Lessons Learned From Complex Hands-on Defence Exercises in a Cyber Range

Frontiers in Education 2017

October 21, 2017

Jan Vykopal
Masaryk University, Brno

KYPO
BY CSIRT-MU

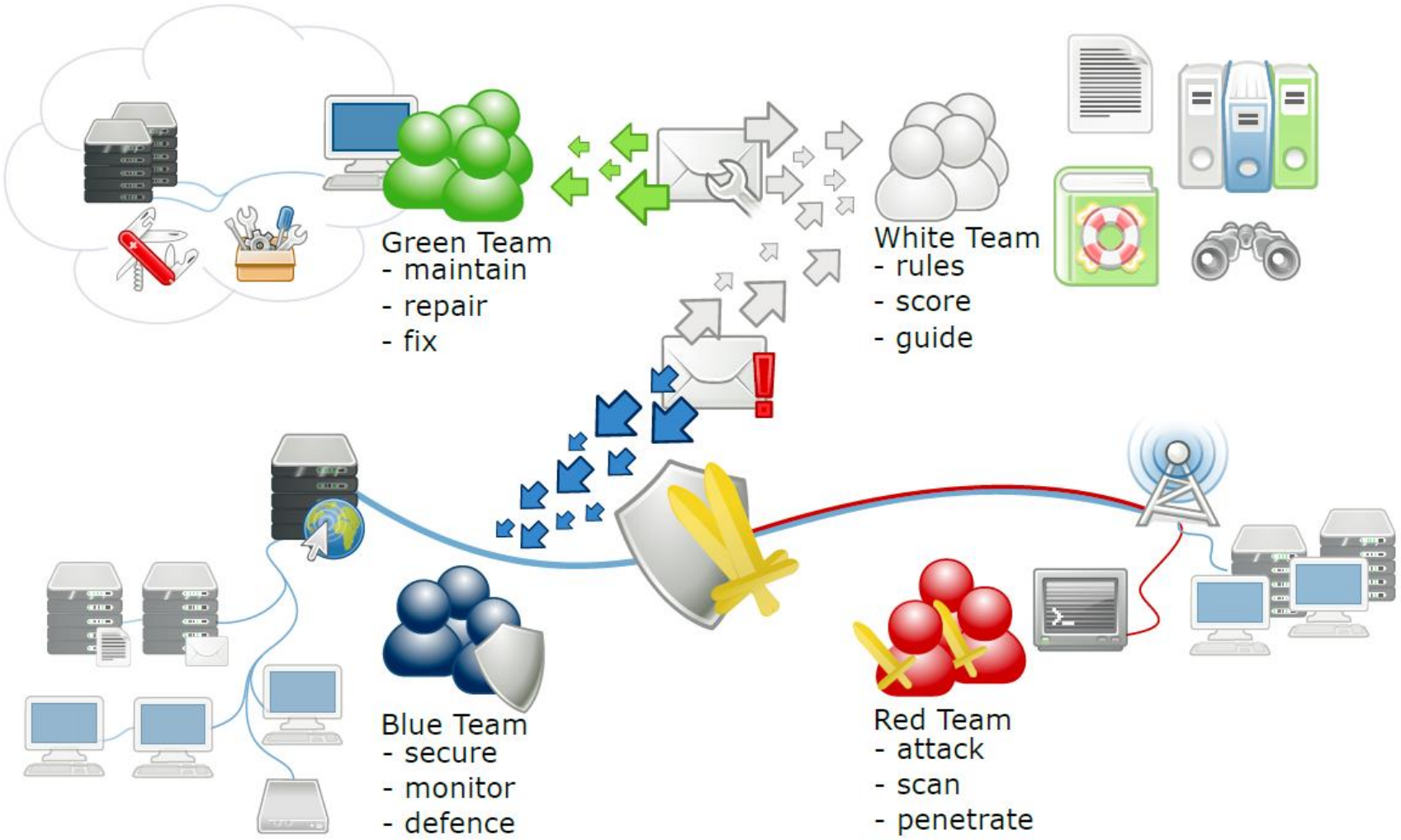
Who am I?

- Post-doc researcher with KYPO – academic cloud-based cyber range.
- Ph.D. graduate in flow-based intrusion detection.
- Founder and head of a certified university operational security team.
- Coordinator and designer of hands-on training session at KYPO platform.

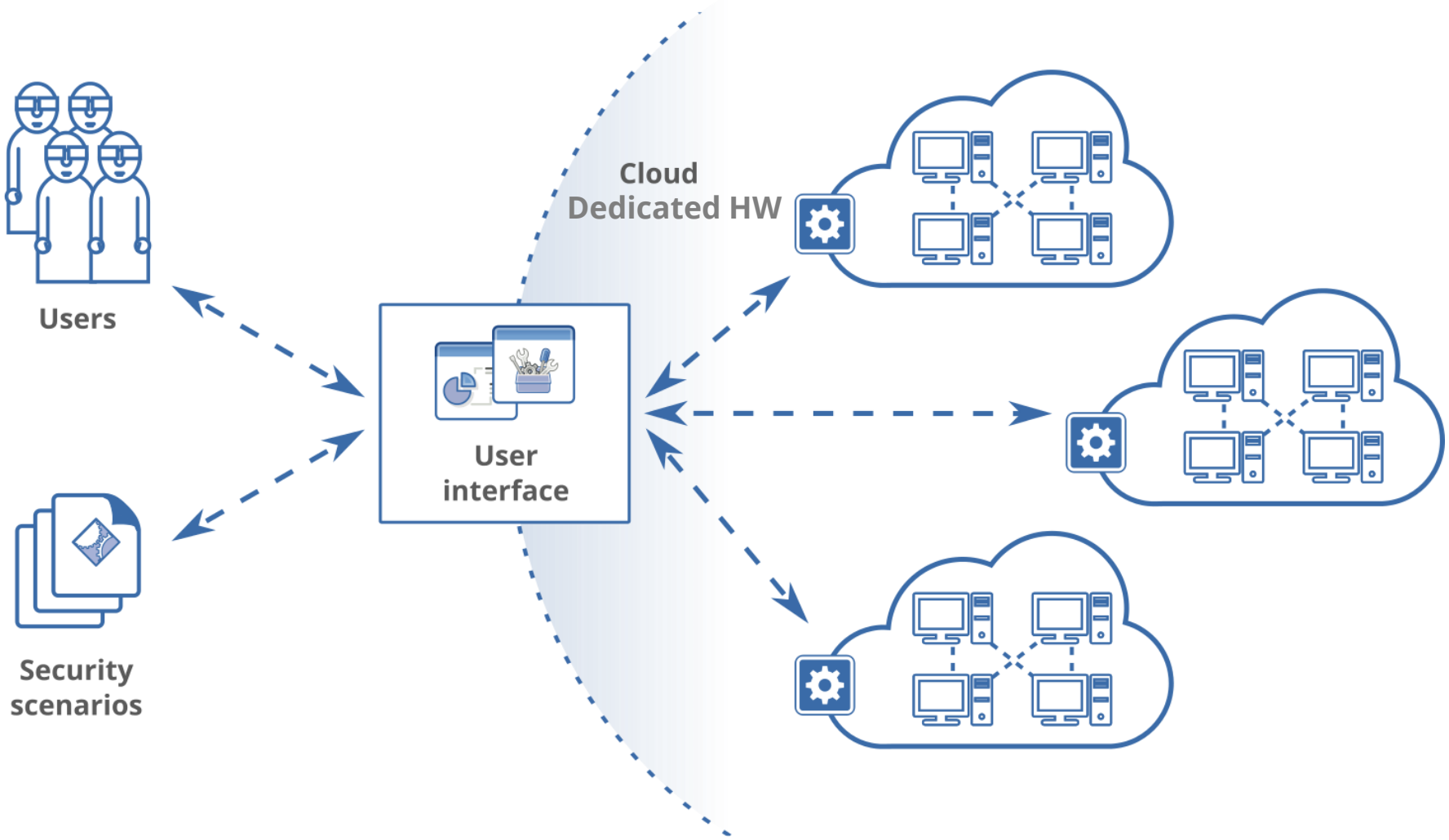
Outline

- Red vs. Blue team exercise format
  - Who is who – team roles
  - Cyber range
- Defence exercise in a cyber range
- Exercise lifecycle – from preparation to evaluation and repetition
- Lessons learned – different viewpoints:
  - Learners
  - Exercise content
  - Exercise infrastructure
- Conclusion and future work

Red vs. Blue team exercise format

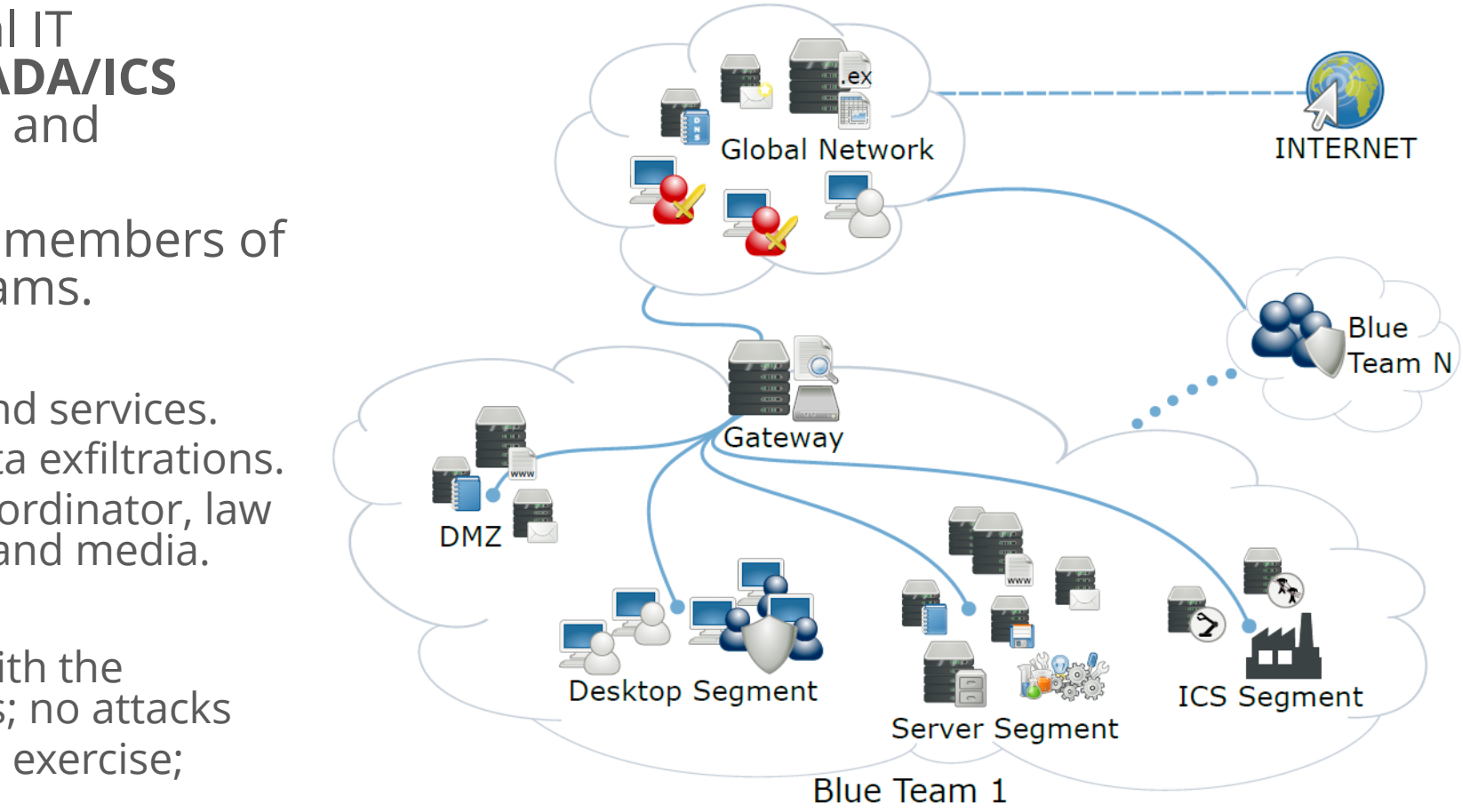


Cyber range


Cloud
Dedicated HW
Users
User
interface
Security
scenarios

Example of a defence exercise in a cyber range

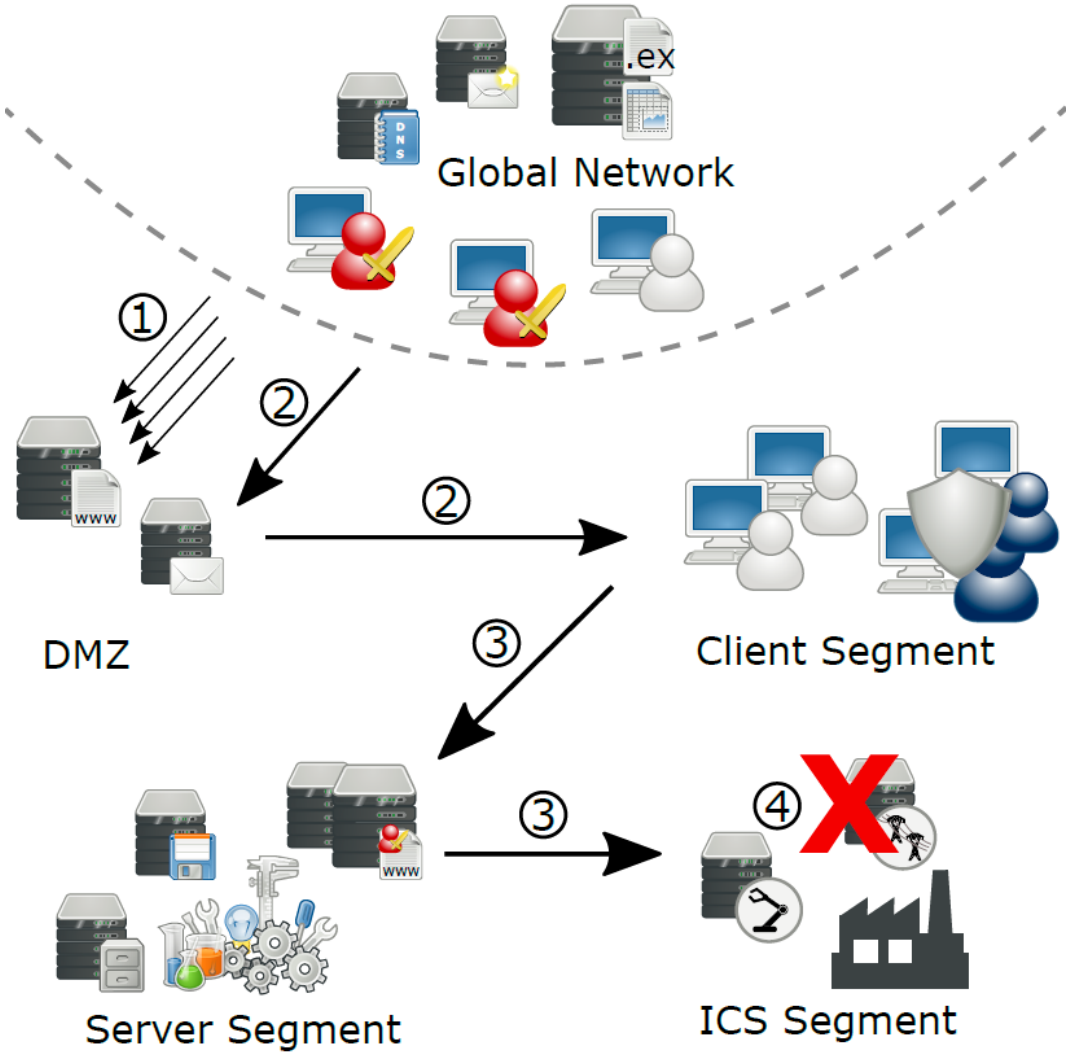
- Topic: defending critical IT infrastructure with **SCADA/ICS** systems against skilled and coordinated attackers
- Learners play a role of members of emergency security teams.
- Their tasks:
  - Secure their network and services.
  - Investigate possible data exfiltrations.
  - Collaborate with the coordinator, law enforcement agencies and media.
- Schedule:
  - Day 1 – familirization with the infrastructure and rules; no attacks
  - Day 2 – actual intensive exercise; no breaks



Exercise scenario

Follows common attack phases:

1. reconnaissance the victim's network
2. exploitation of the unveiled vulnerabilities
3. escalation of privileges on compromised computers and further exploitation
4. completing attackers' mission (e. g., shutdown a control system)



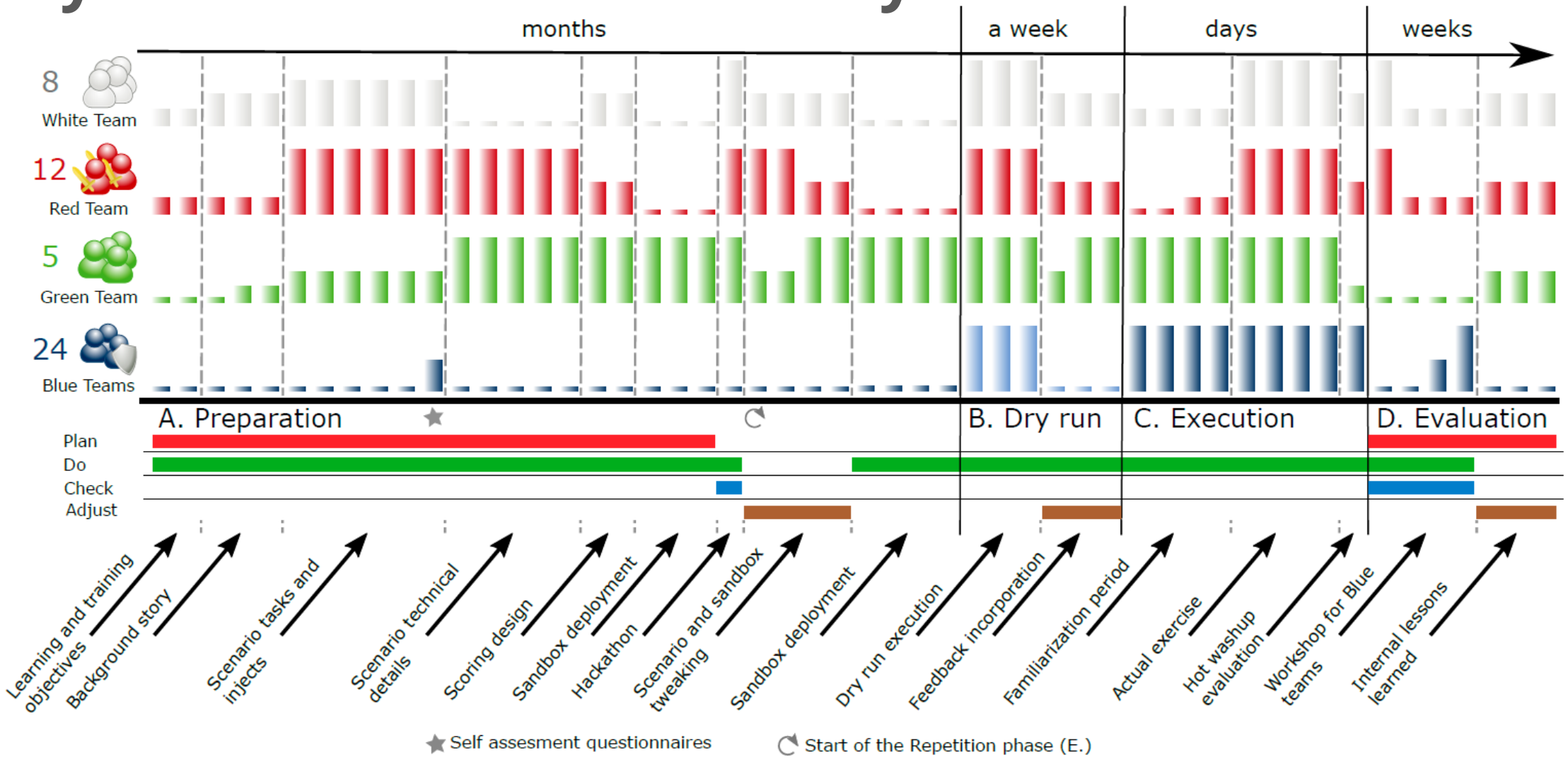
General requirements for a cyber range

- One **sandbox** for each team with exercise network interconnecting all virtual hosts that have to be defended by learners.

- **Monitoring and logging system**
  - Each host in the sandbox sends logs to the central server for further analysis.
  - State of the host's network services is periodically checked and logged.

- **Scoring system**
  - Provides instant feedback to participants during exercise.
  - Penalty and award points are computed automatically from events processed by the logging infrastructure or entered manually.

Cyber defence exercise lifecycle



Lessons learned - preparation

- **Setting learning objectives with respect to the expected readiness of prospective learners**
  - Organizers have limited information about learners' skills before the exercise.
  - Ask for self-assessment or taking part in a test before the exercise.

- **Creating balanced teams**
  - If some learners are experts in one area, distribute them to all teams equally and complement them with experts in another area.

- **Sandbox configuration documents**
  - Continually update specification of systems, network and vulnerabilities.
  - Do not use static documentation, but automation tool such as Ansible.

Lessons learned – dry run

- **Adjusting the scoring system based on the dry run might be misleading**
  - Expertise and size of the Blue teams participating in the dry run may be different.
  - Think about various conditions and events that may not happen in the execution.

Lessons learned – execution I

- **Level of guidance by organizers**
  - Provide some hints to keep learners in flow and not to get frustrated.
  - The guidance should be provided to all teams equally to preserve fair play.

- **Exercise situational awareness for learners**
  - Might be contradictory to the aim and nature of cyber defence exercise.
  - Provide only a basic indication of the learners' performance by displaying a real-time total score of all teams on a shared scoreboard.
  - It also fuels participants with stress as well as a competitive mood.

Lessons learned – execution II

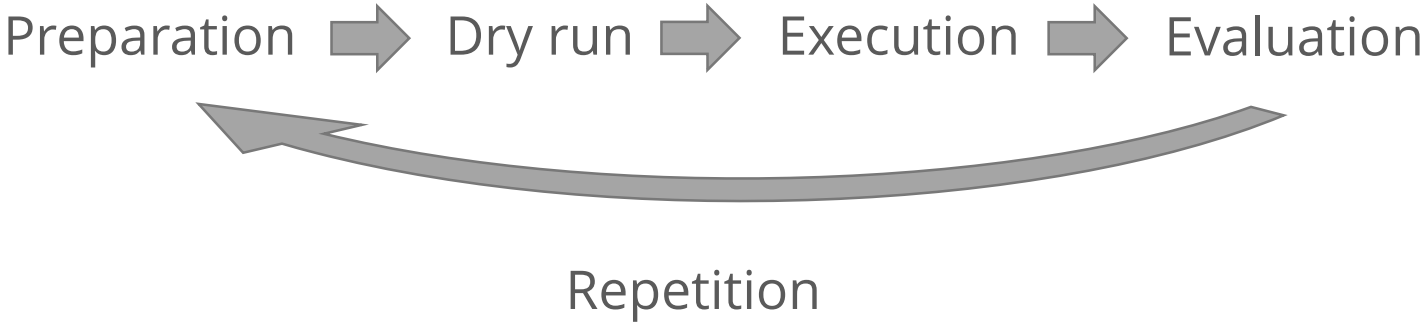
- **Exercise situational awareness for organizers**
  - Familirization period: monitoring the infrastructure enables the White team to provide hints for Blue teams if they unintentionally misconfigure their services.
  - Actual exercise: White team needs to know if some event reported by the Blue teams is a part of the exercise or outage of the infrastructure (cyber range).
- **Automation of the attacks and injects**
  - A need for semi-automated routines that execute attacks and injects in predefined order (=> master's thesis).
  - A need for a generator of network traffic that can emulate typical users.
- **Service access to the exercise's infrastructure**
  - Clearly define what is it and how to distinguish it from a ordinary traffic and attacks by Red team.

Lesson learned - evaluation

- **Ask learners what they want to know**
  - Prepare a questionnaire that is distributed before the evaluation workshop and tailor the content based on their input.
- **Learning also happens in this phase**
  - Evaluation workshop reveals the exercise scenario and timeline from the perspective of the Red and White team.
  - The only opportunity when the learners can authoritatively learn about attacks.
  - Provide a hand-out with best practices that might be useful in the daily routine.

Conclusions

Exercise lifecycle



Each phase brought several lessons from educational and technical perspectives.

Follow-up work - two papers accepted for SIGCSE 2018**:**

- Prerequisite testing of cybersecurity skills
- Timely feedback to learners (just after the exercise)

QUESTIONS?

THANKS FOR YOUR ATTENTION!

www.kypo.cz

@csirtmu

Jan Vykopal

vykopal@ics.muni.cz

KYPO
BY CSIRT-MU