



Evaluation of Cyber Defense Exercises Using Visual Analytics Process

Radek Ošlejšek, Jan Vykopal, **Karolína Burská**, and Vít Rusňák

IEEE Frontier in Education Conference, San Jose, USA, 2018





KYPO Cyber Range

Cloud-based “simulator” of computer networks

So powerful that we can organize *cyber defense exercises, CDXs*

- Extreme use case
- Comprehensive training for IT professionals
- Realism, difficulty (2 days), work under stress, ...
- Protection of complex critical infrastructure by Blue teams
- Escalated attacks of a Red team

... but the preparation and organization is a nightmare :-)

Cyber Defense Exercises – Current Problems

New scenarios are designed from scratch

- No transfer of knowledge and experience between (changing) organizers

The lack of situational awareness

- Monitoring the infrastructure, providing insight, ...

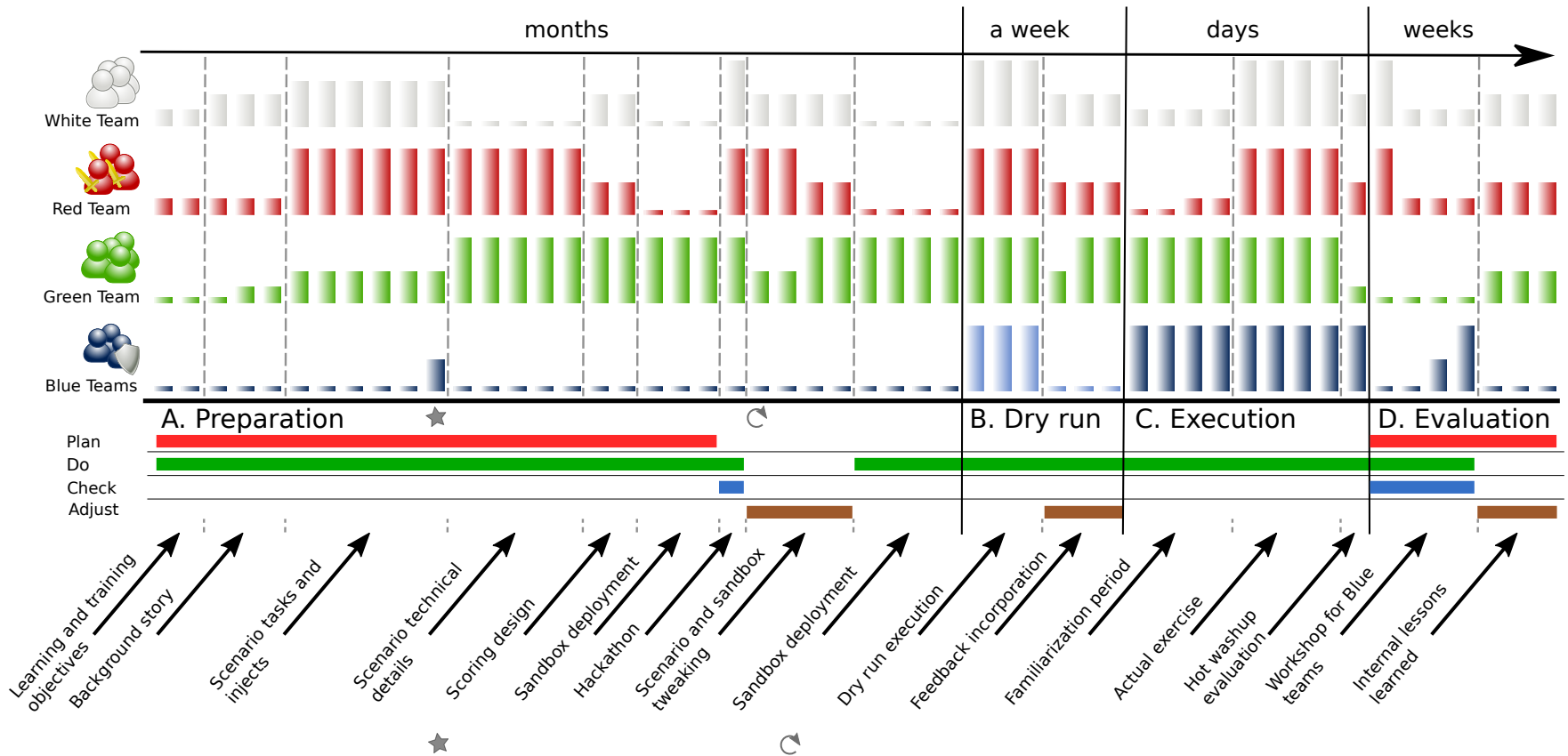
The lack of analytical tools

- Evaluation of scenarios, improving their impact on learners

Reason:

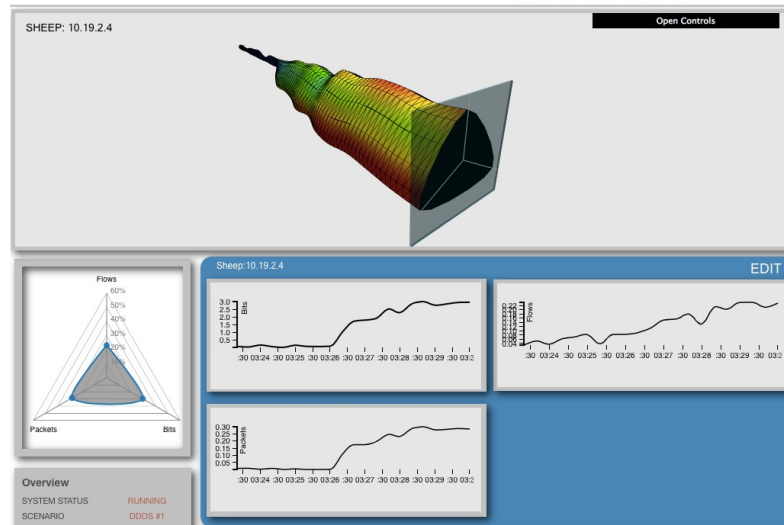
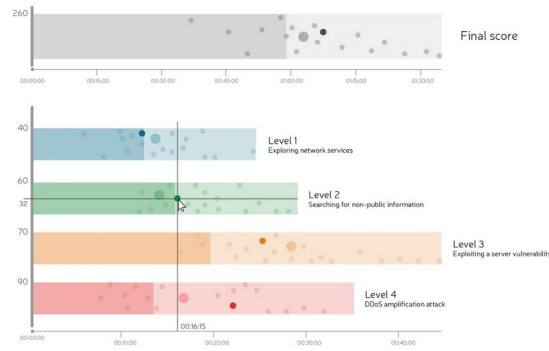
- too many involved people, non-formalized processes, changing data, unclear objectives => a lot of **ad-hoc preparation and manual work.**

Cyber Defense Exercises – Life Cycle



Our Goal

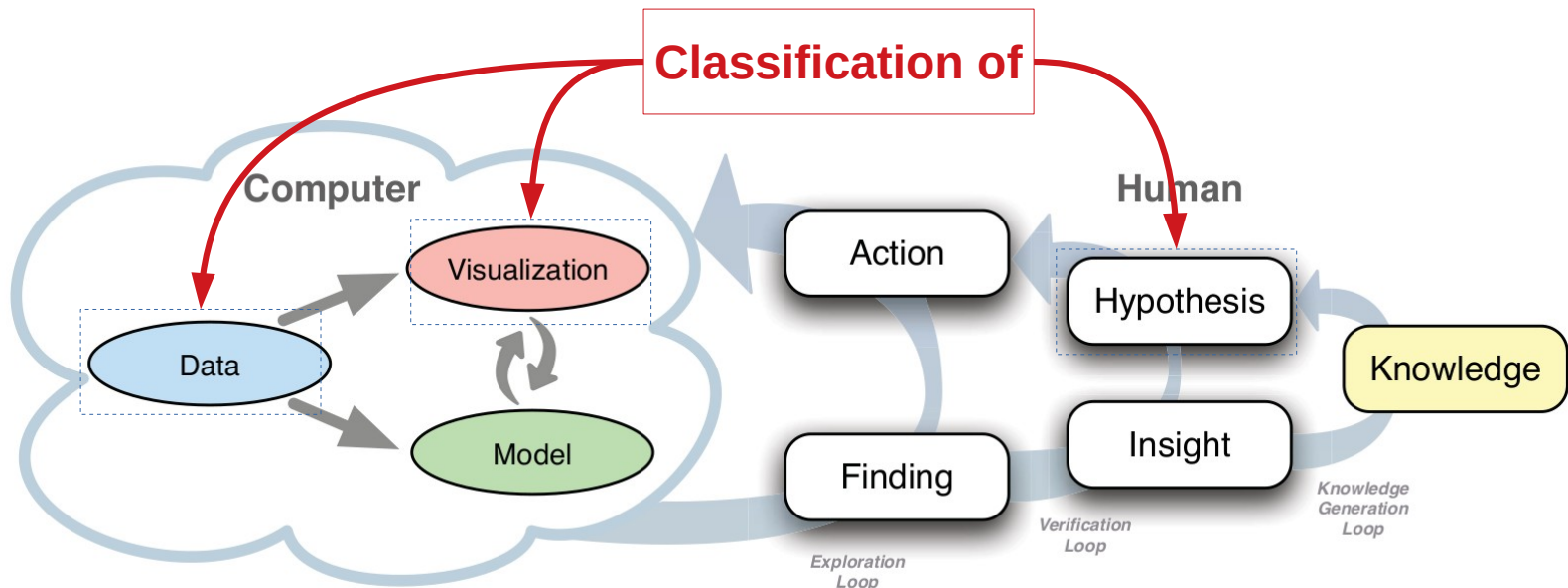
- To clarify data, processes, and requirements
- Systematically support **organizers** in their tasks by means of **interactive visualizations** integrated into the cyber range

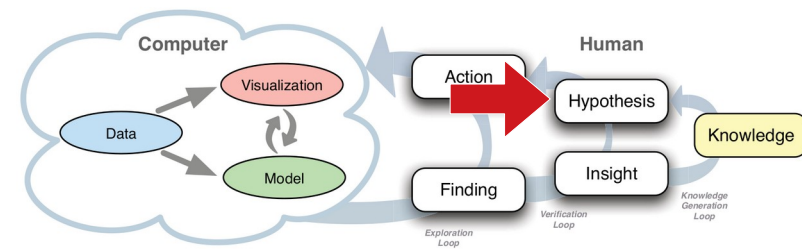


Approach: Using a Visual Analytics Process

Knowledge generation model by Sacha et al.

- **Hypothesis-driven** model extending the model of Keim et al. (the computer part) with hierarchically connected human loops





Analytical Goals (Classification of Hypotheses)

G1: Evaluation of exercise and its parameters

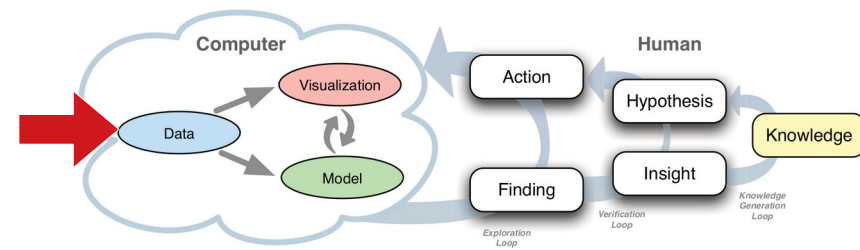
- To make an exercise useful and to keep learners motivated to finish it.
- Hypotheses related to scenario difficulty, learners' confidence and satisfaction, learners' skills, and other qualitative aspects

G2: Behavioral analysis of learners

- To reveal relevant facts about the motivation of learners, learning impact, their level of knowledge, etc.
- Hypothesis related to the study of the behavior of learners during an exercise.

G3: Runtime situational awareness

- We can consider situational awareness as a process of making simple runtime hypotheses in the users' mind.



Classification of Data

Scenario-specific data

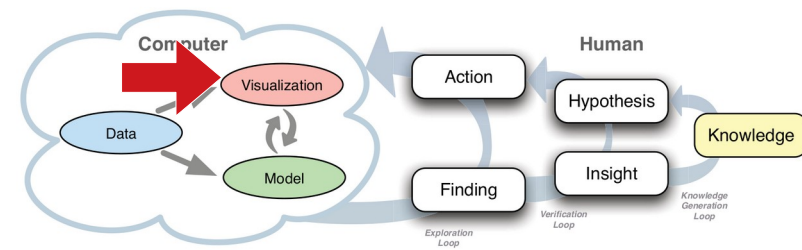
- Configuration data defined by organizers usually in the preparation phase
- Division of learners to teams, network topology, penalties, ...

Exercise runtime data

- A system-generated data gathered and stored during the execution phase of an exercise.
- Obtained penalty points by individual teams, ...

Evaluation data

- User-generated data providing qualitative information
- Post-exercise surveys, online feedback data, notes of organizers, ...



Classification of Visualizations

Exercise infrastructure view

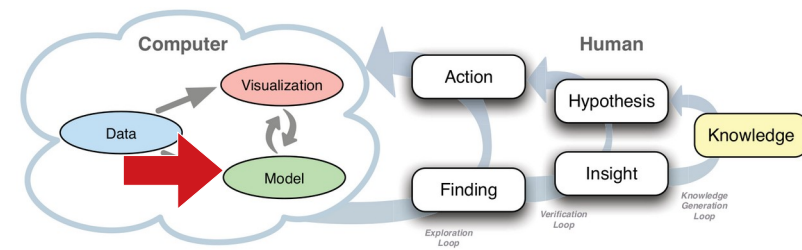
- Monitoring of services and infrastructure (G3 – situational awareness and G2 – behavioral analysis).

Visual insight into the exercise progression

- Primary visualizations for G3 – situational awareness. Moreover, online validation of exercise parameters (G1 – exercise evaluation)

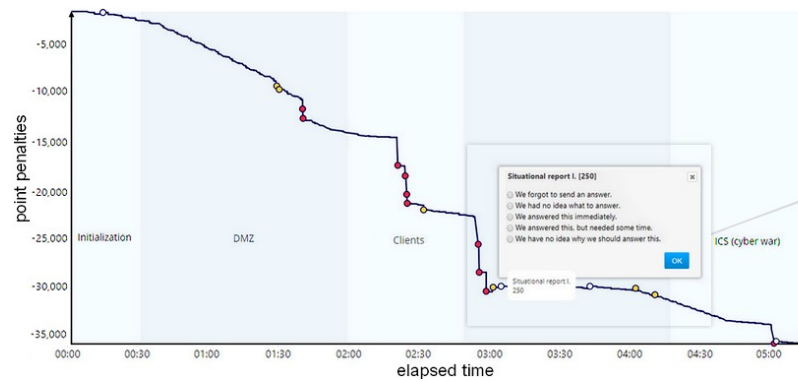
Interactive feedback visualizations

- Interactive = learners provides comments, ranks events, etc. This data is used by organizers to reveal inappropriate exercise parameters (G1 – exercise evaluation) and to collect behavioral data (G2 – behavioral analysis)



Model

- Can be as simple as descriptive statistics or as complex as a data mining algorithms
- Statistical models are used extensively for CDX
- Utilization of advanced models is exceptional and ad-hoc just because of missing conceptual solution to repeated analytical tasks



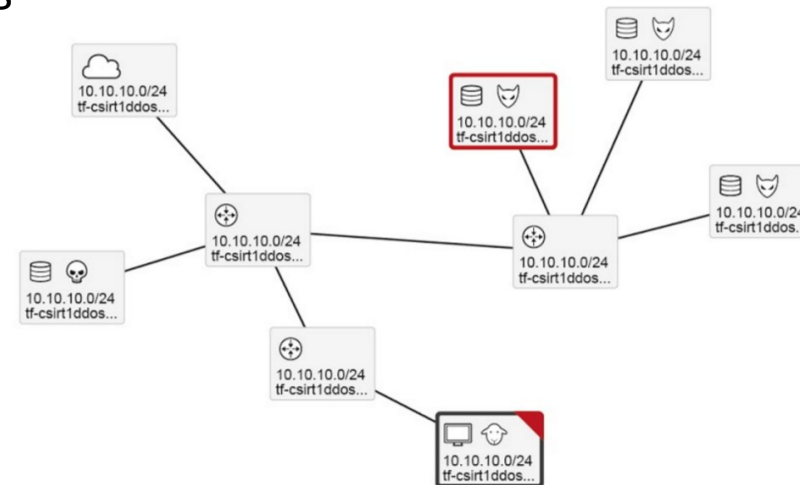
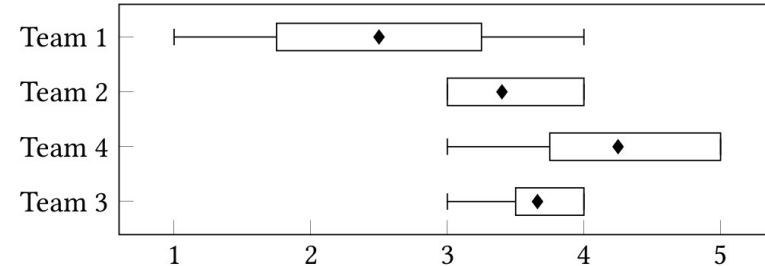
Situational report I. [250]

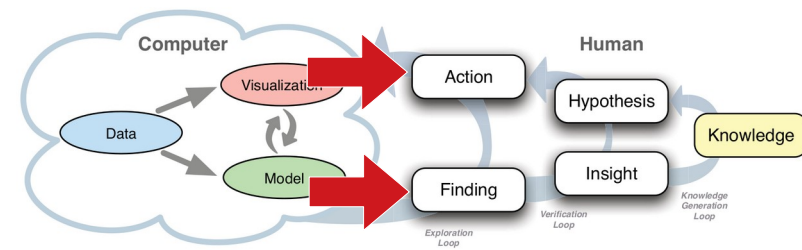
- We forgot to send an answer.
- We had no idea what to answer.
- We answered this immediately.
- We answered this, but needed some time.
- We have no idea why we should answer this.

OK

Case Study

- Hypothesis:
 - The participants improve their skills
- Data
 - Data from scoring and auditing systems
 - Pre- and post-exercise questionnaires
- Model
 - Descriptive statistics
- Visualizations
 - Feedback visualization
 - Statistical visualizations





Exploration Loop: Actions and Findings

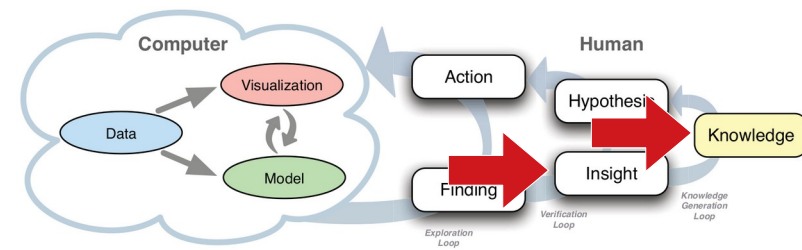
For the hypothesis *“The participants improve their skills”*

Actions:

- Organizers: Data definition, configuration of data sources (sub-systems) and dashboards (visualizations), evaluation
- Learners: Filling questionnaires, interaction with the cyber range and the feedback visualization

Findings:

- Majority of the learners confirmed they learned new skills or re-shaped existing ones.
- Some learners did not learn anything new.
- Some others admitted the lack of necessary skills.



Insight and Knowledge

For the hypothesis *“The participants improve their skills”*

Insight:

- Fairly confirmed. *Individual learners would be affected by their skills and skills of teammates.* A novel ways of prerequisite testing are desired.
- New hypotheses hypotheses have been derived:
 - *The difficulty of the exercise was adequate for learners*
 - *Learners form well-balanced teams*

Knowledge:

- Knowledge is a “justified insight”. In our case study, it is necessary to repeat the exercise so that we get data of more participants

Conclusion

- We proved the applicability of VA process on complex cyber defense exercises
- We proposed a basic classification for hypotheses, data, models, and visualizations and their mapping to CDX life cycle
- Applying the VA process to the organization of cyber defense exercise enabled us to
 - Rethink the organizational and analytical processes in the hypothesis-driven way
 - Identify current limits in the automation and systematic support of important processes in our cyber range
 - Structure our know-how so that it would be possible to build a formalized knowledge and share it across organizers