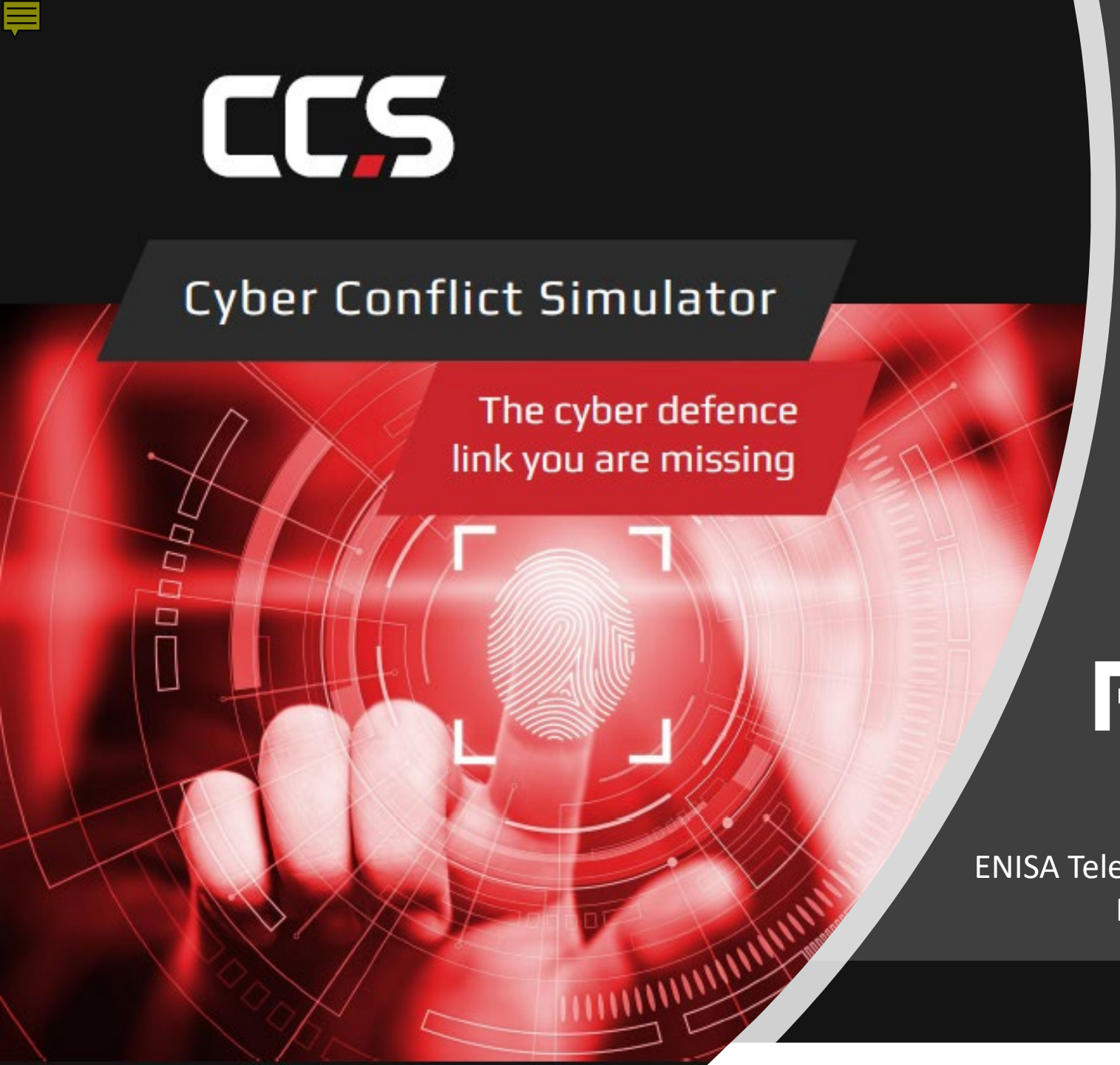


Rethinking Security Exercises

Stjepan Groš
Goran Polonji

UNIVERSITY OF ZAGREB
Faculty of Electrical Engineering and Computing

tilis

ENISA Telecom and Digital Infrastructure Security Forum 2025
March 20, 2025, Amsterdam, Netherlands

Cyber Security Exercises

- Two main types of cyber security exercises
  - Cyber ranges and tabletop exercises
- Each has its own advantages and disadvantages
  - Cyber ranges at technical level, tabletops for management
  - Tabletops easier to setup, cyber ranges harder
  - Consequences in cyber ranges are seen, in tabletops not
  - Tabletops miss time dimension; cyber ranges compromise complexity
  - And many others…
- Also, there are a lot of other exercises on technical level (CTFs)
- It is how it’s done today

Is there another way?

- That integrates all decision-making levels?
- Allows multiple organizations to simultaneously participate?
- Is based on our IT/OT infrastructure, not a generic one?
- Allows training for incidents lasting for weeks, even months?
- Considers available resources and real-world restrictions?
  - For both, defenders and attackers?
- Brings uncertainty and tension as present in real-life incidents?
- **We claim there is – and it's embodied in a simulation tool we created – Cyber Conflict Simulator (CCS)**

How did it all start?

- Participated in Cyber Coalition Exercise
- Not satisfied with some elements of the exercise
- An idea to develop and use simulator as a solution
- EDA dual-use call in 2016
- R&D project 2018 - 2000 develop prototype
- Continuous development and use of CCS since then

R&D Project

- The problem we tried to solve was a hard one
  - Up to the middle of the project's duration we were still struggling to determine exactly what we want and, especially, how it should be done
  - There were no models or examples we could (re)use
  - At the beginning we run exercises manually
  - Several prototypes were developed in due course
- At the end of the project, we had a working prototype
  - Most accurate description „professional wargaming"

Cyber Conflict Simulator Features

- Infrastructure and implemented controls are modelled
- Low level technical details are abstracted and simulated
  - No need to have exact and detailed model of information system
- People are simulated as well
  - Both regular users, and key personnel for incident handling
- Trainees manage key personnel
  - Receive reports from them
  - Make decisions and communicate mutually
  - Assign tasks to key personnel
  - Wait for results
- Time can be sped up or slowed down
- Focus on **WHAT** not HOW

Cyber Conflict Simulator Features (cont'd)

- Supports multiple teams in the same exercise
- Supports participation of multiple organizations simultaneously
  - They cooperate by exchanging resources
- Multiple levels of organization's management can participate
- Business processes are modeled as well
  - With dependency on IT/OT infrastructure

Where we are now

- We’ve done over 30 exercises
- The most complex exercises so far
  - Financial institutions (Banks)
  - Supervisors for financial institutions
  - Exercise for Croatian Armed Forces, Minnesota National Guard
  - Workshops three years in a row on a security conference DEEP
  - Exercise for military cadets in Croatian Military Academy
- Developing Partner Network

Some experiences from those exercises

- It’s immersive – people forget on a time schedule
- Board members and business owners tend to be involved more then they expected
  - And they become aware of uncertainties of a cyber incidents
- Organizations start to grasp usefulness of different security tools, and problems when they are not there
- **And, so far, we never heard anyone did that!**

Further R&D

- We want to integrate CCS with cyber ranges and CTFs
- Evaluating economic consequences of cyber incidents
- Making simulations as close to reality as possible
- Automatically generating topologies and exercises for CCS (and cyber ranges)
- Training red teams in decision making, organization, planning, …

Thank you for your attention!

For business inquires

Goran Polonji

Utilis d.o.o.

Fallerovo šetalište 22HR-10000 Zagreb, Croatia

M: goran.polonji@utilis.biz

W: ccs.utilis.biz

L: www.linkedin.com/in/goran-polonji/

T: +385 91 143 3106

For research inquires

Stjepan Groš

Faculty of Electrical Engineering and Computing

University of Zagreb

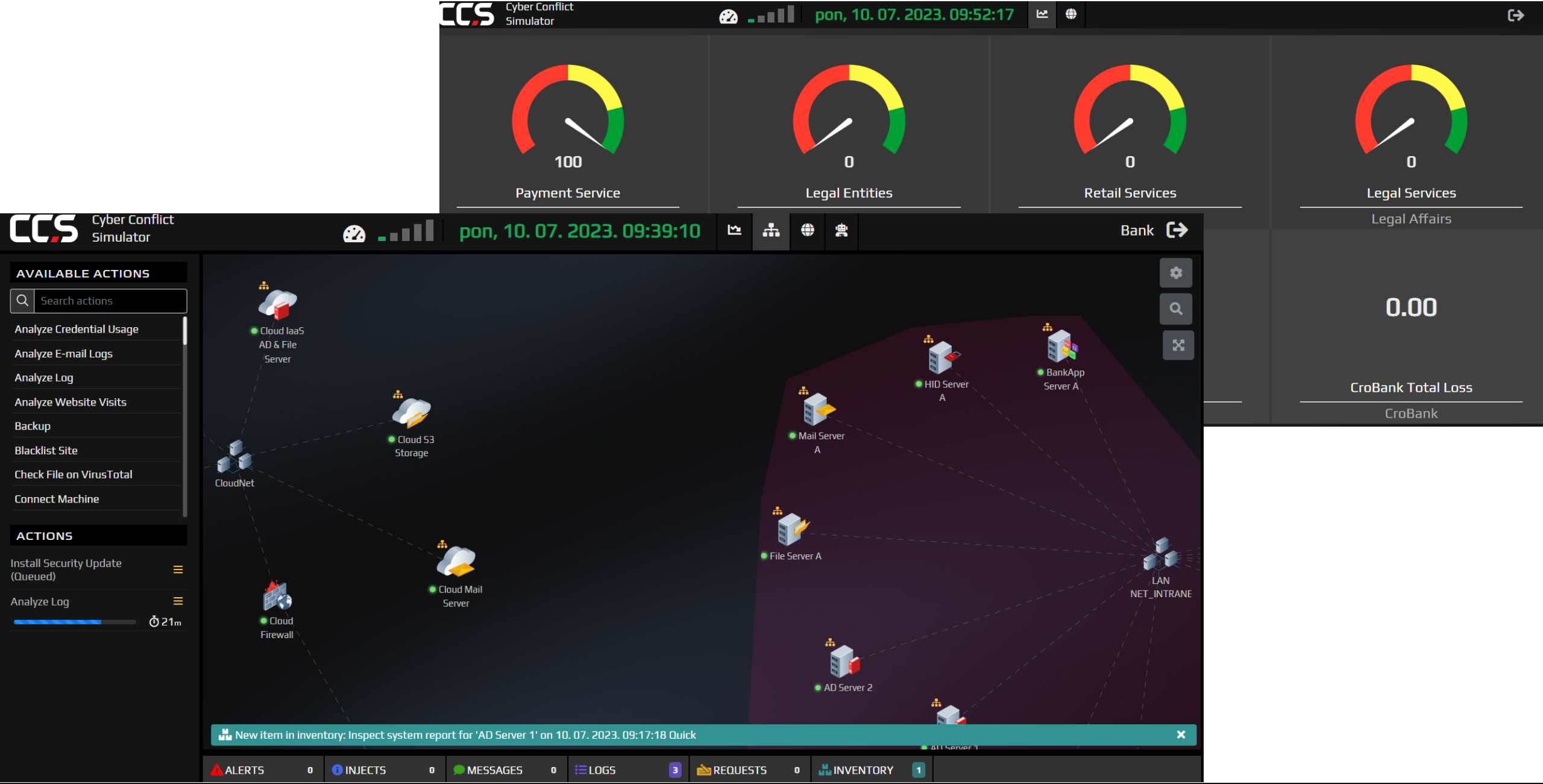
Unska 3, HR-10000 Zagreb, Croatia

M: stjepan.gros@fer.hr

W: www.fer.unizg.hr/stjepan.gros

L: linkedin.com/in/sgros

T: +385 91 6454982


Cyber Conflict Simulator
pon, 10. 07. 2023. 09:52:17
100
Payment Service
0
Legal Entities
0
Retail Services
0
Legal Services
Legal Affairs
0.00
CroBank Total Loss
CroBank
Cyber Conflict Simulator
pon, 10. 07. 2023. 09:39:10
Bank
AVAILABLE ACTIONS
Search actions
Analyze Credential Usage
Analyze E-mail Logs
Analyze Log
Analyze Website Visits
Backup
Blacklist Site
Check File on VirusTotal
Connect Machine
ACTIONS
Install Security Update (Queued)
Analyze Log
21m
Cloud IaaS AD & File Server
Cloud S3 Storage
CloudNet
Cloud Mail Server
Cloud Firewall
HID Server A
BankApp Server A
Mail Server A
File Server A
LAN NET_INTRANE
AD Server 2
New item in inventory: Inspect system report for 'AD Server 1' on 10. 07. 2023. 09:17:18 Quick
ALERTS 0
INJECTS 0
MESSAGES 0
LOGS 3
REQUESTS 0
INVENTORY 1