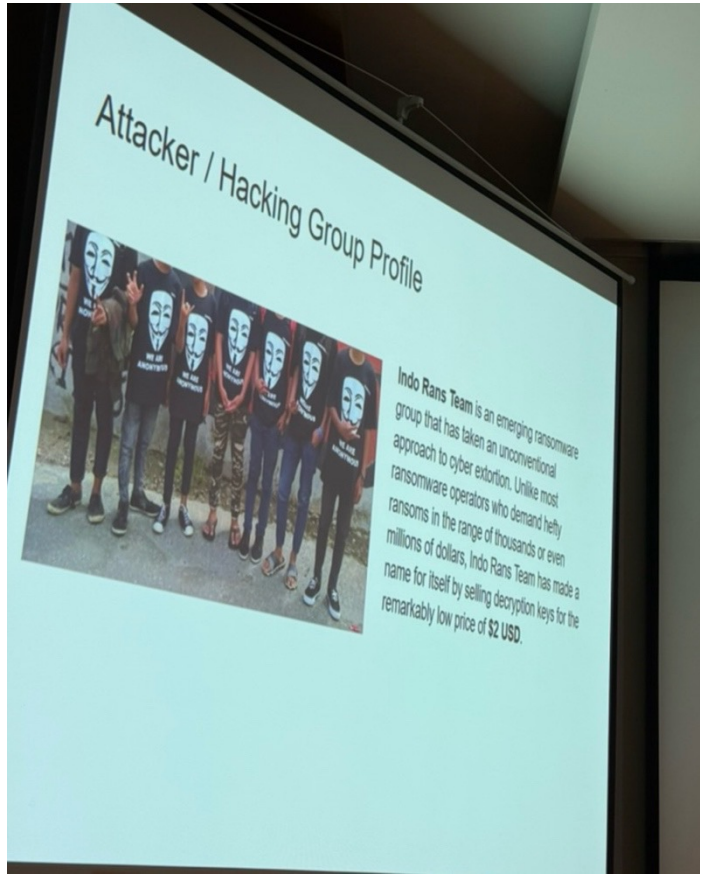
- Purpose: make sure all participants have basic skills

- Participants will do self work to
  - Setup linux servers
    - Web / mail / dns / proxy / ssh
  - Try webdefacement vulnerability exploitation and log analysis

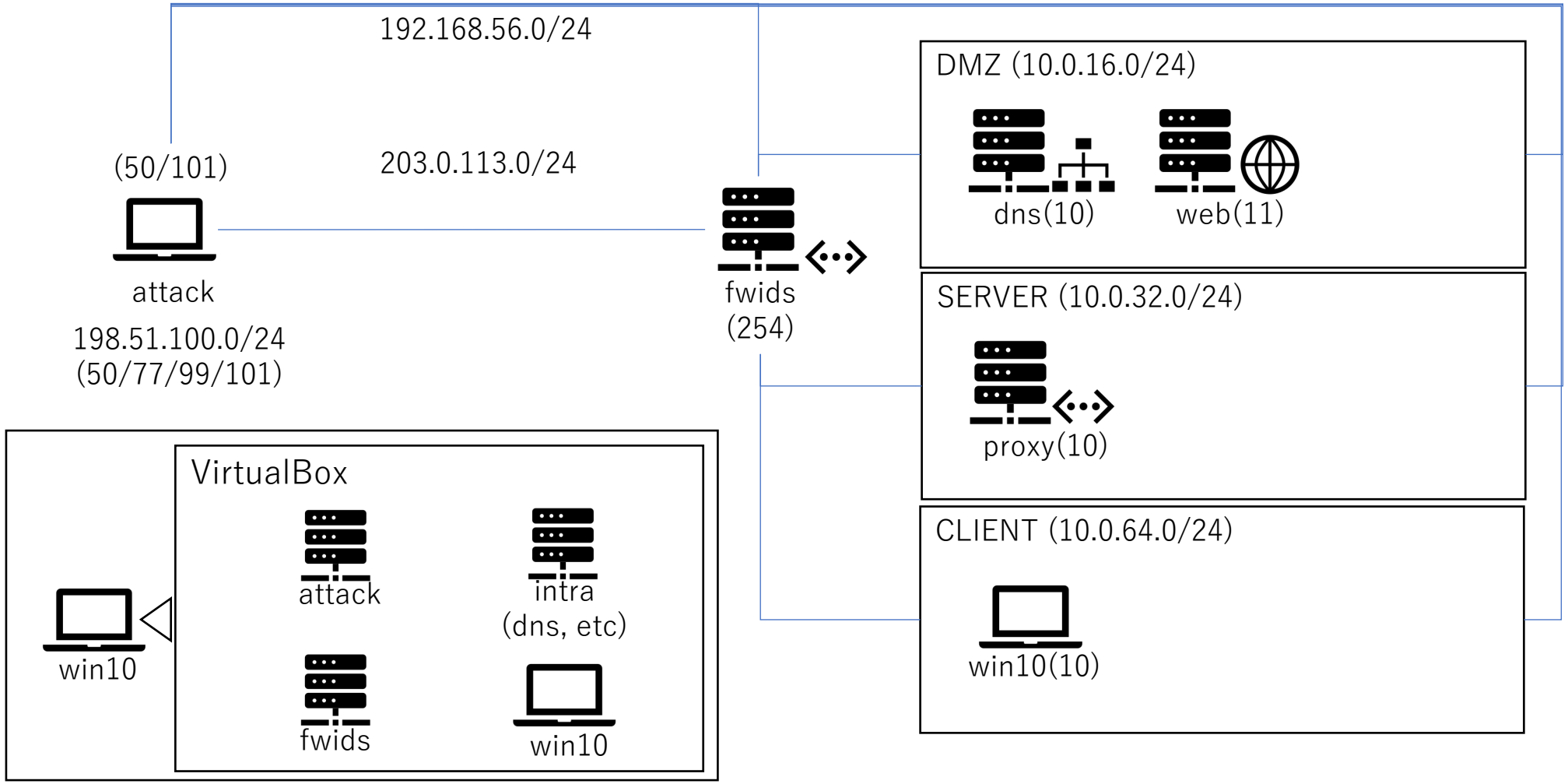
  - Setup windows server and AD environment
  - Log reading practice in windows client and servers

T3 session PI / PII




Attacker / Hacking Group Profile
Indo Rans Team is an emerging ransomware group that has taken an unconventional approach to cyber extortion. Unlike most ransomware operators who demand hefty ransoms in the range of thousands or even millions of dollars, Indo Rans Team has made a name for itself by selling decryption keys for the remarkably low price of $2 USD.

Environement Setup

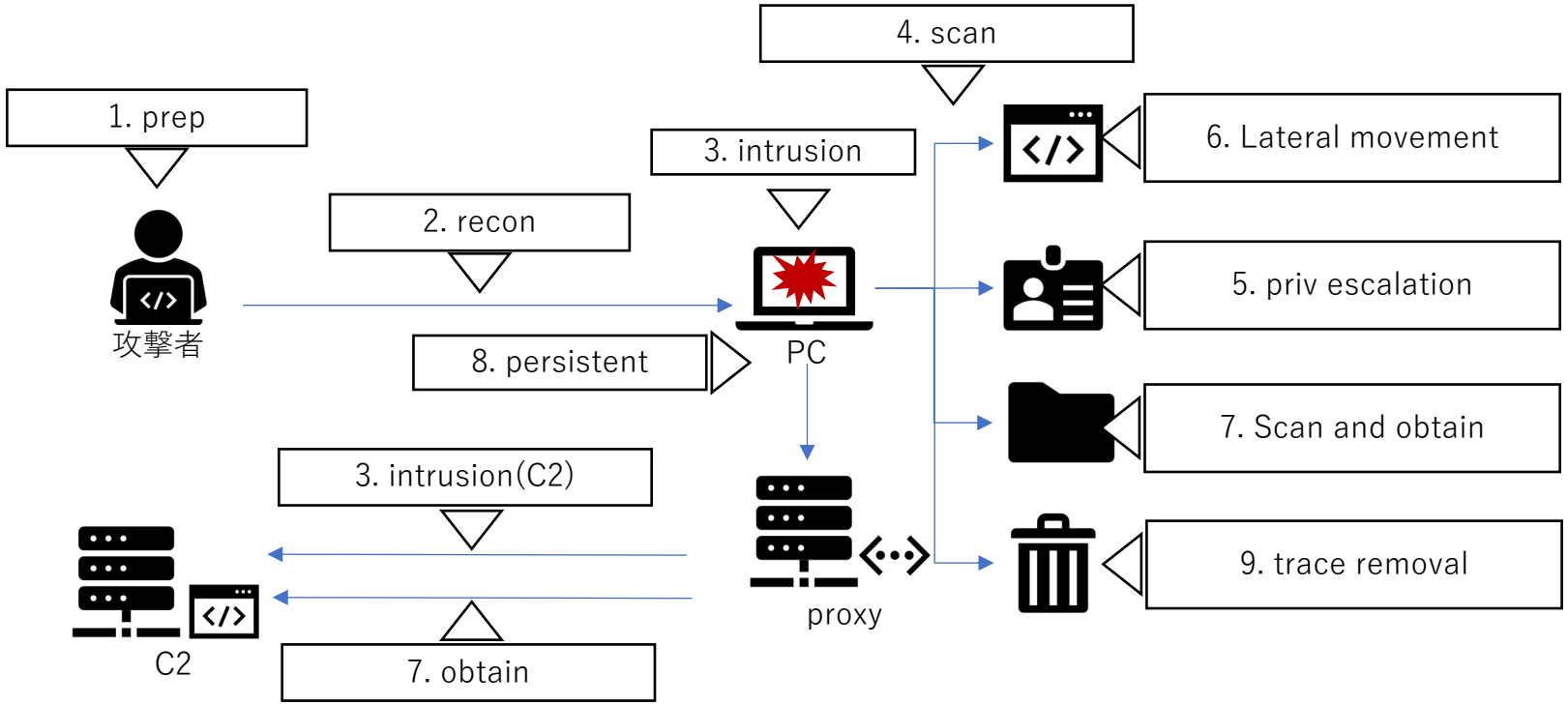


Attack & Defense for APT scenario

Step by step scenario overview:

[Scenario]

1. Attack prep
2. Recon
3. Intrusion
4. Scan
5. Privilege escalation
6. Lateral movement
7. Scan and obtain
8. persistent
9. Trace removal

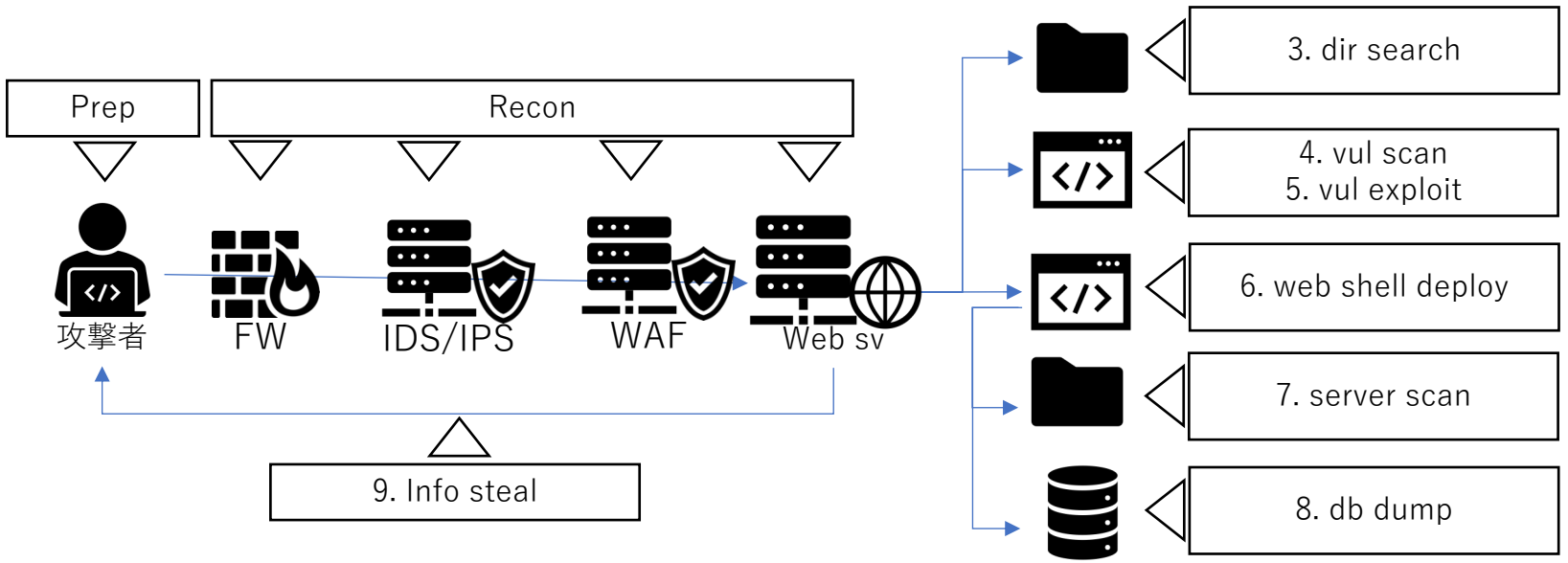


Attack & Defense for webshell scenario

Step by step scenario overview:

[Scenario]

1. Preparation
2. Reconessans
3. Directory search
4. Vulnerability scan
5. Exploitation
6. Web shell deploy
7. Server scan
8. DB dump
9. Information steal




Armoris Cybersecurity Learning
Wonna Phal
Armoris Cybersecurity Learning
Visal Ouk
Armoris Cybersecurity Learning
Tan Sopheak
Armoris Cybersecurity Learning
Renz Delmor V. Zabala
Armoris Cybersecurity Learning
Glenn Mark Arnobit
Armoris Cybersecurity Learning
Lawrence Leah Rosello Sze
Armoris Cybersecurity Learning
Elvian Syafrurizal
Armoris Cybersecurity Learning
Khalid Abdulah
Armoris Cybersecurity Learning
I Gde Dharma Nugraha
Armoris Cybersecurity Learning
Ruki Harwahyu
Armoris Cybersecurity Learning
Yan Maraden
Armoris Cybersecurity Learning
Anggi Rifa Pradana
Armoris Cybersecurity Learning
Wahyu Sutejo
ARMORIS
JICA

Exercise Design

Real world situation

203.0.113.0/24

Redteam (you)

Attacker

Technical Scenario

DMZ (10.0.16.0/24)

dns(10)

web(11)

fwids (254)

SERVER (10.0.32.0/24)

proxy(10)

file(11)

CLIENT (10.0.64.0/24)

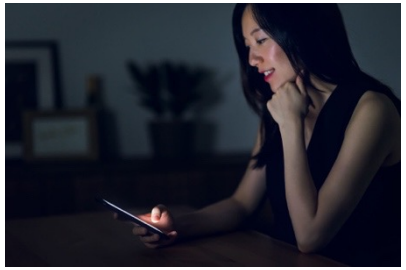
win10(10)

bluetam

Tech

Mgmt

Business Scenario



customer

regulator

police

Top management (or CISO)

Business Scenario

Scenario development example

- Technical
  - Scan
  - SQL Injection
  - Information leakage
  - Attacker publish leaked info to darkweb
- Business
  - Customer contact to company claiming their information is leaked
  - Top management order to Management team to report

Development of technical scenario

- Identify "nice" vulnerability to use
  - By daily vulnearbility research
  - Find PoC code to exploit
- Setup lab environment
- Test PoC code to know how it works
  - Make sure you can analyze (logs/pcap/etc)
- Think about business scenario later

Development of business scenario

- What will happen after "the technical scenario" runs in real world?

- Who will be involved?
  - Internally: CxO, sales, PR, business, marketing, leagal, compliance
  - Externally: Government, police, customer, media, business partner

- What management team people should learn from the exercise?

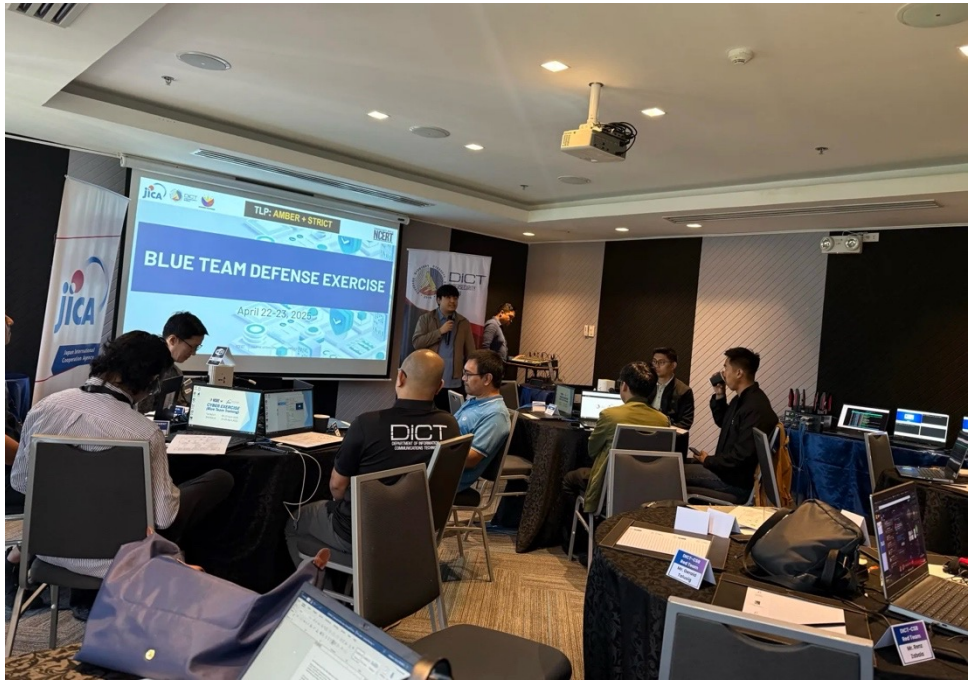
Trainings in each country

Cambodia

Trainers:
Ministry of ICT

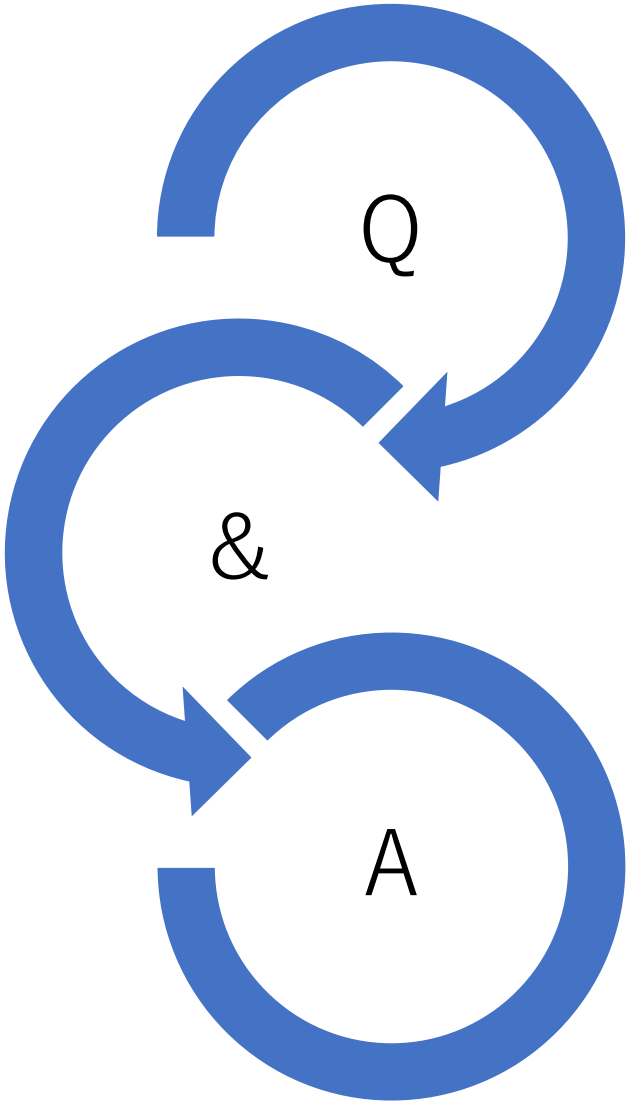
Indonesia
Trainers
University of Indonesia++

Philippines
Trainers:
Department of ICT



Challenges identified

- Leadership dependency & need for multiple trainers
- Limited originality in scenario creation
- Gap between technical and management skills
- Sustainability: maintain Cyber Range & retaining talent


Q
&
A