Cyber situational awareness

A systematic review of the literature

By Ulrik Franke and Joel Brynielsson

lasaris LAB OF SOFTWARE ARCHITECTURES AND INFORMATION SYSTEMS

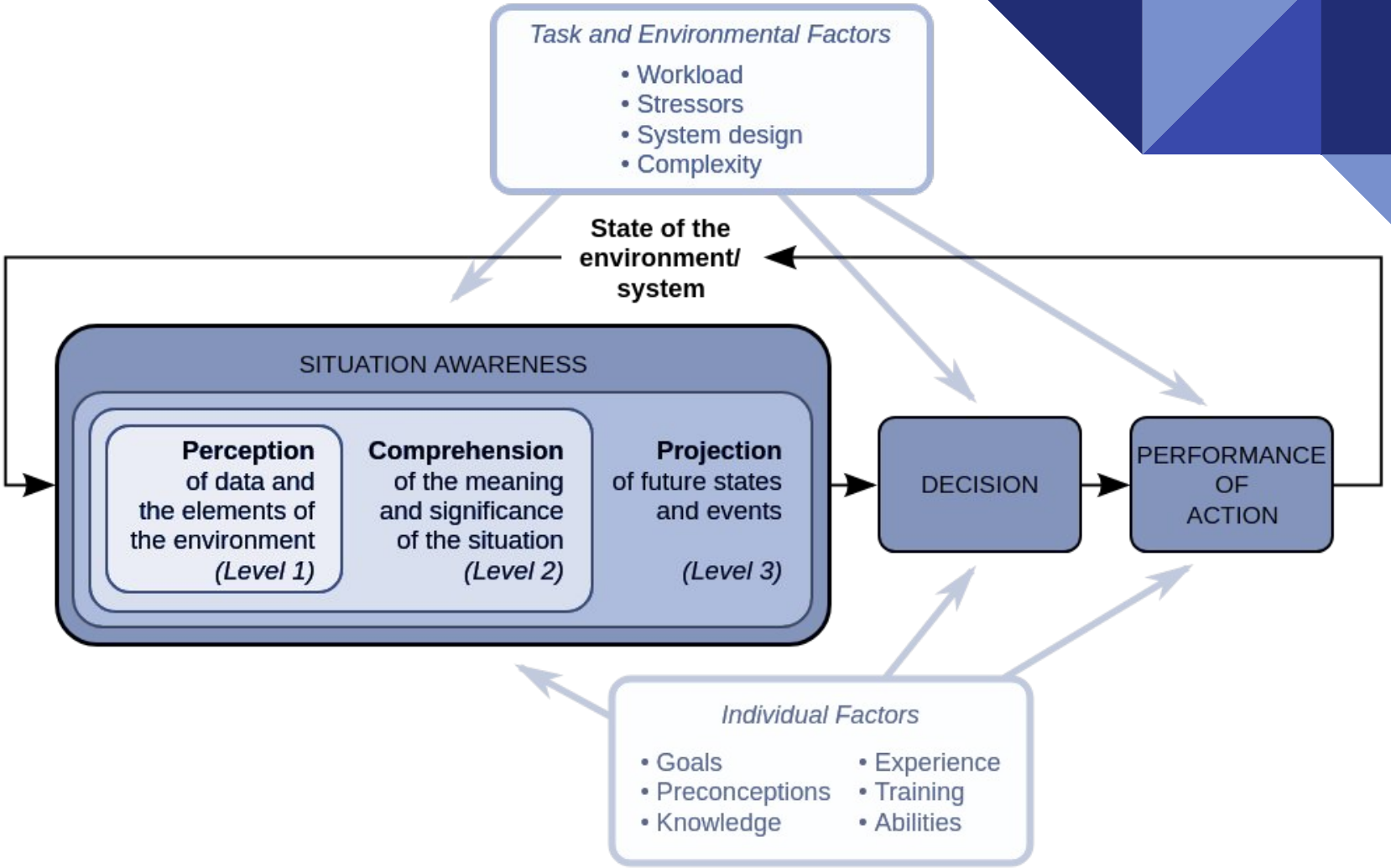
Presented by Karolína Burská

Introduction

- Cyber issues attract evermore attention
- Especially in power grid and other **c**ritical **i**nformation **i**nfrastructure areas (crisis management, military planning...)
- Need to process amounts of data, gain a rational estimate of their importance and make decisions
- SA is the result of data fusion, i.e., “the process of combining data to refine state estimates and predictions”

Situation(al) Awareness

- A mental state that can be reached to a varying degree
- Well-studied phenomenon, first model introduced by **Mica Endsley**
- Perception of events with respect to time or space, the comprehension of their meaning, and the projection of their future status
- Measures, to what extent a human decision-maker is aware of the situation.


Task and Environmental Factors
• Workload
• Stressors
• System design
• Complexity
State of the environment/ system
SITUATION AWARENESS
Perception of data and the elements of the environment (Level 1)
Comprehension of the meaning and significance of the situation (Level 2)
Projection of future states and events (Level 3)
DECISION
PERFORMANCE OF ACTION
Individual Factors
• Goals
• Preconceptions
• Knowledge
• Experience
• Training
• Abilities

Cyber Situation Awareness

- Subset of situational awareness
- Includes awareness taking place in cyberspace (computer network-related activity)
- Involves both technical and cognitive challenges (underlying infrastructure + human understanding)
- Purpose:
  - enhance comprehension of critical cybersecurity events
  - facilitate operational responses to them

Cyber Situation Awareness

- Two contexts:
  - routine operational production
  - command and control work related to a specific situation (e.g., crisis management)

- Sought by governments, enterprises and other stakeholders

Focus Outline

- General cyber situational awareness (CSA)
- CSA for industrial control systems (mostly the power grid)
- CSA for emergency management
- Tools, architectures, and algorithms for CSA
- **Information fusion**
- **Visualization for CSA**
- **Human-computer interaction, design specifications & workflows for CSA**
- Nation-wide, large scale CSA
- **Exercises relating to CSA**
- Information exchange for CSA
- Military CSA

Application Area, Threats

- Industrial control systems (ICS)
- Comand/control systems (SCADA)
- Civilian or military command and control networks (crisis management, operational or tactical command)
- CSA in organizational operations management networks (e.g. intranets)

Threat types

- Espionage, i.e. covert copying and reading information
- Dissemination of information, i.e. making information public
- Degrading information availability, DoS attacks or obscure networking errors
- Degrading information integrity, i.e. to change or destroy application information

Methodology & Technology

- Visualization, user interaction and/or usability
- Cyber situational awareness workflow
- Detection/analysis of adversarial network activity
- Battle damage assessment

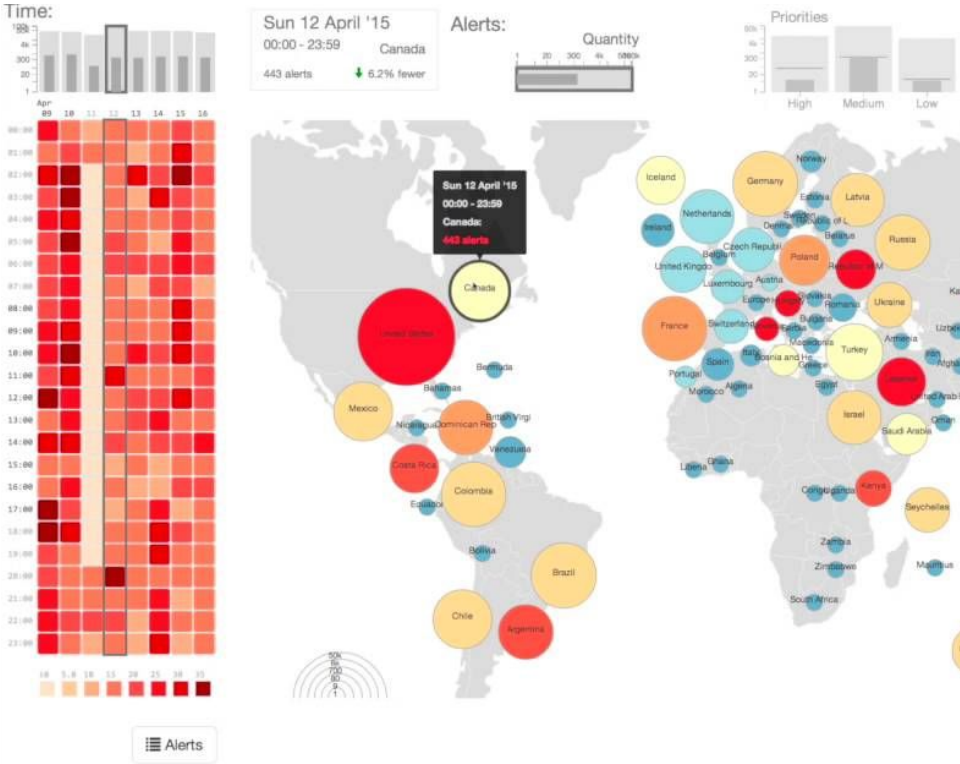
Application area	
Industrial control systems (ICS)	17
Command & Control	15
Operations management networks	7
Experiments, methodology, technology	
Design	76
Implementation	56
Empirics	45
Visualization	24
Workflow	28
Attack detection & analysis	60
Attacker ID & purpose	12

Information Fusion

- Fusion of information from different sources
- Systems for collaboratively combining data from sensors using ontology methods
- Usage of security audit data
- Game theory insight - estimation of cyber attack patterns, useful in cyber exercises

Visualization for CSA

- Generally believed to be important to attain cyber situational awareness
- “human in the loop” design - to find appropriate visualizations
- Employment of cognitive task analysis to support the work of analysts



HCI, design specifications & workflows for CSA

- Includes modeling and understanding the target domain (i.e., the users/organization) from a design perspective
- Findings from a cognitive task analysis, definitions of analyst roles, discussions on proper visual representations
- A narrative-based training in network security analysis tasks

Exercises relating to CSA

- Suitable for empirical investigation of cyber situational awareness
- Usage of data from an exercise, collecting data on team collaboration, scoring data, interview data, network packets and logs

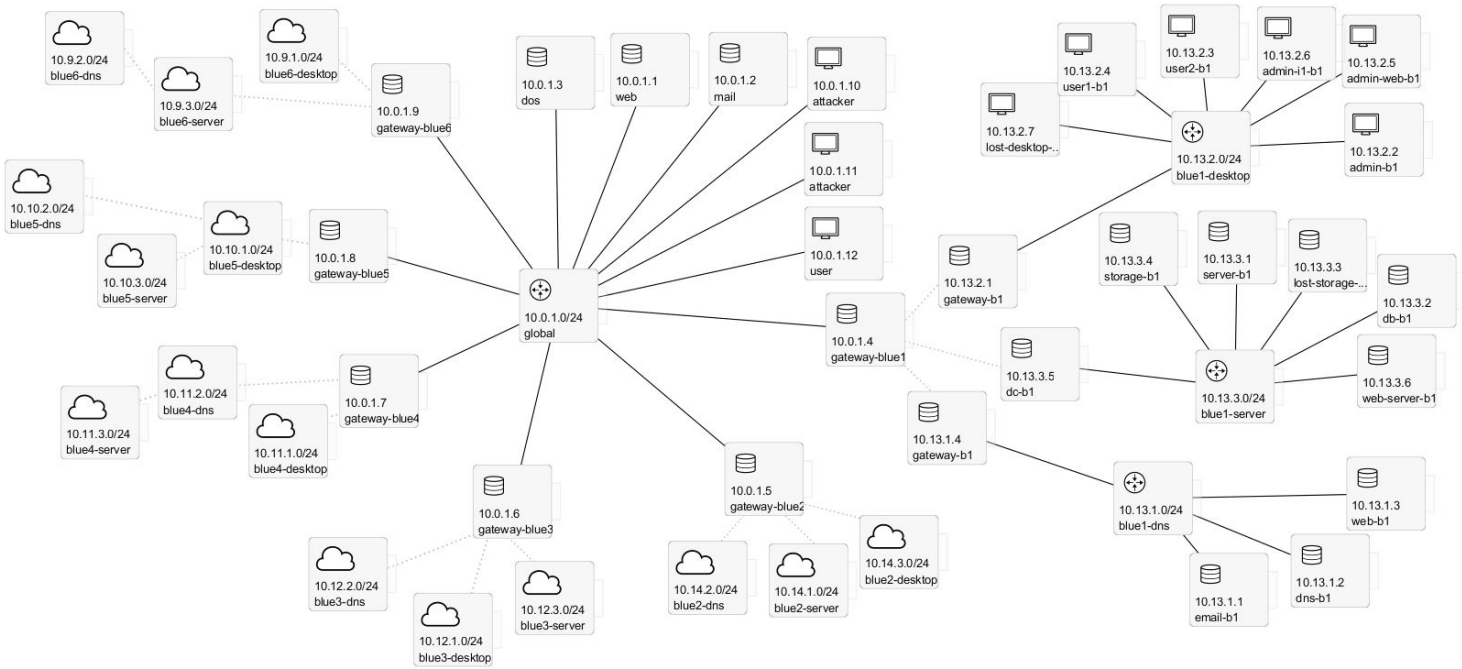
KYPO

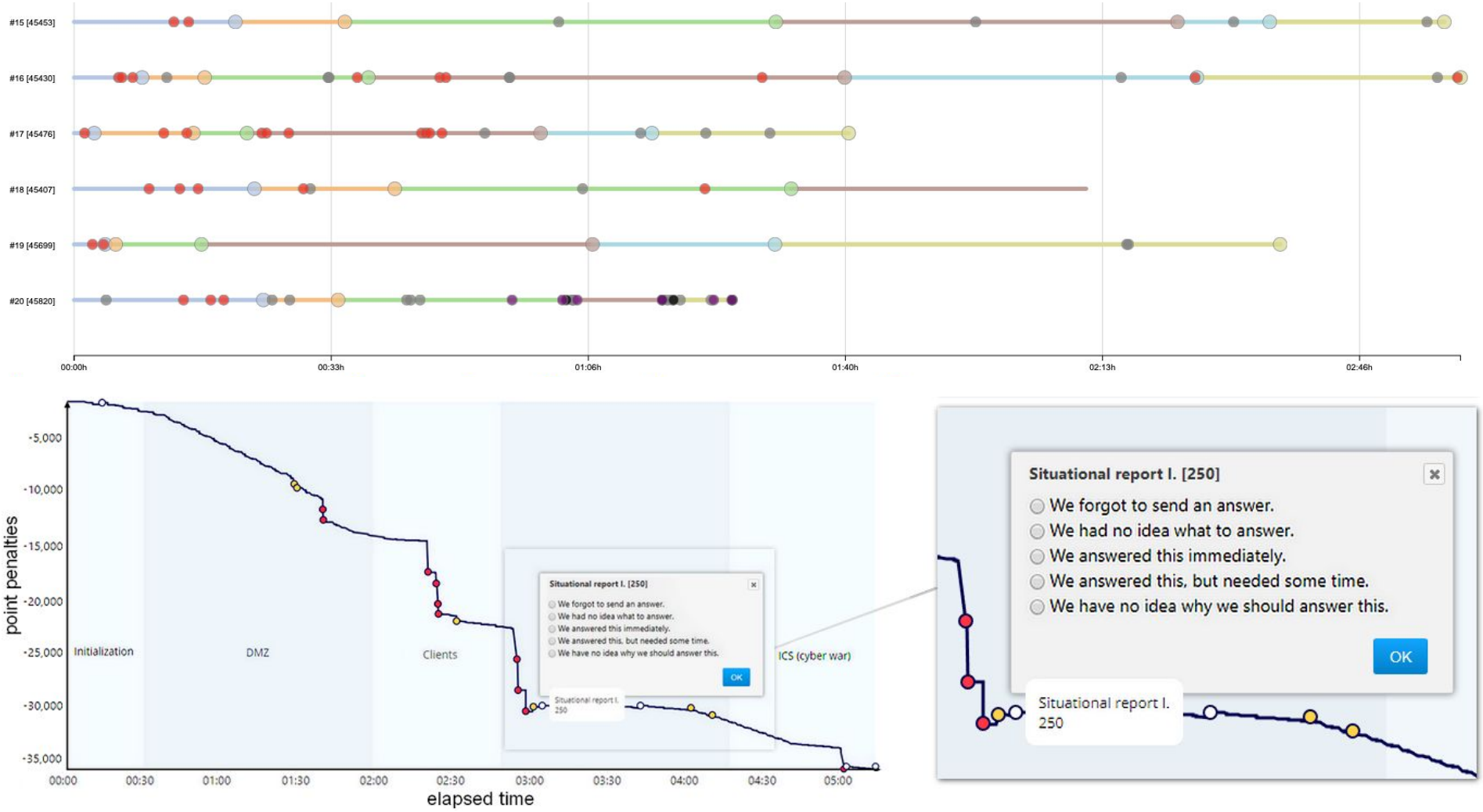
- Platform for analyzing security threats to critical information infrastructure
- Enables creating computer networks for detailed study of the emergence, spread, and impacts of current cybernetic threats
- Can be effectively used for interactive training and exercise sessions

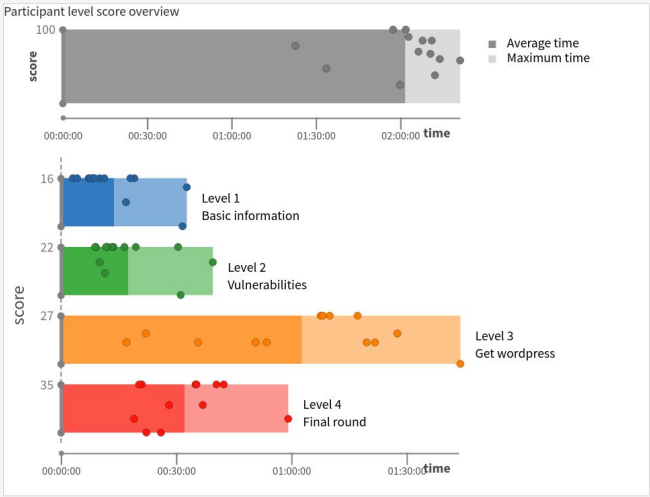
Situational Awareness in KYPO

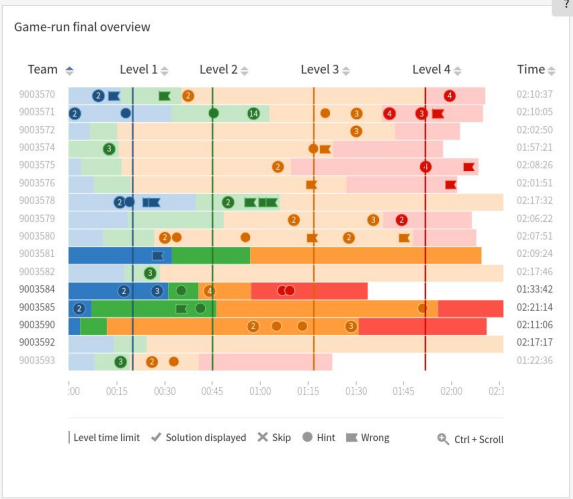
- We make an advantage of organization of cyber exercises
  -> collect network data, logs, scenario-related and scoring data
- Our aim is to provide an insight into the actions of the participants and help them improve their skills

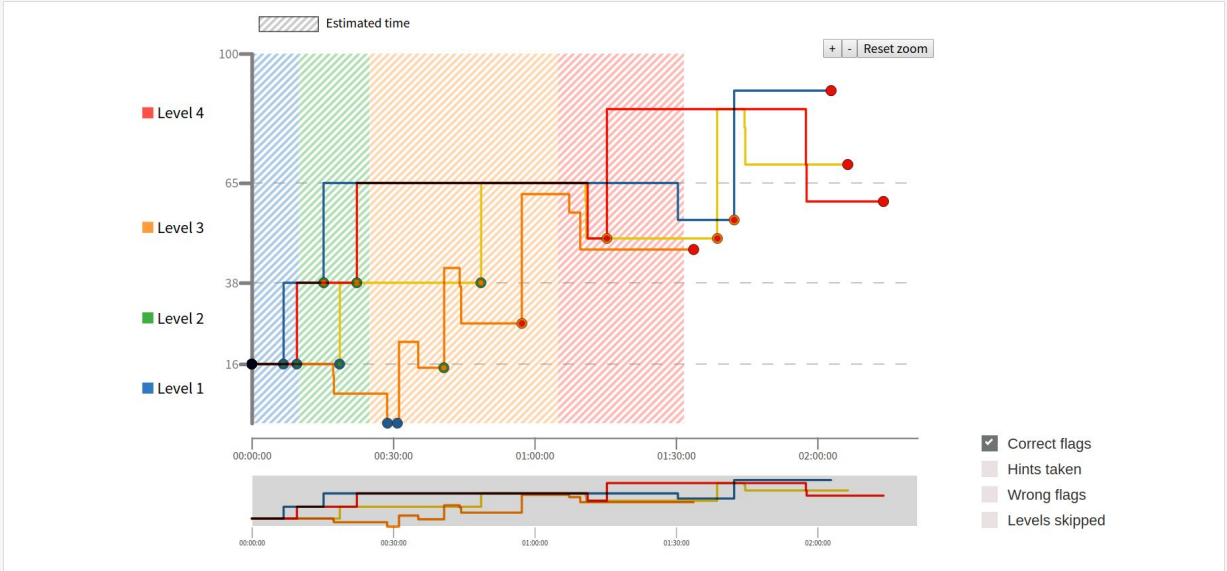
KYPO - Topology for SA




#15 [45453]
#16 [45430]
#17 [45476]
#18 [45407]
#19 [45699]
#20 [45820]
00:00h
00:33h
01:06h
01:40h
02:13h
02:46h
point penalties
-5,000
-10,000
-15,000
-20,000
-25,000
-30,000
-35,000
Initialization
DMZ
Clients
ICS (cyber war)
00:00
00:30
01:00
01:30
02:00
02:30
03:00
03:30
04:00
04:30
05:00
elapsed time
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
Situational report I. 250


Participant level score overview
score
100
Average time
Maximum time
00:00:00
00:30:00
01:00:00
01:30:00
02:00:00
time
16
Level 1
Basic information
22
Level 2
Vulnerabilities
27
Level 3
Get wordpress
35
Level 4
Final round
00:00:00
00:30:00
01:00:00
01:30:00
time


Game-run final overview
Team
Level 1
Level 2
Level 3
Level 4
Time
9003570
9003571
9003572
9003574
9003575
9003576
9003578
9003579
9003580
9003581
9003582
9003584
9003585
9003590
9003592
9003593
02:10:37
02:10:05
02:02:50
01:57:21
02:08:26
02:01:51
02:17:32
02:06:22
02:07:51
02:09:24
02:17:46
01:33:42
02:21:14
02:11:06
02:17:17
01:22:36
00:15
00:30
00:45
01:00
01:15
01:30
01:45
02:00
Level time limit
Solution displayed
Skip
Hint
Wrong
Ctrl + Scroll


Estimated time
+
-
Reset zoom
100
65
38
16
Level 4
Level 3
Level 2
Level 1
00:00:00
00:30:00
01:00:00
01:30:00
02:00:00
Correct flags
Hints taken
Wrong flags
Levels skipped

Conclusion

- Large pool of related areas for CSA
- The actual level of situational awareness improvement is seldom measured, empirical research is missing
- Cyber defense exercises can enable us to deal with the issue of SA effectively

Thank you for your attention!