Types of Cybersecurity Training in KYPO and Their Visualization

Karolína Dočkalová

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION, YOUTH AND SPORTS

lasaris

MUNI

KYPO

Motivation

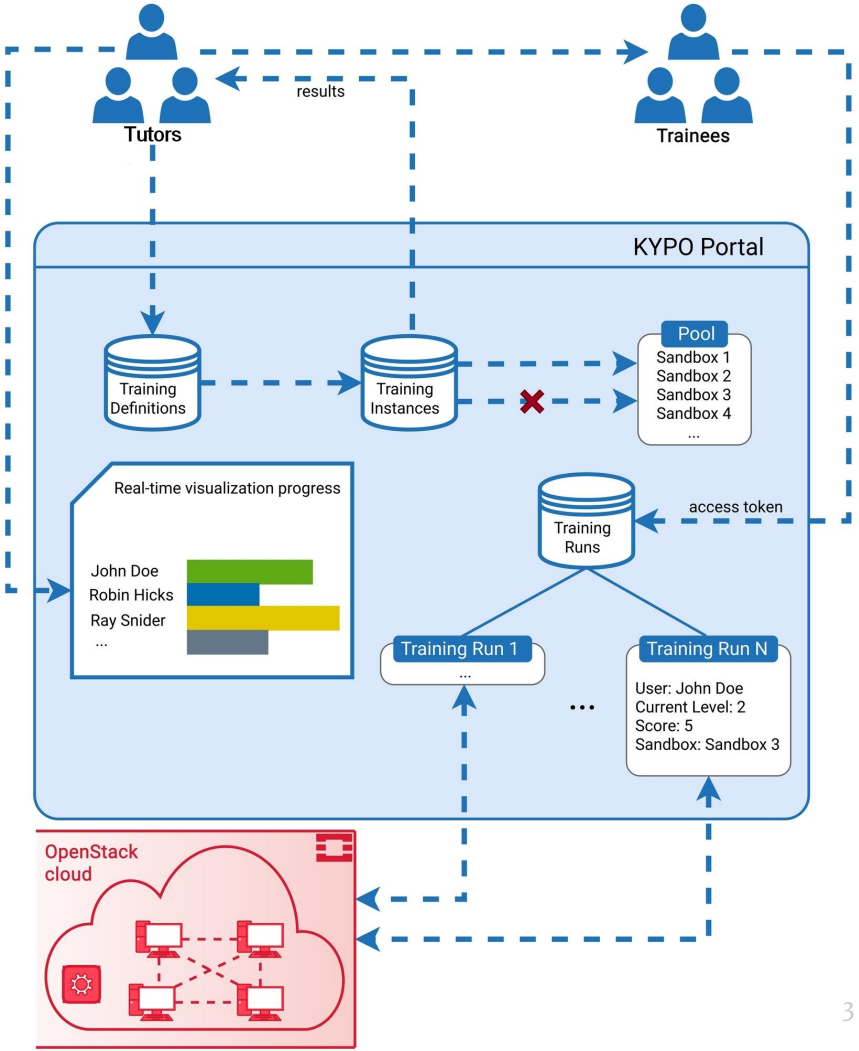
- Insufficient level of people's (professionals or ordinary computer users) skills to prevent or respond to cyber security attacks ->
  - Hands-on exercises
  - Platform to enable safe execution of unusual and potentially harmful actions
- How to increase the impact of those exercises?

What's going on during/after Cybersecurity Training?

- The platform is ready and improving
- How can we see what is going on?
  - Are the exercises even helpful?
  - Too difficult or too easy?
  - Are the tasks well defined?

KYPO Cyber Range

- Open-source cloud-based simulator of computer networks
- Environment for execution of cybernetic attacks in sandboxes
- The cyber range enables us to collect player-specific data regarding individual training runs.
- Different types of hands-on exercises
  - CDX
  - linear or adaptive CtF

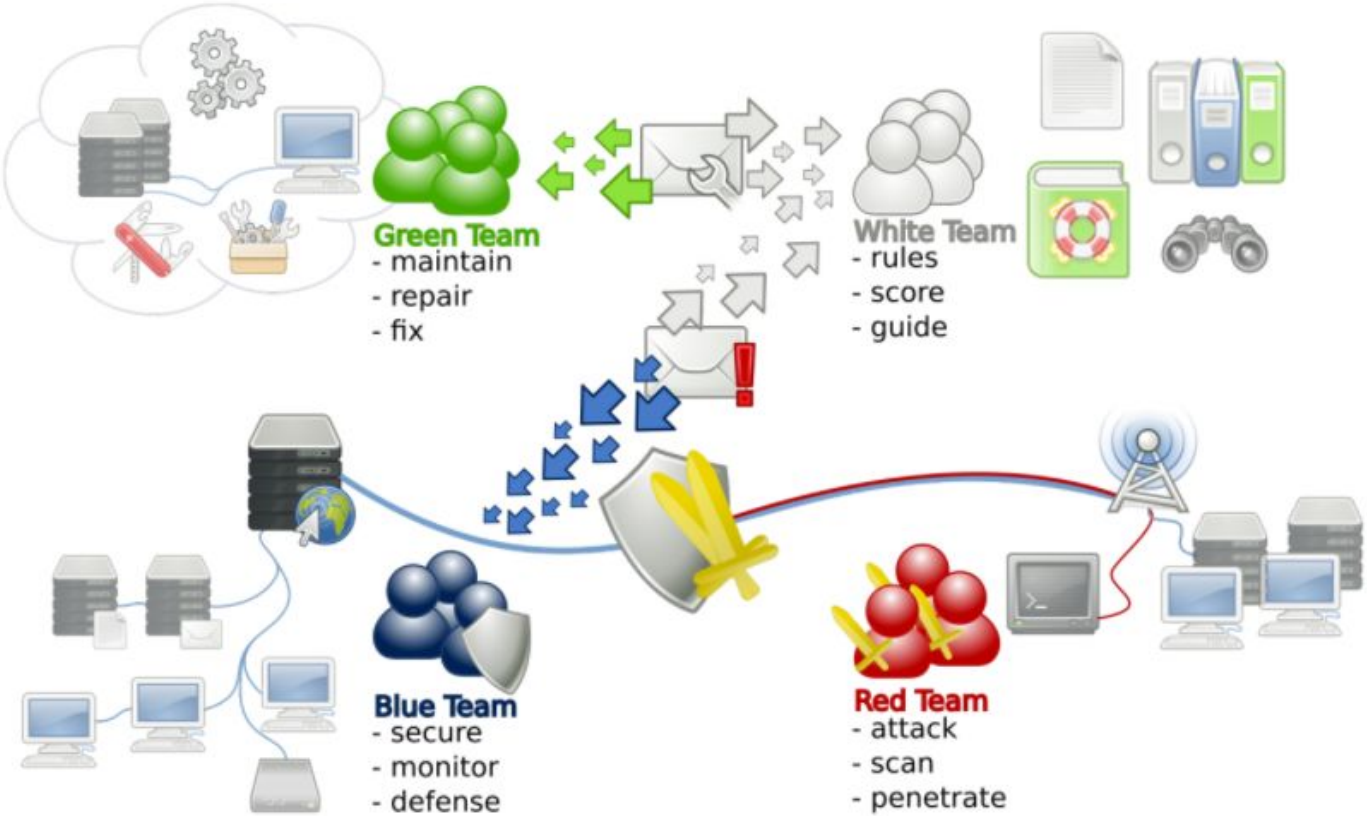


CDX, Cyber Defense Exercises

- Unstructured, step-by-step hands-on training
- To enable participants to experience cyber attacks first-hand with real-life limitations
- Intensive, short-term events lasting several days

A need to gather feedback or training overview for the participants (both organizers and players)

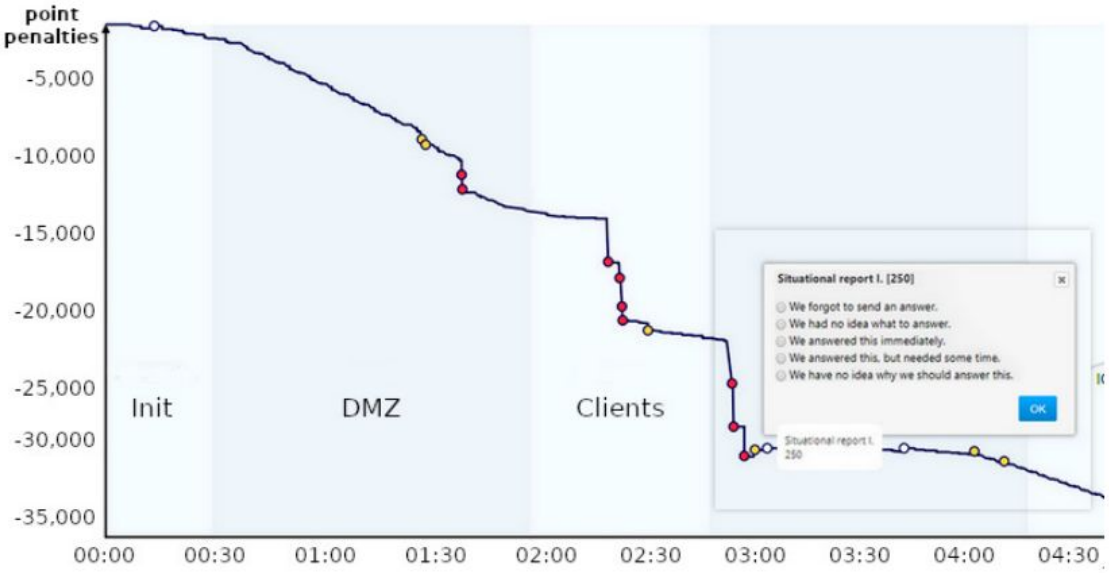
Cyber Defense Exercises – Teams



Post Training Feedback for the Blue Team

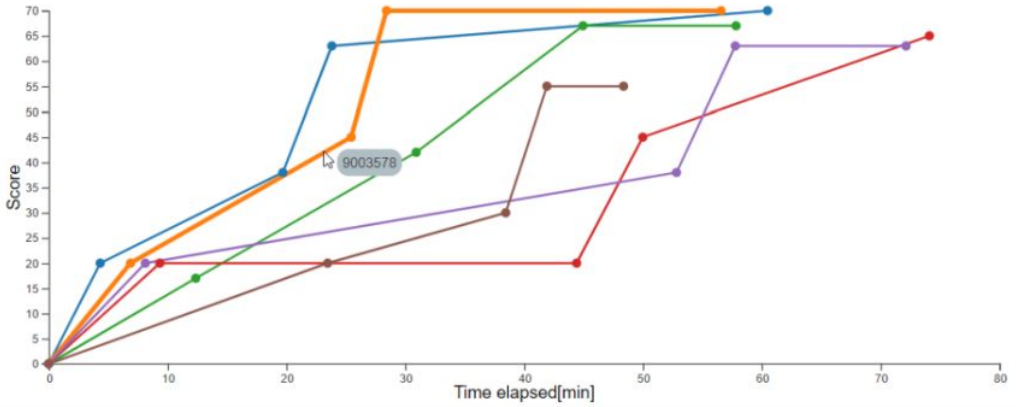
- the players, **defending** the prepared network against hackers
- during exercise, they should have **no information** regarding what is going on -> real-life conditions
- right after the exercise – an ideal time to give them **fast feedback**

Order	Phase	Duration	Day
1	Exercise familirization	3 hrs	1
2	Actual exercise	6 hrs	2
3	Post-exercise survey	5 mins	2
4	Break	25 mins	2
5	Scoring timeline interaction	10 mins	2
6	Scoring timeline survey	5 mins	2
7	Quick exercise debriefing	15 mins	2

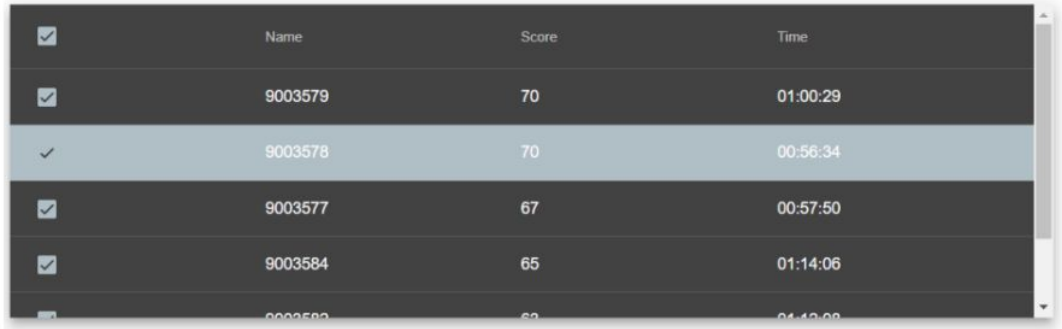


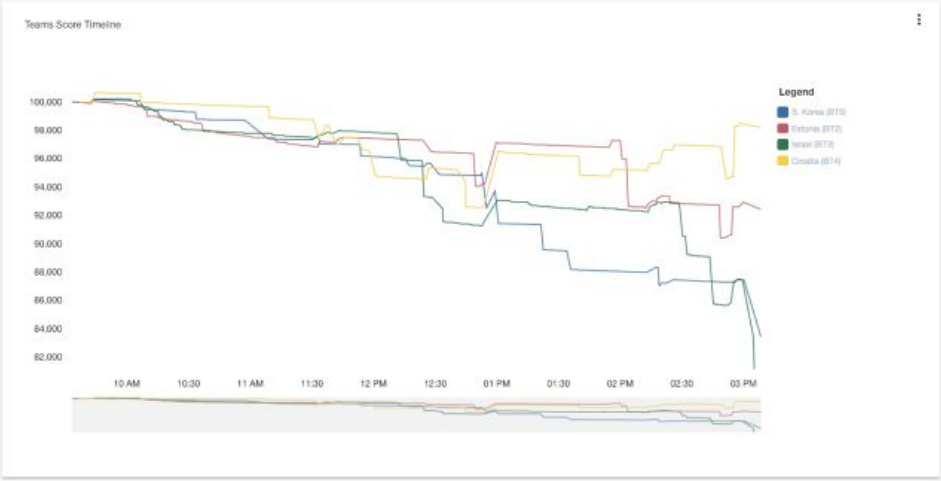
Post Training Feedback for the Blue Team

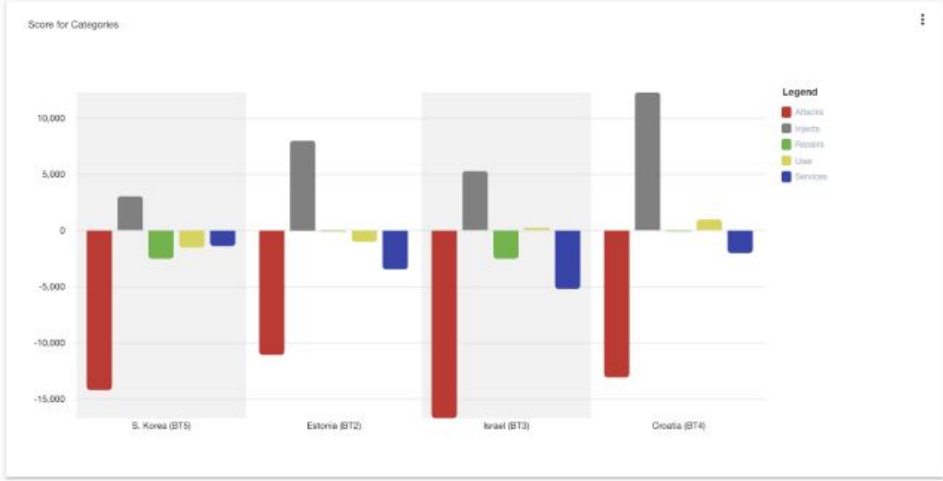
- the players, **defending** the prepared network against hackers
- during exercise, they should have **no information** regarding what is going on -> real-life conditions
- right after the exercise – an ideal time to give them **fast feedback**

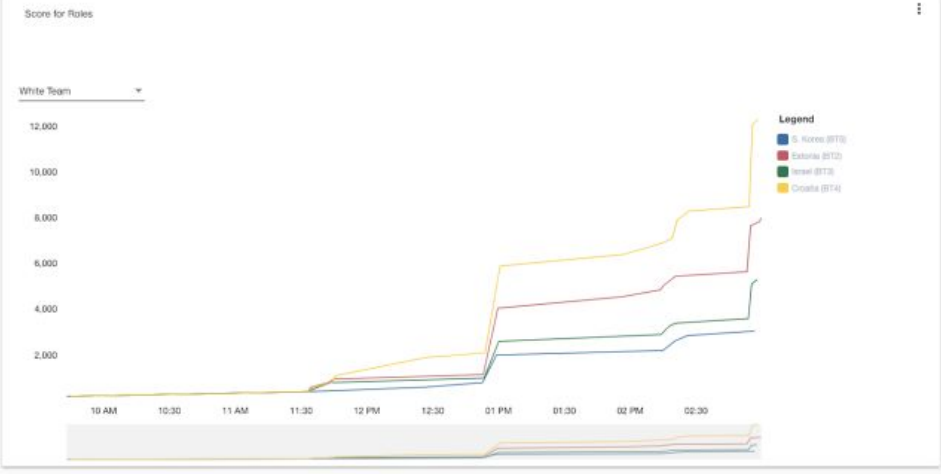


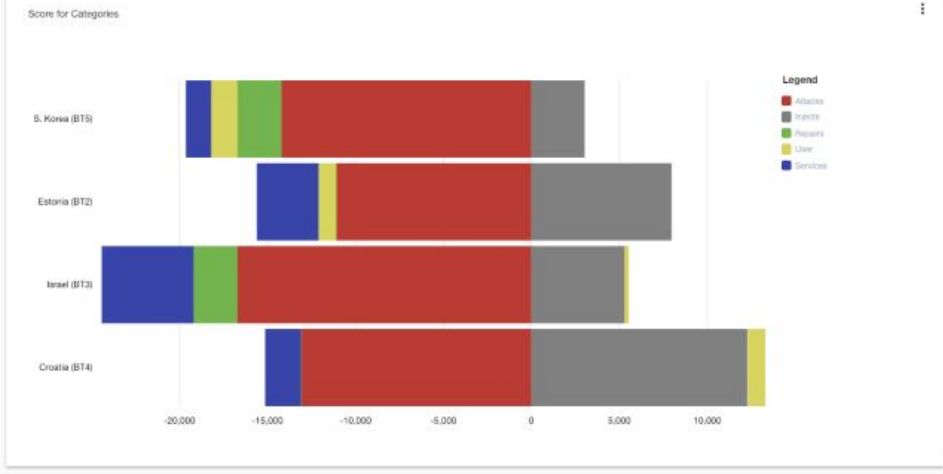
Order	Phase	Duration	Day
1	Exercise familirization	3 hrs	1
2	Actual exercise	6 hrs	2
3	Post-exercise survey	5 mins	2
4	Break	25 mins	2
5	Scoring timeline interaction	10 mins	2
6	Scoring timeline survey	5 mins	2
7	Quick exercise debriefing	15 mins	2




Teams Score Timeline
100,000
98,000
96,000
94,000
92,000
90,000
88,000
86,000
84,000
82,000
10 AM
10:30
11 AM
11:30
12 PM
12:30
01 PM
01:30
02 PM
02:30
03 PM
Legend
S. Korea (BT5)
Estonia (BT2)
Israel (BT3)
Croatia (BT4)


Score for Categories
10,000
5,000
0
-5,000
-10,000
-15,000
S. Korea (BT5)
Estonia (BT2)
Israel (BT3)
Croatia (BT4)
Legend
Attacks
Injects
Repairs
User
Services

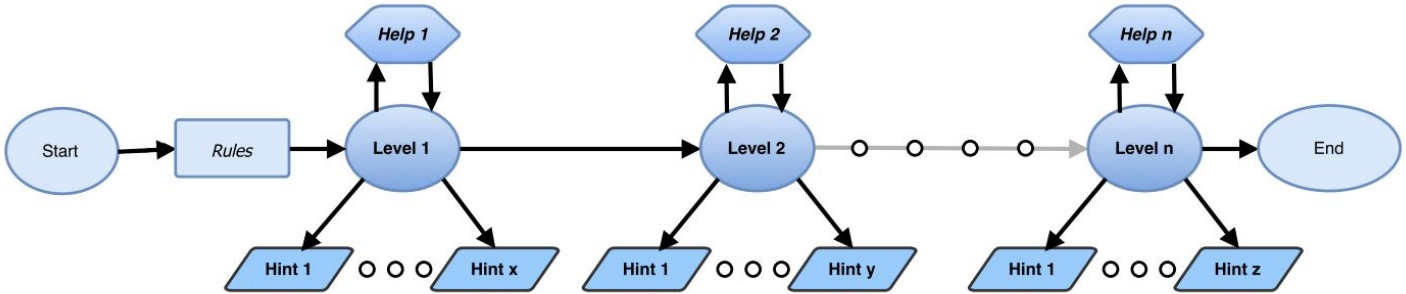

Score for Roles
White Team
12,000
10,000
8,000
6,000
4,000
2,000
10 AM
10:30
11 AM
11:30
12 PM
12:30
01 PM
01:30
02 PM
02:30
Legend
S. Korea (BT5)
Estonia (BT2)
Israel (BT3)
Croatia (BT4)


Score for Categories
S. Korea (BT5)
Estonia (BT2)
Israel (BT3)
Croatia (BT4)
-20,000
-15,000
-10,000
-5,000
0
5,000
10,000
Legend
Attacks
Injects
Repairs
User
Services

Analysis for CDX Organizers

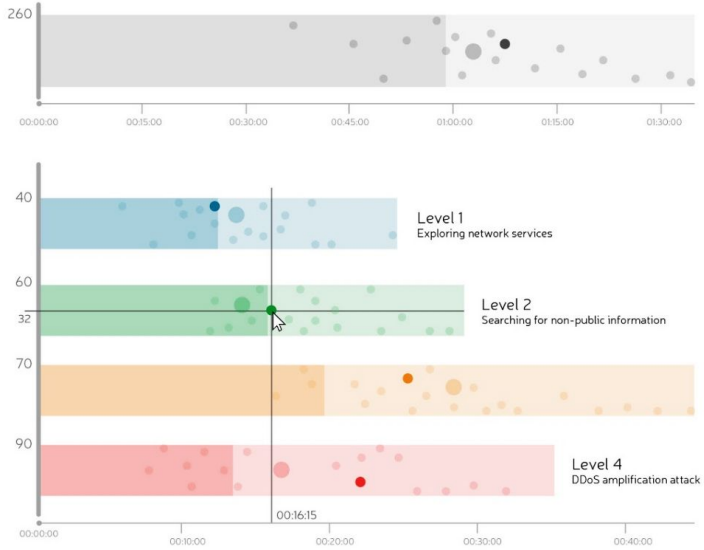
CtF, Capture the Flag Games

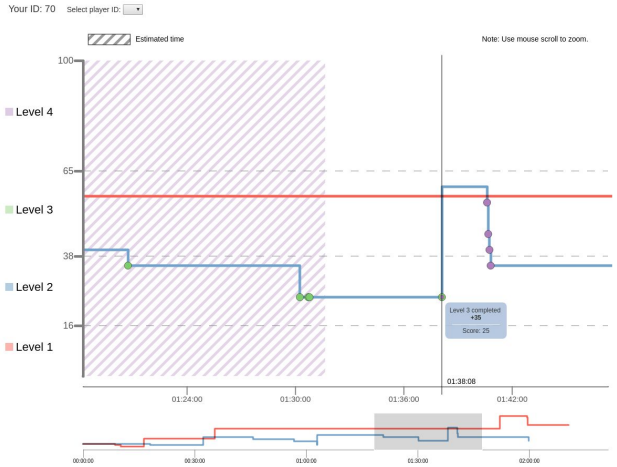
- Hands-on education-oriented cybersecurity games
- The players fulfill individual tasks and receive or lose points according their progress
- A tutor is present to oversee the game and help the players



CtF – Feedback for Players

- Simple and straightforward
- Show the players their results in a competition

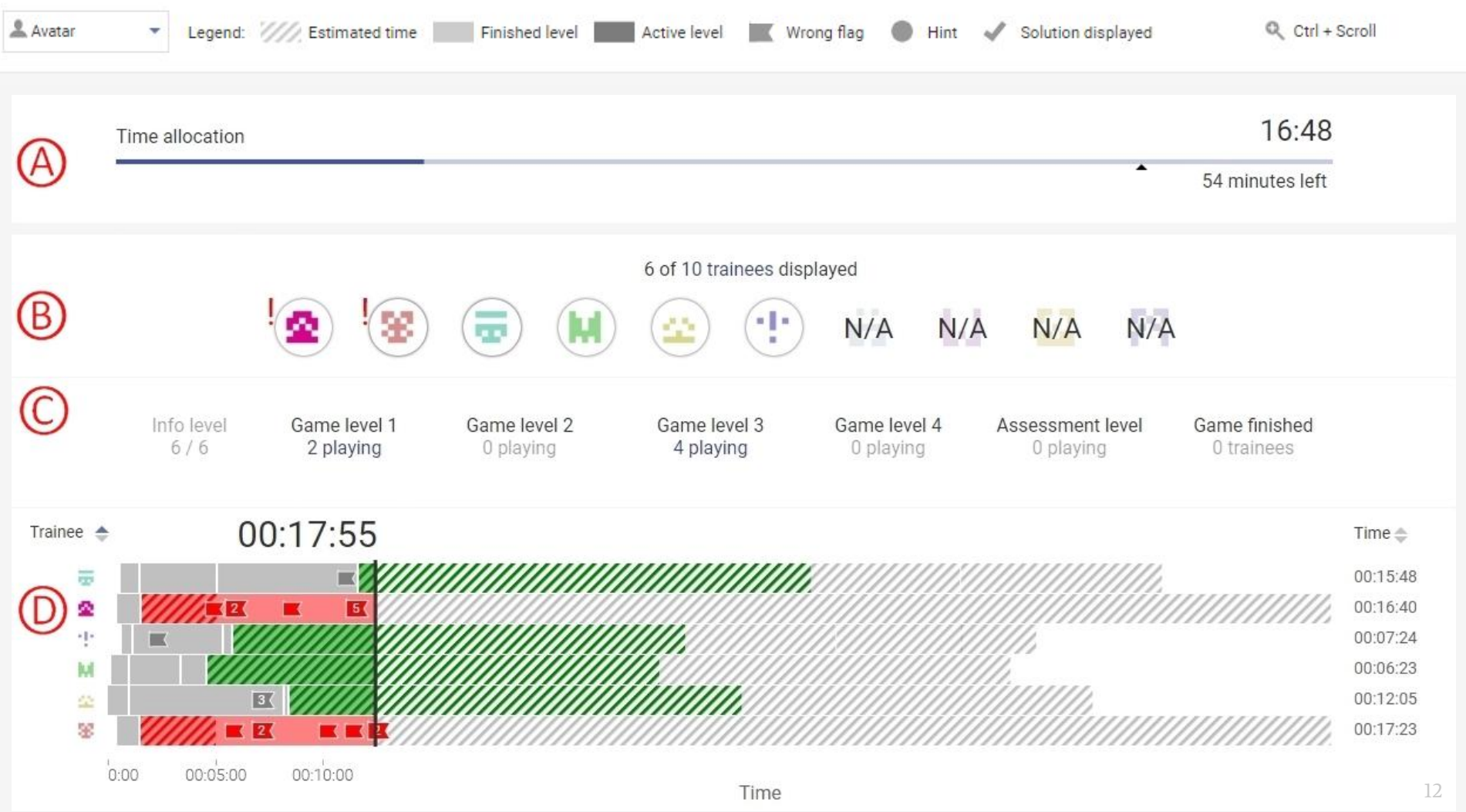




Player	Level 1 Score ↑ / Wrong / Hint	Level 2 Score / Wrong / Hint	Level 3 Score / Wrong / Hint	Level 4 Score / Wrong / Hint	Final Score
82	16 / 0 / 0	22 / 3 / 0	0 / 0 / 0	-	38
74	16 / 0 / 0	22 / 3 / 0	27 / 1 / 1	35 / 0 / 0	100
85	16 / 2 / 0	15 / 1 / 1	27 / 0 / 1	0 / 0 / 0	58
92	16 / 0 / 0	22 / 0 / 0	-	-	38
72	16 / 0 / 0	22 / 0 / 0	17 / 0 / 3	35 / 0 / 0	90
91	16 / 1 / 0	22 / 3 / 0	27 / 0 / 0	35 / 0 / 0	100
80	16 / 0 / 0	22 / 0 / 0	12 / 4 / 4	35 / 0 / 0	85
81	16 / 1 / 0	22 / 0 / 0	-	-	38
93	16 / 0 / 0	10 / 1 / 2	17 / 0 / 3	35 / 0 / 0	78
79	16 / 0 / 0	22 / 0 / 0	12 / 1 / 4	20 / 0 / 2	70
90	16 / 0 / 0	22 / 0 / 0	12 / 3 / 4	35 / 0 / 0	85
76	16 / 0 / 0	22 / 0 / 0	27 / 1 / 0	35 / 1 / 0	100
75	16 / 0 / 0	22 / 0 / 0	12 / 0 / 2	10 / 1 / 4	60
71	13 / 2 / 1	0 / 12 / 2	12 / 0 / 4	0 / 4 / 4	25
78	8 / 3 / 2	10 / 3 / 2	-	-	18
70	8 / 1 / 2	22 / 1 / 0	27 / 0 / 2	10 / 0 / 4	67
84	0 / 1 / 2	15 / 0 / 1	12 / 0 / 4	20 / 0 / 2	47
73	0 / 22 / 2	0 / 4 / 2	0 / 0 / 4	0 / 0 / 4	0

Event filters

- Correct flags
- Wrong flags
- Hints taken
- Level skips


Avatar
Legend:
Estimated time
Finished level
Active level
Wrong flag
Hint
Solution displayed
Ctrl + Scroll
A
Time allocation
16:48
54 minutes left
B
6 of 10 trainees displayed
N/A
N/A
N/A
N/A
C
Info level
6 / 6
Game level 1
2 playing
Game level 2
0 playing
Game level 3
4 playing
Game level 4
0 playing
Assessment level
0 playing
Game finished
0 trainees
Trainee
00:17:55
Time
D
00:15:48
00:16:40
00:07:24
00:06:23
00:12:05
00:17:23
0:00
00:05:00
00:10:00
Time

Player 4

00:16:36 (~ 6 minutes behind)

in 2. level, Find the Vulnerable SSH Server

Used 3 of 3 hints:

How to find out CVE
9 minutes ago

Name of the SSH lib
11 minutes ago

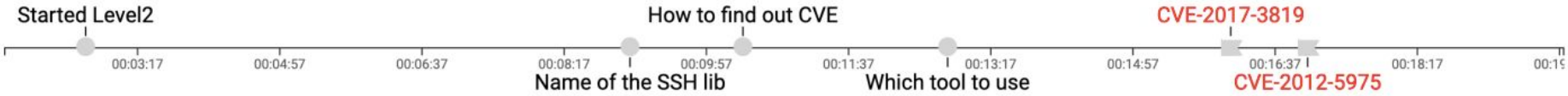
Which tool to use
7 minutes ago

CVE-2018-10933
(correct flag)

CVE-2017-3819
1x
4 minutes ago

CVE-2012-5975
1x
3 minutes ago

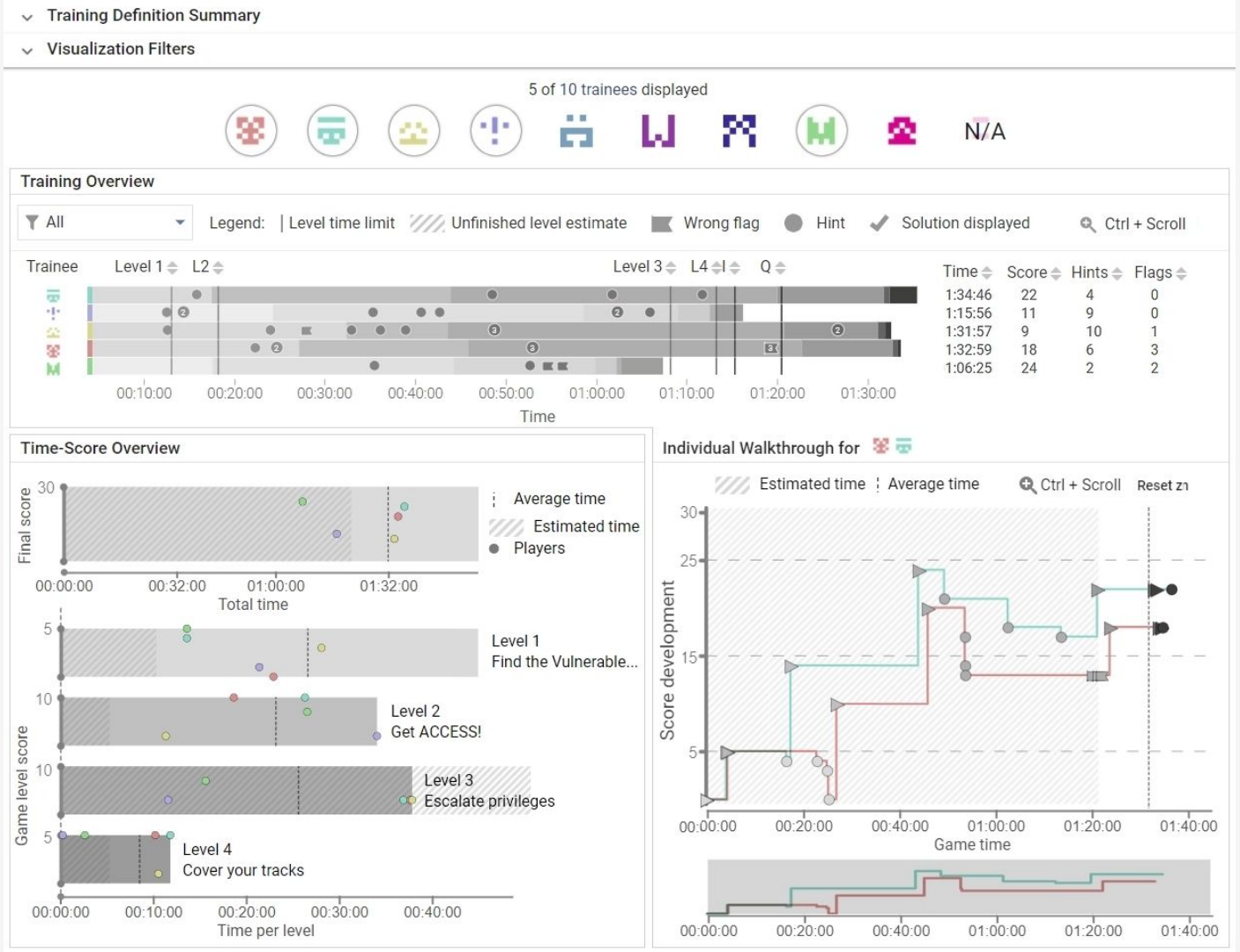
Detailed timeline



Command timeline

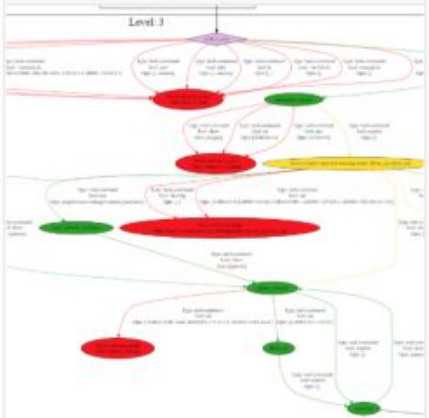
Post-training tool

- For organizers
- Interactive view of trainee actions
- Further developed



Capture the Flag Games – Commands Processing

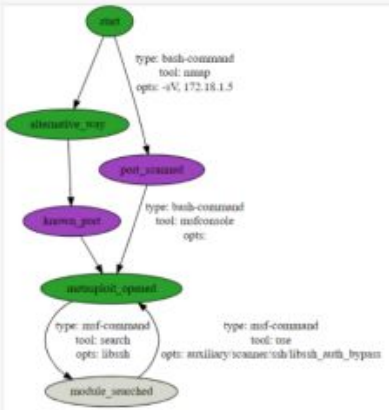
Trainee Graph



State diagram, unique for every trainee, provides granularity per level

Show me

Reference Graph



State diagram showing reference solution of training

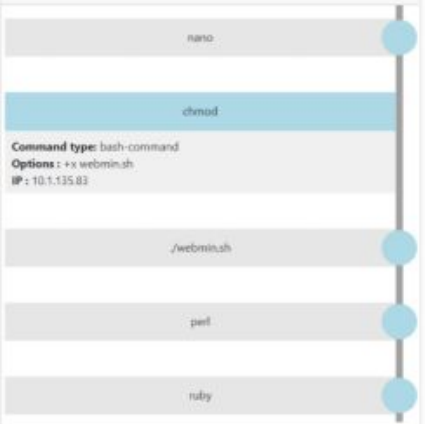
Show me

Command Analysis

Shows syntax and semantic mistakes in commands and their frequencies

Show me

Timeline

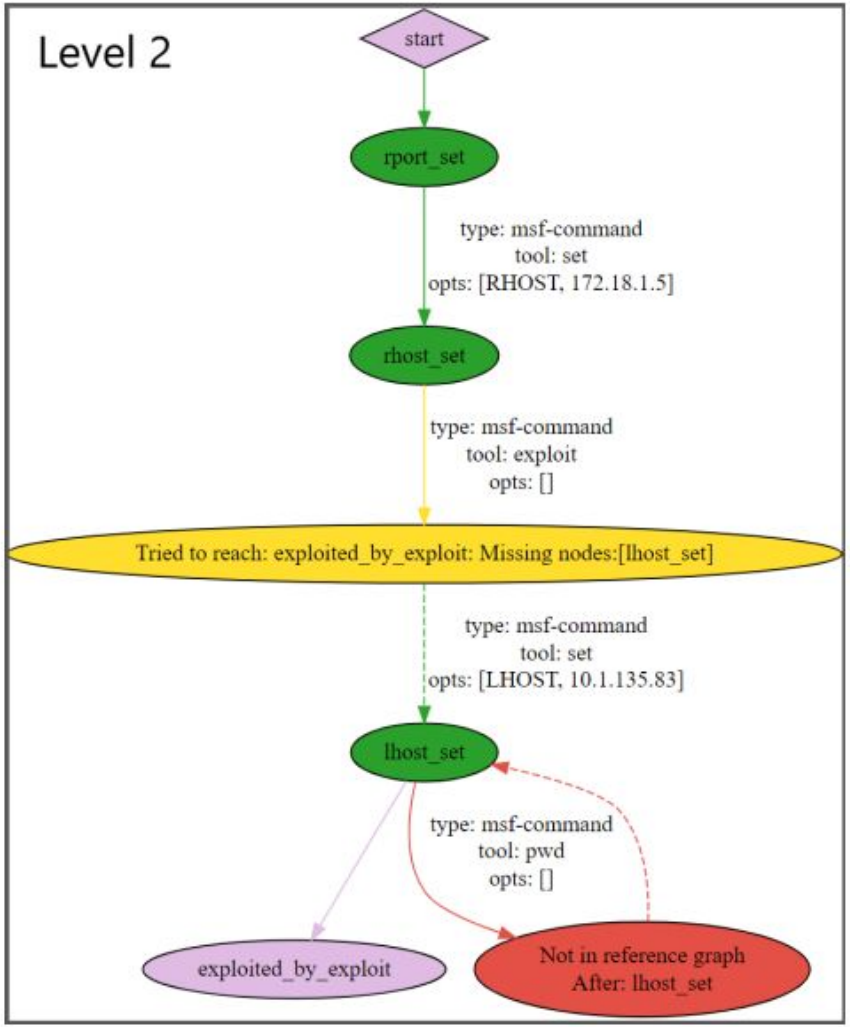


Interactive timeline of submitted commands and their details

Show me

Capture the Flag Games Commands Processing

- Graph for one individual level of a single player

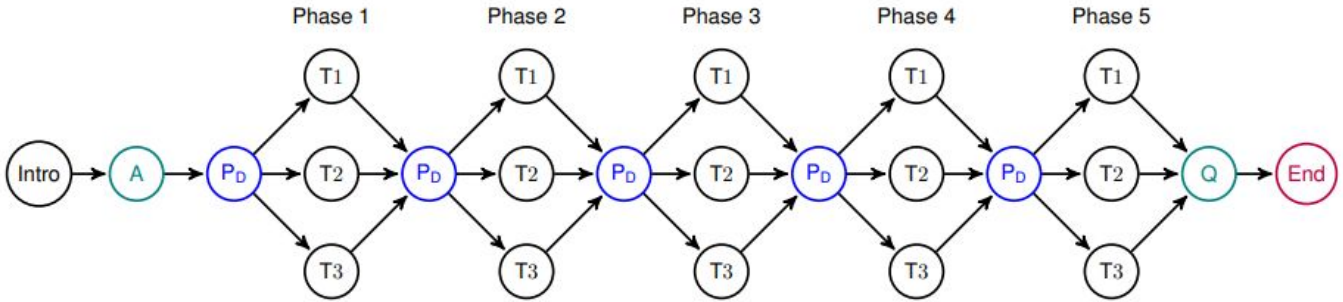


Post-training Dashboard Across Multiple Instances

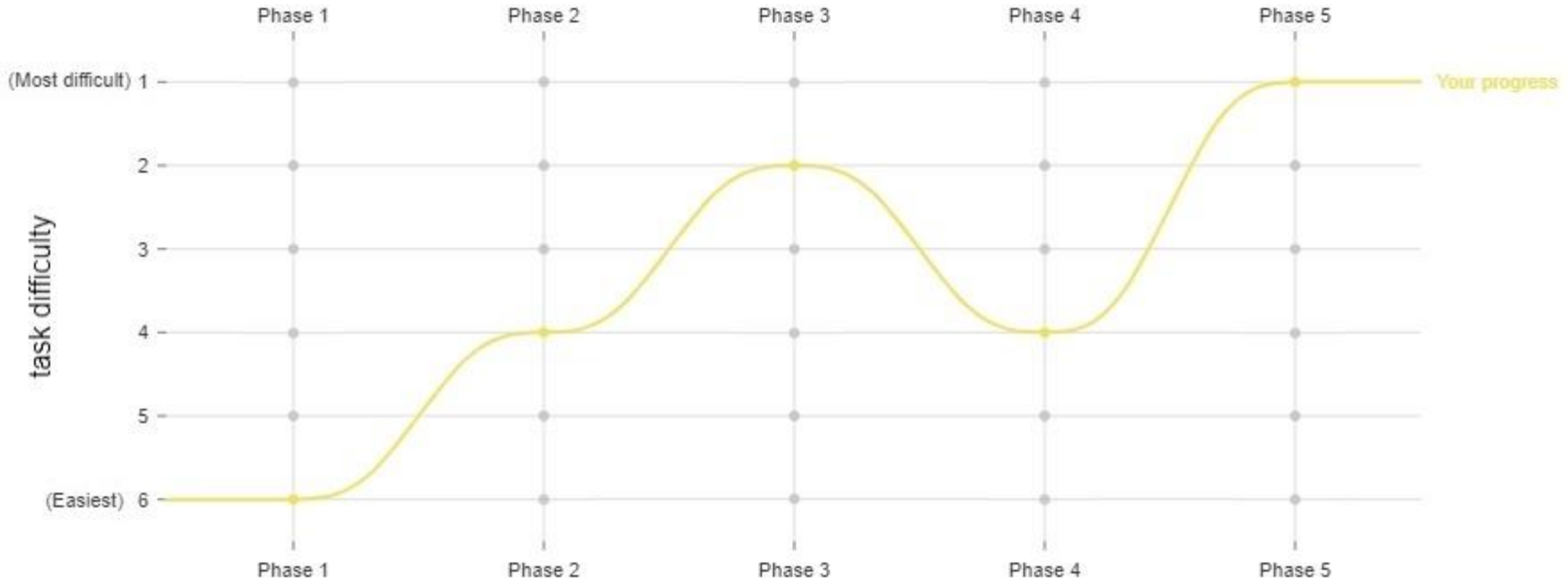
- Not for just single game, but for a whole definition (scenario)
- Statistical views to compare player actions and results
- To help see in a large scale and find patterns or improper parameter settings.

Adaptive Capture the Flag Games

- Consist of several phases, each with tasks of **various difficulty**
- The game itself determines how well the players perform and adjusts its difficulty individually per player
- Uses a decision matrix to compute the difficulty



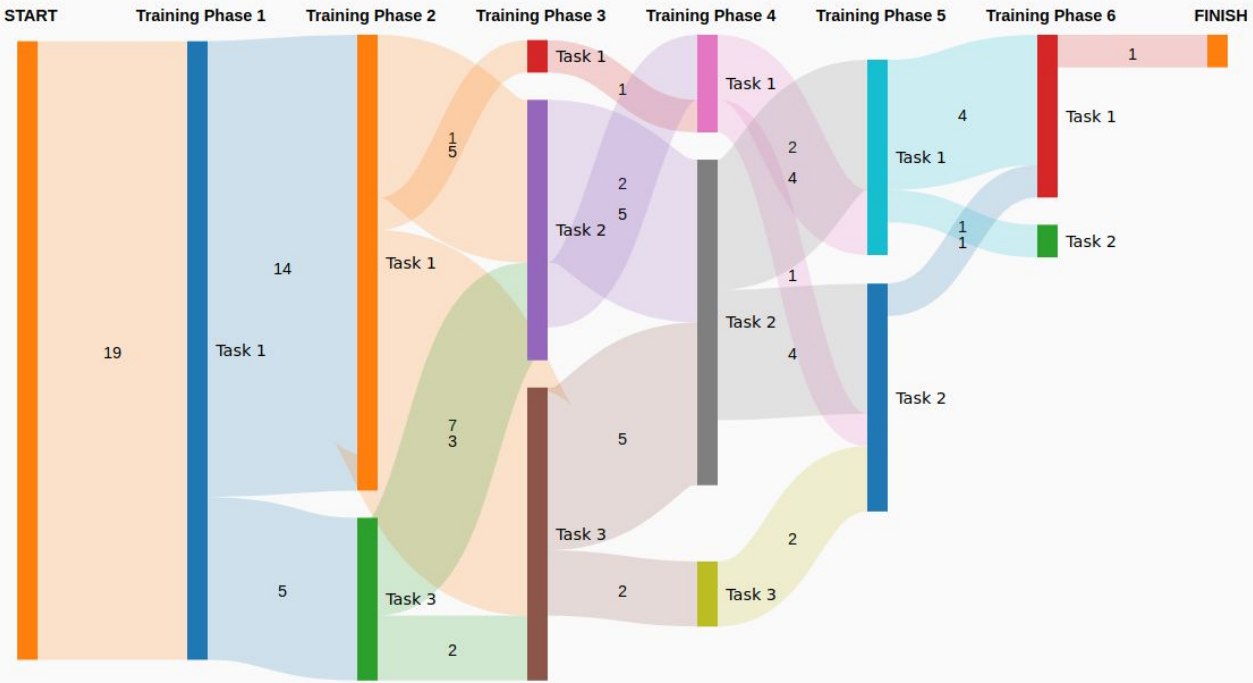
Adaptive CtF with pre-training assessment (A), decision component (PD) applying the proposed model, and a post-training questionnaire (Q). This training contains five phases. Each contains one base task (T1) and two variant tasks (T2, T3).



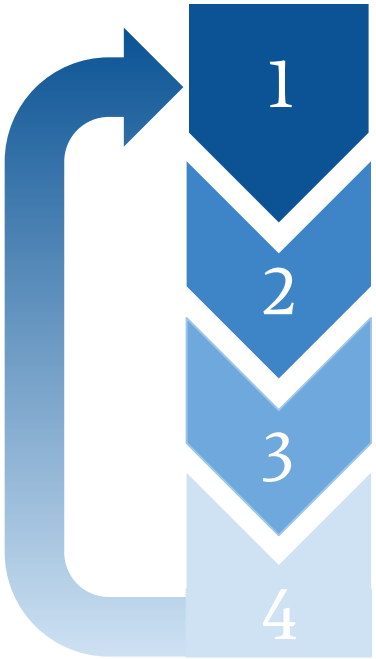
To see the content of individual tasks, click on the corresponding dots in the visualization

Results of Junior Hacker Training

Participants' Transitions Between Phases



Next Steps



Conduct experiments.

a. Currently, adaptive CtF visualizations and behavioral analysis graphs.
b. Qualitative evaluations with organizers, field tests at best (if possible…)

Publish the results.

Refactor/extend the visualizations based on new remarks and evaluation feedback.

Repeat.

Lasaris Seminar PV226, Fall 2021

Any questions?

lasaris