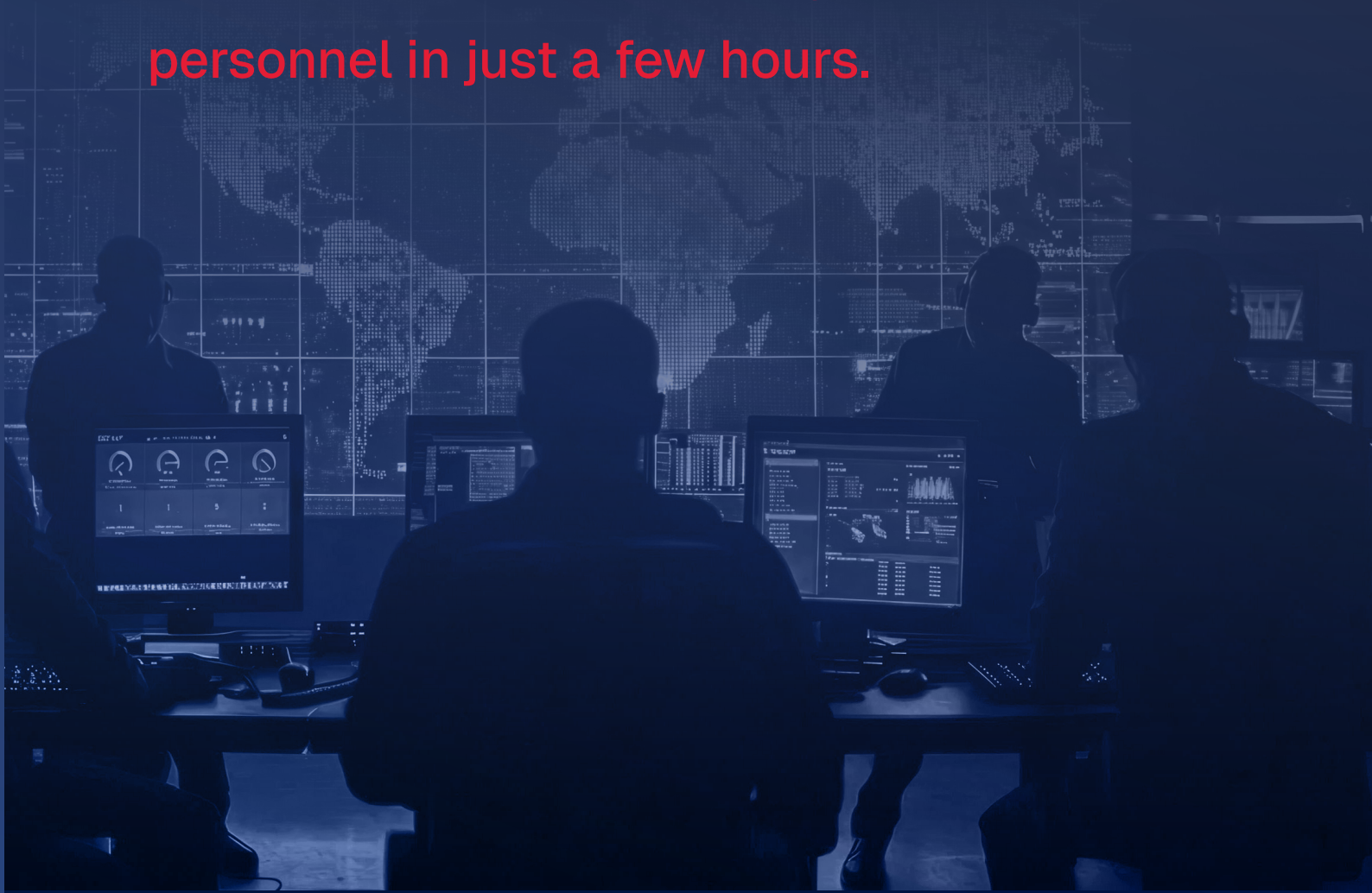




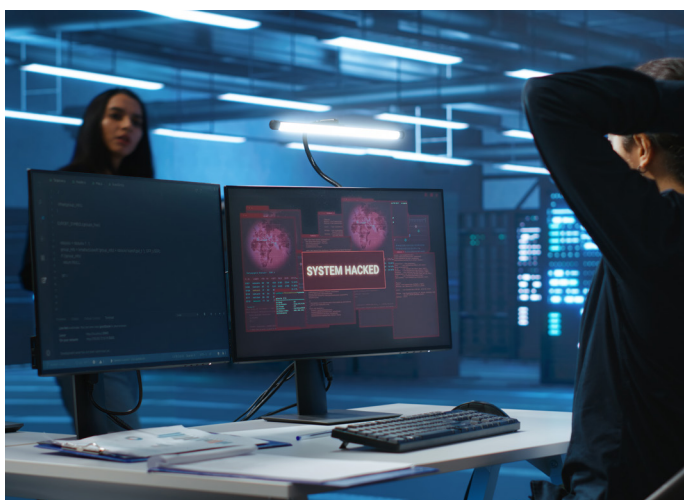
The cyber defense link **you are missing**

Carry out a realistic cyber incident
response exercise **involving all responsible
personnel in just a few hours.**



Are You Ready for a Cyberattack?

The reliance of society on cyberspace is constantly increasing. Cyberspace is recognized as the fifth operational domain of military activity where the preparedness of military forces should be assured with appropriate training. Cybercriminals are becoming more skilled and daring, and their methods and vectors of attack are becoming more sophisticated.



Cyber defense training is a requirement for civilian organizations and institutions. In addition to substantial financial losses, cyber adversaries can cause damage that threatens critical infrastructure, utilities, services, and even lives.

Organizations invest significant financial resources in cyberattack prevention measures, both technical and organizational. Prevention is important, but keeping all cyberattackers out should not be a company's sole security focus, experts say. What if, despite all the measures in place, an attack still occurs and your organization faces a cyber incident? Are you able to correctly identify its cause?

Numerous studies indicate that the average time between the occurrence of an incident and its detection is measured in months. Detection is followed by an analysis of the cause of the incident.

How good are you at containing incidents, eliminating their root causes, and restoring

information systems and business operations? Unlike fires, earthquakes, or even pandemics, cyberattacks involve a specific target and an active attacker who can adapt their actions to your defensive measures.

Do you practice cyber incident scenarios and improve your defensive tactics, techniques, and procedures based on lessons learned?

In defending against cyberattacks, technology will certainly play an important role, but people remain the key component. Special emphasis should be placed on those who manage incidents and make decisions at the operational and strategic levels.

Training and Exercises

As stated earlier, the possibility of an incident cannot be completely ruled out. When one occurs, who would you rather have at the helm: a team that already has experience or a team facing an incident for the first time? Since relatively few people have experienced an incident, exercises are the only way for those without that experience to gain it.



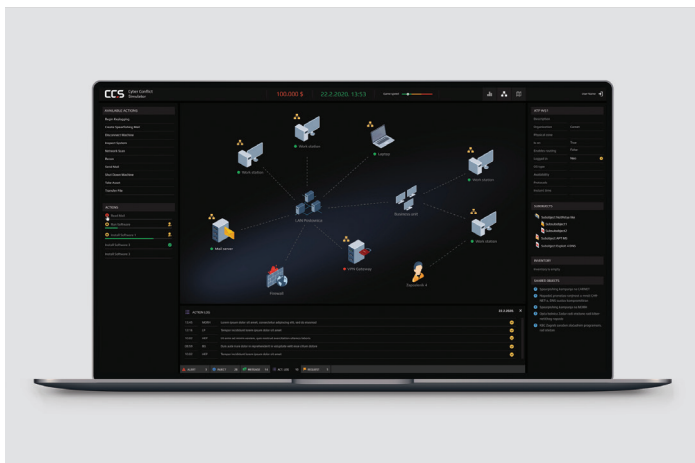
Many demanding jobs require training. Firefighters achieve speed and efficiency through regular emergency exercises. Surgeons start by assisting in operations, then work under supervision before performing operations on their own. Air traffic controllers train in simulators where “pseudo-pilots” simulate air traffic. Training generals is even more complex and expensive. Training cyber incident response teams presents a similar challenge.

Responding to a cyber incident is a demanding task that involves managing many people and activities. Some activities may take a long time, and their outcomes are important for decisions about the next steps. Incidents can last for days, weeks, or even longer. The decisions that need to be made typically go beyond IT and extend into business operations, involving people in key business roles.

All of this makes organizing and conducting exercises a demanding task. It is difficult to release key personnel from their regular duties for extended exercises. As a result, such exercises are unlikely to be conducted often enough to build experience within a reasonable timeframe.

Regulators have also recognized the importance of exercises, now often making them a requirement for organizations of particular importance, such as critical infrastructure operators. The EU’s NIS and NIS2 directives identify exercises as one way to prepare effectively for a possible incident.

All these challenges led to the development of Cyber Conflict Simulator - an interactive simulator that takes a different approach to cyber incident response.



Cyber Conflict Simulator (CCS) is a software system designed for people responsible for managing cyber incidents in both the civilian and military sectors.

HOW IT WORKS

Cyber Landscape

Imagine being able to transfer your IT and business systems into a virtual environment. You can configure them to work just as they do in the real world. CCS allows you to describe how business services or production processes depend on the IT systems targeted by an attack, as well as the consequences of disrupting those systems.

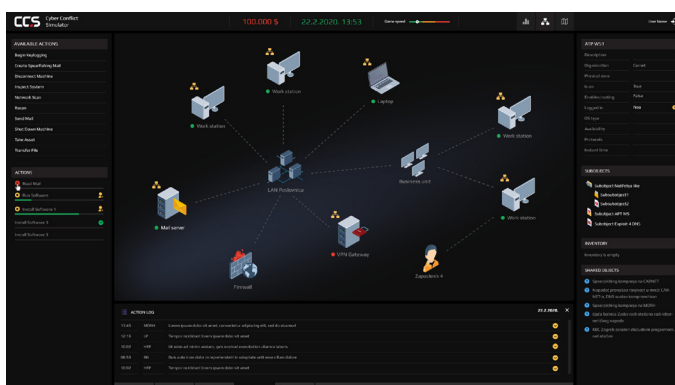
The IT system is represented by objects such as computers, servers, mobile devices, networks, operating systems, software, services, files, databases, and SCADA systems. CCS also allows you to define dependencies on external services. These services can be disrupted by a cyber incident or serve as an entry point for an attacker.

People are an important part of any organization — system administrators, digital forensics specialists, technicians, analysts, and all other staff. They form a virtual team that participants manage during the simulation.

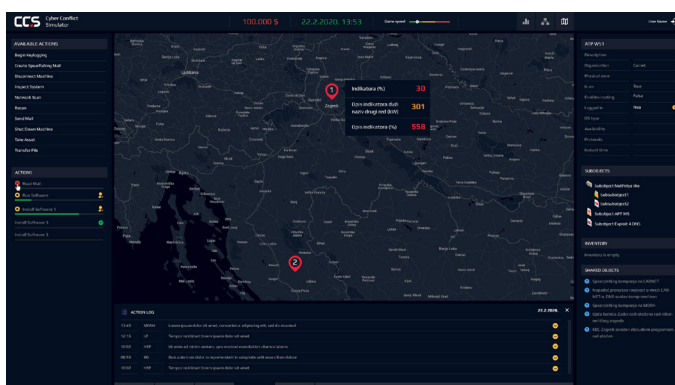
Attackers can be modeled to represent different sources of threats, including states, criminal groups, and individuals.

Simulation

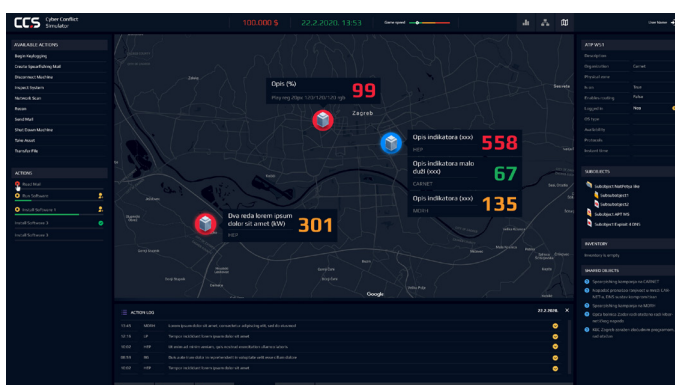
To be realistic, an exercise must accurately model events in the IT infrastructure, where the problem originates. Business impacts must also be modeled, as they reflect the actual damage or losses that can occur.



The simulation can follow predefined scenarios and planned steps or involve the active participation of a red team. The exercise can begin when offensive activities start or later, when the incident is detected and the attacker has already achieved some of their goals. The author of the exercise scenario decides when it begins.



There can be several groups of participants in the simulation. Several organizations can take part in the exercise, with each seeing only the information that would be available to it in a real situation.



Participants assign tasks to members of their virtual team. We call these team members actors. An actor's skills determine which tasks they can perform and how long those tasks take, just as in real life.

Actors report on their work and results. Based on this information, participants decide on the next steps to resolve the incident.

During the exercise, participants often have to wait for the results of actors' activities. At these points, the simulation can be sped up and slowed down again at any time. This allows the exercise to be completed much faster than the corresponding events would unfold in real life. With CCS, a cyberattack that would last for days or weeks can be simulated in just a few hours.

Once the virtual cyberspace has been defined, you can conduct an unlimited number of exercises with different scenarios. The exercise is largely determined by the resources available to the attacker and the attack techniques they use. This creates a wide range of possibilities for exercise scenarios.



All steps and events in the exercise are logged and included in the simulation report. This enables improvements to defense strategy, tactics, techniques, procedures, and the entire system.

Many questions are important for cyber defense. Can an attack be detected early? How easily can an attacker move through your organization to reach their goal? The list goes on.

The best way to find the answers is to test your defenses. CCS is a valuable tool for testing your IT system. It allows you to simulate various attacks on your organization and assess how easily you can detect and contain an attack and ultimately understand what really happened.

You can introduce zero-day vulnerabilities into any component of your system and test how they affect your defenses in the event of an attack.

Key Features



FLEXIBILITY

Create a virtual cyberspace that fully corresponds to your real information system.



SCALABILITY

Model complex systems by including all related organizations.



INTERACTIVITY

The outcome of the simulation depends entirely on the participants' actions.



EXTENSIBILITY

Expand the system with new objects, actions, and controls through a plug-in mechanism.



TIME MANAGEMENT

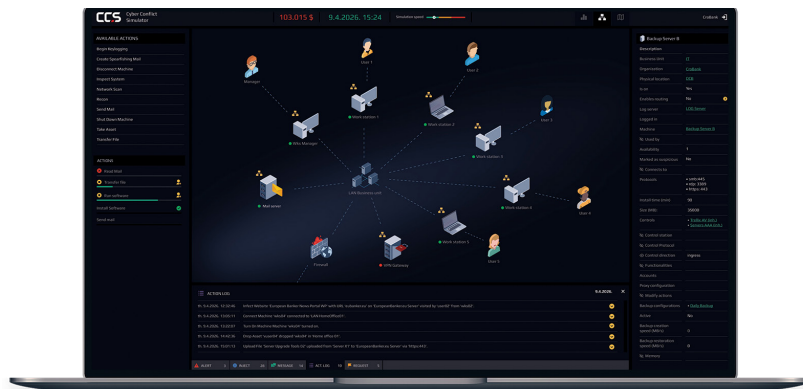
Speed up the simulation whenever you want to shorten the exercise and save time.



LESSONS LEARNED

Use after-action reviews to analyze the steps taken during exercises and improve your team's defense tactics and techniques.

Turn Practice into Readiness



CCS

**The cyber
defense link you
are missing**

Utilis CCS enables you to assess your organization's readiness to respond to cyber incidents. It helps you test the robustness of your IT system and prepare the most important element of your defense - your people.

CCS is designed for those responsible for managing cyber incidents in the civilian and military sectors. It simulates various types of cyberattacks on your information system and allows you to define a virtual cyberspace composed of different objects.

CCS makes it easy to:

- Assess the response and performance of your system and cyber incident response team in the event of an attack
- Test your cyber incident response procedures and communication plans
- Save time and other resources when preparing exercises, so you can conduct more exercises with less effort
- Simulate cyber incidents that would last for days or weeks in a matter of hours
- Gain experience and skills through exercises involving various attack scenarios
- Raise awareness of threats to your IT system

“Learn from your mistakes,” as the saying goes. Mistakes during real cyber incidents can be very costly, so it is better to make them during exercises first. We designed CCS to be very easy to use. It can also be easily extended through a plug-in system.

In its initial phase, CCS was recognized by the European Defence Agency (EDA) as an innovative dual-use project with military and civilian applications and was selected to receive technical support.

Arrange an Exercise

A team of Utilis and FER experts can prepare everything needed to conduct an exercise with minimal involvement from your organization.

Contact us with any additional questions, to request a presentation, or to arrange an exercise tailored to your organization.

+385 (1) 36 35 666

info@utilis.biz



Utilis Ltd.
Fallerovo šetalište 22
10000 Zagreb, Croatia
www.utilis.biz
ccs.utilis.biz



**Co-funded by
the European Union**