Strategy for Developing Cybersecurity Workforce in CSTEC

: a Link between Lab-based Training and a Live-Fire Competition

Hanjin Park (Senior Researcher, Ph.D.), Soonjwa Hong (Principal Researcher, Ph.D.)

CSTEC (CyberSecurity Training and Exercise Center)

South Korea
Overview

• Need for cybersecurity workforce is increasing
• CSTEC (CyberSecurity Training and Exercise Center), Oct. 2014 in South Korea
• Two tracks
  • Trainings
    • Technical, Lab-based, Practice with a scenario, Chronological order
  • Exercise
    • CCE (Cyber Conflict Exercise): A live-fire attack-defense competition
• Problem
  • Skill-gap between trainees of Lab-based training and participants of CCE
• Solution
  • Re-design training courses
    • Work role using NICE Cybersecurity Workforce Framework (NCWF)
    • Level
      • Beginner, Intermediate, Advanced
      • Assessment attempt to assess trainees using KSAs unit [Survey]
    • Match the work role and the level between a trainee and a course
Lack of Cybersecurity Workforce

• Need for cybersecurity workforce is increasing

• Global
  • Lack of cybersecurity workforce: 1.8 Million people until 2022 year [1]

• Domestic (South Korea)
  • Lack of cybersecurity workforce: 9,854 people until 2020 year [2]

History of CSTEC

• NISA (National Information Security Academy)
  • 2011, 3.4 DDoS attack, Nonghyup bank network failure
  • 2011, National cybersecurity master plan
  • Awareness trainings
    • basic essentials, knowledge-based, lecture-based, without practice
    • also have a special awareness training for executives (policy makers)

• CSTEC (CyberSecurity Training and Exercise Center)
  • 2013, 3.20 Cyber terror
  • 2013, National cybersecurity comprehensive measures
  • About 1800 Employees in public sector / Year
  • Awareness trainings
    + Lab-based trainings
    + Cyber attack defense competition
Two Tracks

• Trainings
  • Awareness trainings
  • Lab-based trainings
    • Vulnerability scan/Penetration test training
    • Cybersecurity incident response training
      • Web servers
      • Government IT systems
      • ICS/SCADA system
      • Mobile/Wireless system
    • Comprehensive attacks and defense training
      • 20- people, a combination of multiple training contents

• Exercises
  • Cybersecurity attack defense competition (Cyber Conflict Exercise, CCE, Large scale, 200+ people, Live-fire competition, 2016 ~)
Lab-based Trainings

- Virtualized environment
- Instructor makes an attack to VMs or offers VM that is already compromised
- Trainees have to write on report at each step
- Workbook which contains the detail procedures is provided
- Some course contains role-play, some don’t
- 5 steps for cybersecurity incident response
# 5 Steps for Cybersecurity Incident Response

<table>
<thead>
<tr>
<th>5 Steps</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection</td>
<td>Using various cybersecurity defense tools (e.g., IDS alerts, firewall, traffic log) to find cyber attack or to detect abnormal symptoms.</td>
</tr>
<tr>
<td>Initial Measure</td>
<td>Blocking networks from the internet connection, activating temporary service, and collecting data (forensic) from system and networks</td>
</tr>
<tr>
<td>Analysis</td>
<td>Identifying the malicious code and analyzing it statically and dynamically</td>
</tr>
<tr>
<td>Recovery</td>
<td>Removing the malicious code and recovering the system to the normal status</td>
</tr>
<tr>
<td>Security Enhancement</td>
<td>Updating new rules on the cybersecurity defense tools (e.g., IDS, firewall, network access control, MDM) to prevent the future attack that exploits the same vulnerabilities. Updating Anti-Virus with new rules.</td>
</tr>
</tbody>
</table>
CCE: Cyber Conflict Exercise

- Cybersecurity attack-defense exercise with multi-layer networks
- Live-fire, on-line quals and offline finals
  - After quals, select 10 Red teams, 16 Blue teams, (4 people in each team)
- Most participants are experts, 200+ people, 600+ VMs, 20+ Servers

Red team
- Realtime Attack
- Step-by-Step Intrusion (Pivoting)
- Realistic Scenarios

Blue team
- Threat Hunting
- 5-step Response
  1. Detection
  2. Initial Reaction
  3. Analysis
  4. Recovery
  5. Security Enhancement
- Info. Sharing
Skill-gap between Trainees of Course and Participants of Competition

[Limitation 1]
- Trainee’s work role is too general (coarse-grained work role)
  - E.g. Android ransomware response course
    - Work role
      - “IT or Cybersecurity Manager/Officer of Public Sectors (includes governments)”

[Limitation 2]
- There is no pre-test for trainees
  - Trainee’s levels are various

- Mismatched work role / level between trainees and courses

- Let’s see them with an example
  - Android ransomware responses course (which I teach)
Android Ransomware Response Course

- Screenshots and pictures will be encrypted
- The victim downloaded Adobe flash players (malicious app) via 3rd party app market
- 5 steps to response
Step 1: Detection

• Using various cybersecurity defense tools (e.g., IDS alerts, firewall, traffic log) to find cyber attack or to detect abnormal symptoms.
  • Smartphone screen has been locked!
Step2: Initial Measure

- Blocking networks from the internet connection, activating temporary service, and collecting data (forensic) from system and networks
  - Power Off
  - Image backup
    - There are several ways
    - Use ADB (Android Debug Bridge) backup command
Step 3: Analysis

- Identifying the malicious code and analyzing it statically and dynamically
  - Collecting the malicious app
  - Decompile / Dissemble
  - Understand what malicious behaviors are
Step4: Recovery / Step5: Security Enhancement

• Removing the malicious code and recovering the system to the normal status
• Updating new rules on the cybersecurity defense tools (e.g., IDS, firewall, network access control, MDM) to prevent the future attack that exploits the same vulnerabilities. Updating Anti-Virus with new rules.
NICE Cybersecurity Workforce Framework (NCWF)

- 7 Categories, 33 Specialty Area, 52 Work Roles
- 1007 Tasks, 630 Knowledge, 374 Skills, 176 Availability

- 7 Categories
  - Securely Provision
  - Operate and Maintain
  - Oversee and Govern
  - Protect and Defend
  - Analyze
  - Collect and Operate
  - Investigate

- Specialty Area
- Work Role
- Task
- KSAs
# Adopting NCWF to Android Ransomware Response Course

<table>
<thead>
<tr>
<th>5 Steps</th>
<th>Process</th>
<th>Category</th>
<th>Specialty</th>
<th>Work Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection</td>
<td>Using various cybersecurity defense tools (e.g., IDS alerts, firewall, traffic log) to find cyber attack or to detect abnormal symptoms.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initial Measure</td>
<td>Blocking networks from the internet connection, activating temporary service, and collecting data (forensic) from system and networks</td>
<td>Protect and Defend</td>
<td>Incident Response</td>
<td>Cyber Defense Incident Responder [1]</td>
</tr>
<tr>
<td>Analysis</td>
<td>Identifying the malicious code and analyzing it statically and dynamically</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery</td>
<td>Removing the malicious code and recovering the system to the normal status</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Enhancement</td>
<td>Updating new rules on the cybersecurity defense tools (e.g., IDS, firewall, network access control, MDM) to prevent the future attack that exploits the same vulnerabilities. Updating Anti-Virus with new rules.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[1] Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
Various Categories

- Participants of the survey: Android ransomware response course in Nov/26/2018 – Nov/28/11, 14 people

- **Category: Protect and Defend (only 7%)**

  - Securely Provision (SP) 15%
  - Operate and Maintain (OM) 57%
  - Oversee and Govern (OG) 7%
  - Protect and Defend (PD) 7%
  - Collect and Operate (CO) 7%
  - Investigate (IN) 7%
Various Work Roles

- Participants of the survey: Android ransomware response course in Nov/26/2018 – Nov/28/11, 14 people

- Work role: Cyber Defense Incident Response (0%)
Various Levels

- Participants of the survey: Android ransomware response course in Nov/26/2018 – Nov/28/11, 14 people

- Level: Basic (72%), Intermediate (21%), Advanced (7%)
Matching Work Role / Level

• Guideline for Course Enrolment
  • Work role
    • Analyzing the trainee’s work role before he or she enrolled the class using NCWF
    • Notifying specific work roles of the course
  • Level
    • Design three different courses depending on levels
      • Beginner, Intermediate, Advanced
        • In the android ransomware response course,
          • Beginner: A version of no encryption, just move files
          • Intermediate: Encryption key which is in a malicious app
          • Advanced: Never decrypt version (because key had been removed)
    • Pre-test to identify trainee’s level

• How can we assess a trainee’s level?
About Assessment of Trainee’s Level

• [Pilot Study]
  • Course: Android ransomware response course
  • Work role: cyber defense incident role (CIR)
  • Mapping KSAs of CIR to the course
  • Derive the related KSAs from the course
  • Unit assessment of trainees' using the selected KSAs
  • Classify the level according to range of points
## Selected Knowledges

- 10 Knowledge are selected

<table>
<thead>
<tr>
<th>ID</th>
<th>Knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>K0001</td>
<td>Knowledge of computer networking concepts and protocols, and network security methodologies.</td>
</tr>
<tr>
<td>K0005</td>
<td>Knowledge of cyber threats and vulnerabilities.</td>
</tr>
<tr>
<td>K0021</td>
<td>Knowledge of data backup and recovery.</td>
</tr>
<tr>
<td>K0033</td>
<td>Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).</td>
</tr>
<tr>
<td>K0041</td>
<td>Knowledge of incident categories, incident responses, and timelines for responses.</td>
</tr>
<tr>
<td>K0042</td>
<td>Knowledge of incident response and handling methodologies.</td>
</tr>
<tr>
<td>K0046</td>
<td>Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.</td>
</tr>
<tr>
<td>K0070</td>
<td>Knowledge of system and application security threats and vulnerabilities (e.g., malicious code).</td>
</tr>
<tr>
<td>K0259</td>
<td>Knowledge of malware analysis concepts and methodologies.</td>
</tr>
<tr>
<td>K0332</td>
<td>Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.</td>
</tr>
</tbody>
</table>
Selected Availabilities and Skills

- 4 Skills and 1 Ability are selected

<table>
<thead>
<tr>
<th>ID</th>
<th>Skill</th>
</tr>
</thead>
<tbody>
<tr>
<td>S0003</td>
<td>Skill of identifying, capturing, containing, and reporting malware</td>
</tr>
<tr>
<td>S0047</td>
<td>Skill in preserving evidence integrity according to standard operating procedures or national standards.</td>
</tr>
<tr>
<td>S0077</td>
<td>Skill in recognizing and categorizing types of vulnerabilities and associated attacks.</td>
</tr>
<tr>
<td>S0079</td>
<td>Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>Ability</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0128</td>
<td>Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies</td>
</tr>
</tbody>
</table>
Self-Assessment using KSAs

• Self-assessment checking value
  • Select from 0 to 5 for each equation
    • 0: Unexperienced
    • 1: Having Basic knowledge
    • 2: Beginner (Limited experience, Need professionals’ help to do problem solving)
    • 3: Intermediate (Possible to adopt practical usage, Need occasional professionals’ help to do problem solving)
    • 4: Expert (problem solving without external help, subject to be inquired from others)
    • 5: Professionals (certificated professionals)

• Trainee selects one of the five choices
**Results of Self-Assessment (1/2)**

- Android ransomware response course in Nov/26/2018 – Nov/28/11, 14 people
  - One trainee did not answer the KSAs question
  - Two times survey:
    - **Before** taking the course, **After** taking the course

<table>
<thead>
<tr>
<th></th>
<th>K0001</th>
<th>K0005</th>
<th>K0021</th>
<th>K0033</th>
<th>K0041</th>
<th>K0042</th>
<th>K0046</th>
<th>K0070</th>
<th>K0259</th>
<th>K0332</th>
</tr>
</thead>
<tbody>
<tr>
<td>User01</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>User02</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>User03</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>User04</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>User05</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>User06</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>User07</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>User08</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>User09</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>User10</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>User11</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>User12</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>User13</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>
Results of Self-Assessment (2/2)

- Android ransomware response course in Nov/26/2018 – Nov/28/11, 14 people
  - One trainee did not answer the KSAs question
  - Two times survey
  - Before taking the course, After taking the course

<table>
<thead>
<tr>
<th>User</th>
<th>S0003</th>
<th>S0047</th>
<th>S0077</th>
<th>S0079</th>
</tr>
</thead>
<tbody>
<tr>
<td>User01</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>User02</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>User03</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>User04</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>User05</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>User06</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>User07</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>User08</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>User09</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>User10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>User11</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>User12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>User13</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User</th>
<th>S0003</th>
<th>S0047</th>
<th>S0077</th>
<th>S0079</th>
</tr>
</thead>
<tbody>
<tr>
<td>User01</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>User02</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>User03</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>User04</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>User05</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>User06</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>User07</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>User08</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>User09</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>User10</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>User11</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>User12</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>User13</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User</th>
<th>A0128</th>
</tr>
</thead>
<tbody>
<tr>
<td>User01</td>
<td>0</td>
</tr>
<tr>
<td>User02</td>
<td>4</td>
</tr>
<tr>
<td>User03</td>
<td>1</td>
</tr>
<tr>
<td>User04</td>
<td>2</td>
</tr>
<tr>
<td>User05</td>
<td>3</td>
</tr>
<tr>
<td>User06</td>
<td>3</td>
</tr>
<tr>
<td>User07</td>
<td>2</td>
</tr>
<tr>
<td>User08</td>
<td>3</td>
</tr>
<tr>
<td>User09</td>
<td>2</td>
</tr>
<tr>
<td>User10</td>
<td>3</td>
</tr>
<tr>
<td>User11</td>
<td>3</td>
</tr>
<tr>
<td>User12</td>
<td>3</td>
</tr>
<tr>
<td>User13</td>
<td>2</td>
</tr>
</tbody>
</table>
Limitation of Self-Assessment

• An assessment method
  • [Simple math]
    • 15 items (10 Knowledge, 4 Skills, and 1 Ability) with range [0, 5]
    • Summation of checking values
      • Sum in [0, 75] : Possible
      • Sum in [0, 25] ➔ Beginner Level
      • Sum in [25, 50] ➔ Intermediate Level
      • Sum in [50, 75] ➔ Advanced Level

• [Limitation] Since the result of self-assessment is subjective, it is difficult to make range for leveling such as basic, intermediate, advanced

• Assessment of trainees is still open question!

• However, we can see the improvement of trainee after taking this course.
Assessment of a Trainee (Before/After Comparison)

- Android ransomware response course in Nov/26/2018 – Nov/28/11, 14 people
- Before taking the course, After taking the course
- A user
  - User7

![Graph showing before and after assessment results.](image-url)
Future Work

• For level-tests
  • Design pre-test for each course
    • E.g., Unit test using KSAs
    • Classify the trainees as the one of three levels, such as Beginner, Intermediate, Advanced

• Verify and research the effects of this with more trainees
Conclusion

- CSTEC
  - Two tracks
    - Lab-based trainings
    - Cybersecurity attack defense competition

- Skill-gap between participants of Lab-based trainings and competitions
  - Mismatched work role and level between trainees and courses

- Solutions
  - [Case Study] Android ransomware response course
  1. Matching work role between trainees and courses
  2. Matching level between trainees and courses
Thank you

Q&A

hjpark001@nsr.re.kr