LESSONS LEARNED FROM KYPO–CYBER EXERCISE & RESEARCH PLATFORM PROJECT

SPI 2015

Wednesday 20th May, 2015

Jakub Čegan
Martin Vizváry
cegan@ics.muni.cz

KYPO
BY CSIRT-MU

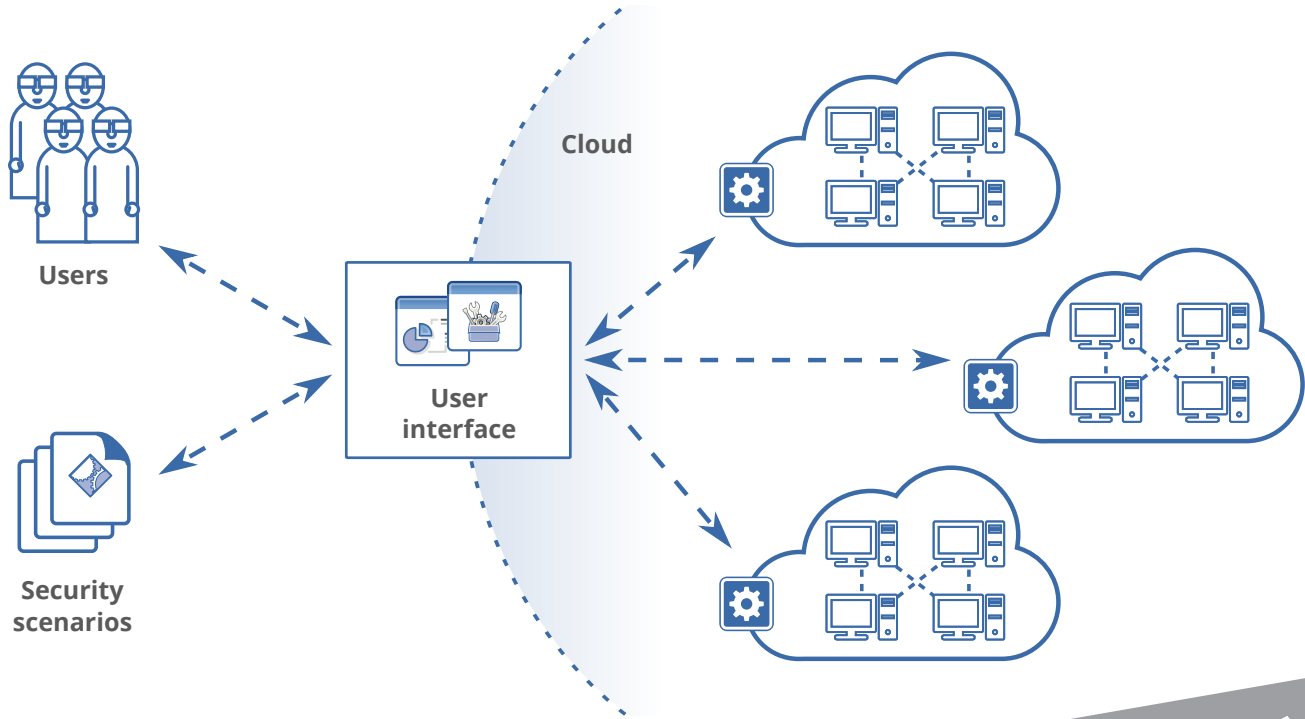
KYPO – Cyber Exercise & Research Platform

- Follows three use cases – Security Training and Exercises, Cyber Research and Development, and Forensics Analysis.
- Built on top of a common cloud provided as a IaaS.
- Uses advanced visualization and integrated monitoring.

KYPO
BY CSIRT-MU

KYPO Architecture & Implementation

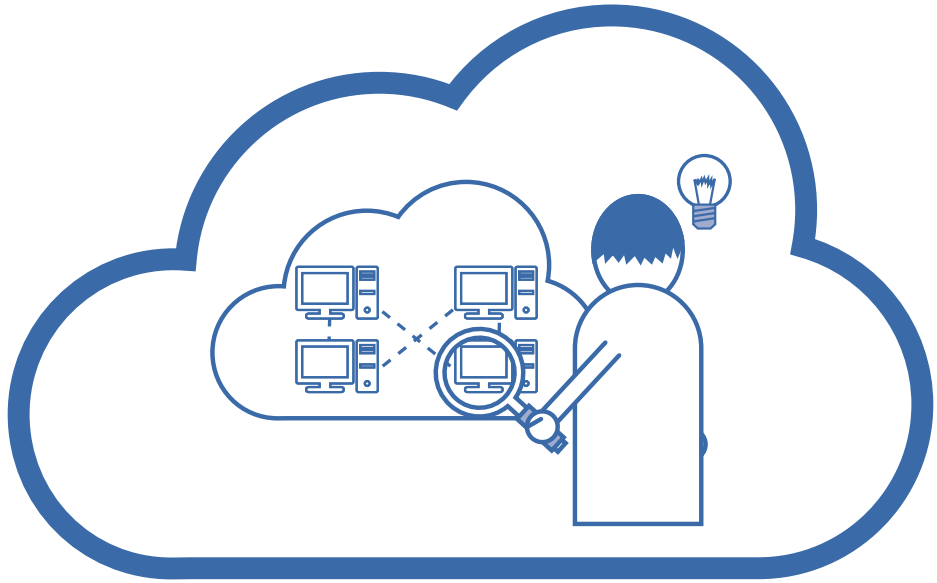
- Implemented in a cloud operated by Masaryk University and the Czech National Research and Education Network (CESNET).
- Interfaces use a REST-base architecture and JSON format to deploy and modify sandboxes.



KYPO
BY CSIRT-MU

Cyber Research & Development

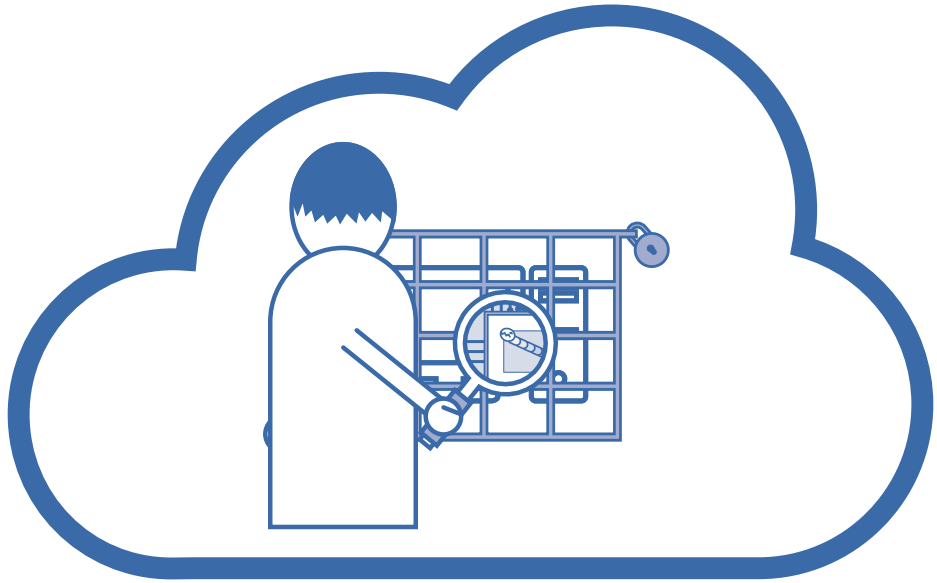
- Provides monitoring using NetFlow and packet capture (pcap).
- Data is stored for further analysis or fast replay of experiment.
- Sandbox design makes experiments easily repeatable.



KYPO
BY CSIRT-MU

Forensics Analysis & Network Simulations

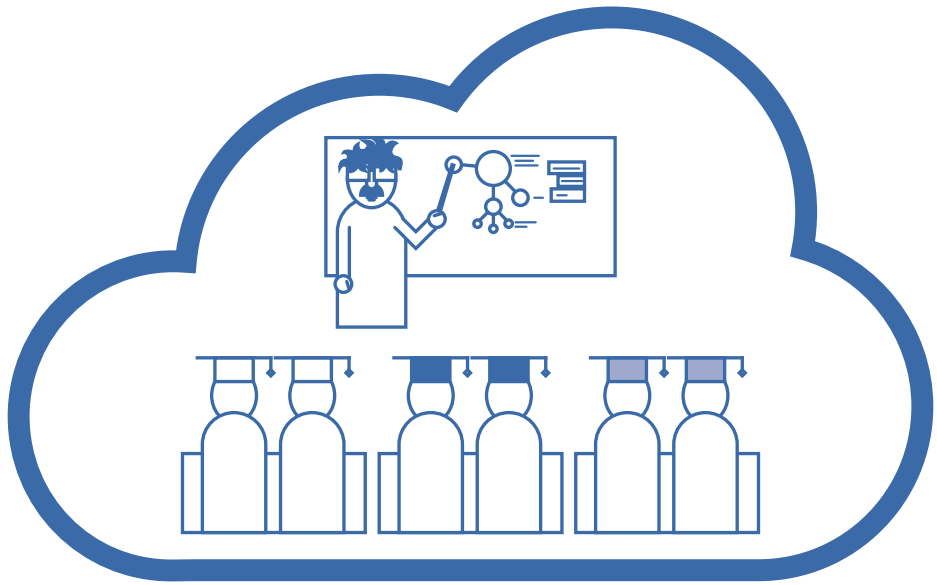
- Adjustments of the sandbox according to malware actions.
- Malware is kept in a safe isolated environment.
- Various tools can be used during the analysis in the sandbox.



KYPO
BY CSIRT-MU

Security Training & Exercises

- Covering skills needed by both users and ICT administrators.
- Main advantages are high rate of interactivity, built-in monitoring, and remote access to all computers for a lecturer.



KYPO
BY CSIRT-MU

Training & Exercise Use Case Evaluation

Training Scenario Description

- Focused on teaching of basics techniques of penetration testing of computer network and its services.
- Contains four levels with increasing difficulty.
- For correct solution of each level player gains score.

Participants

- Participants came from different organizations and have various sets of skills in area of ICT and especially a computer security.
- For our purposes are participants split into three groups defined by skills (beginners, experienced, and advanced users).

Evaluation & Experience

- Average scoring is between 431-538 points (600 points max).
- Average game time is between 89-45 minutes.
- Average level difficulties are (0 – very easy; 5 – extremely hard):

	Level 1	Level 2	Level 3	Level 4
Beginners	1	3	2	3
Experienced	0	2	2	3
Advanced	0	1	1	2

- Surprisingly second level is considered as a second most difficult level in the game.
- The last level discovered unexpected fact that users are too dependent on an interactive shell.

Lessons Learned

- Always group similar advanced users into same groups.
- Advanced user in group of beginners can finish too early and he will get bored.
- Beginner in group of advanced people will be frustrated from his relatively slow progress.
- Users, especially experienced and advanced ones, do not read information, manuals, and texts in game.
- Advanced users can find unintentional vulnerabilities and try to use them to complete game levels.
- Unfamiliar operating systems and other unexpected things can confuse an inexperienced lecturer.

Future Work

- Implementation of more cost-effective simulation of critical information infrastructures.
- Development of more advanced tools for cyber security trainings and exercises management, execution, and evaluation.
- Implementation of remote attendance on trainings and exercises and remote communication.
- Development of tool for remote connection of physical piece of hardware to KYPO environment.

THANK YOU FOR YOUR ATTENTION!

www.kypo.cz

@csirtmu

Jakub Čegan

cegan@ics.muni.cz

UNIVERSITAS MASARYKIANA BRUNENSIS

ÚVT

CSIRT-MU