KYPO – KYBERNETICKÝ POLYGON (CYBERNETIC PROVING GROUND)

Radek Ošlejšek

LAB OF SOFTWARE ARCHITECTURES AND INFORMATION SYSTEMS

FACULTY OF INFORMatics MASARYK UNIVERSITY
KYPO – Cyber Exercise & Research Platform

- KYPO2: 2016 – 2020
KYPO Architecture and Principles
Basic Use Cases

- Cyber research and development
  - Data storage, fast replay, sandbox cloning, isolated environment, ...

- Forensic analysis
  - Pre-configured nodes, connection of physical devices, ...

- Security training and exercises
  - Collaboration modes, interactivity, ...
Cyber Czech – A National Defense Exercise

- In cooperation with National Security Authority
- Focused on defending critical information infrastructure (nuclear power plant)
- Two-days hands-on drill
- One team of attackers against 4 teams of defenders
- Two additional supporting teams playing the role of referees, organizers, journalists and storytelling members.
- Cca 40 participants at all
Cyber Czech – A National Defense Exercise

**Green Team**
- maintain
- repair
- fix

**Blue Team**
- secure
- monitor
- defense

**White Team**
- rules
- score
- guide

**Red Team**
- attack
- scan
- penetrate
KYPO Portal

Web application.

**Challenge:** Dynamic actors and use cases defined “on the fly” via security scenarios
GUI Example: Topology
KYPO Lab – Equipment

- All-in-one touch computers
- 4 FullHD displays + 2 UHD/4K displays
- 5m wide 3D projection screen
- 5x3 FullHD true multi-touch display wall (detection up to 10 simultaneous touches)
- Dynamic input-output mapping
- Leap motion devices
- Eye-tracking