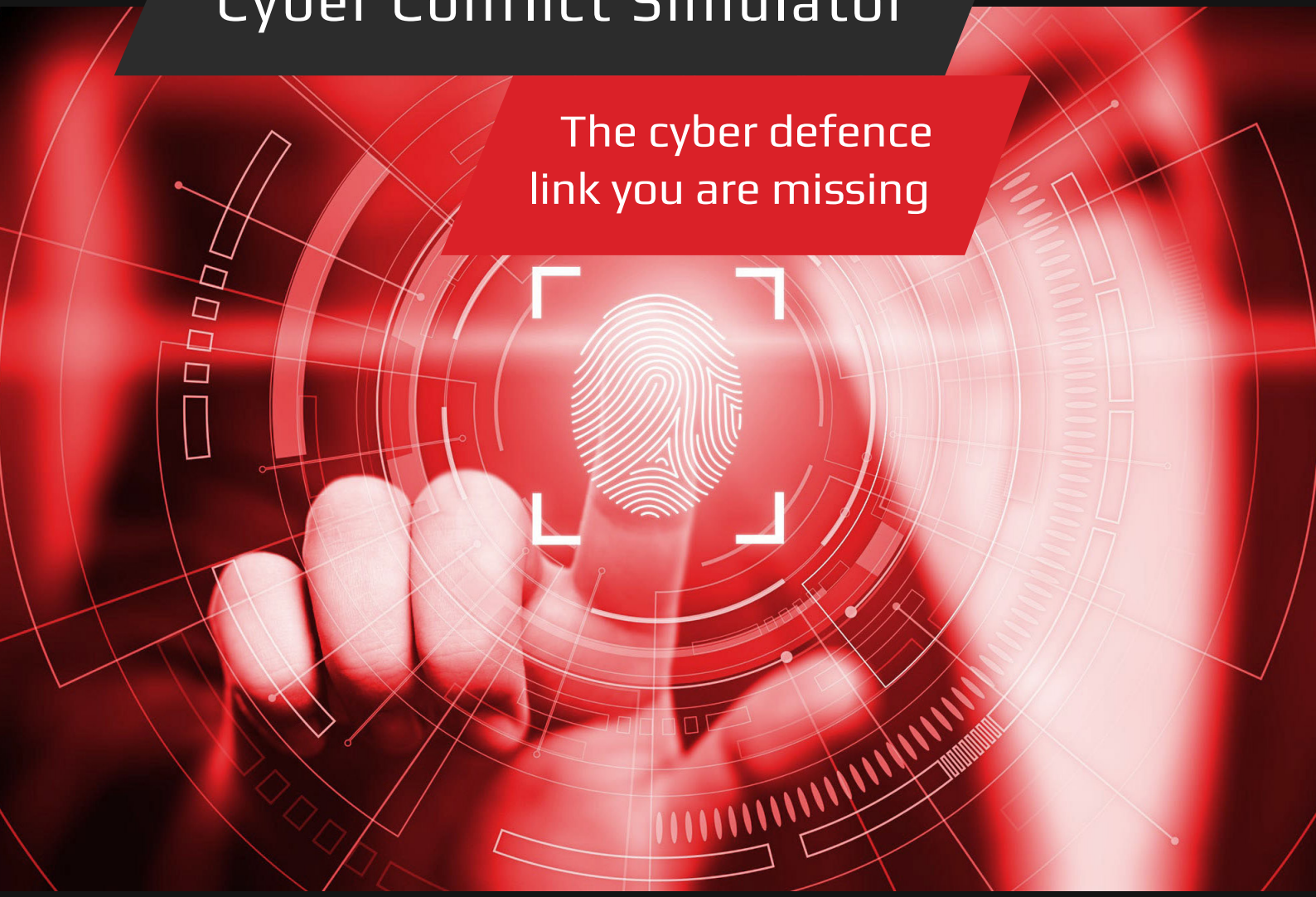
CCS

Cyber Conflict Simulator



The cyber defence link you are missing

Carry out a realistic cyber incident response exercise with the participation of all responsible persons in just a few hours.

Are You Ready for a Cyber Attack?

The reliance of society on cyberspace is constantly increasing. Cyberspace is recognized as a 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 defence training is a requirement for civil organizations and institutions. Aside from very big financial losses, cyber adversaries could cause damage that threaten critical infrastructure, utilities, services and even lives.

Organizations invest significant financial resources in cyber attack prevention measures, both technical and organizational.

Prevention is important but locking out all cyberattackers should not be a company's sole security focus, experts say.

What if, despite all the measures in place, the attack still happens and we face a cyber incident?

Are you able to properly detect its cause? A large number of studies indicate that the average time from the occurrence of an incident to its detection is measured in months. This is followed by an analysis of the cause of the incident.

How good are you in incident containment, cause eradication, and IS and business recovery? Unlike fires, earthquakes or even pandemics, cyber attacks have their target and an active attacker who can adapt his steps to our defensive actions.

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

In the defence from cyber attacks, technology will certainly play an important role, but still, people are the key component. Special emphasis should be placed on people who are managing incident events and making decisions at the operational and strategic level when incidents happen.

Training and Exercises

As stated earlier, the possibility of an incident cannot be completely ruled out. And when it happens, who would you rather have at the helm? A team that already has experience or a team that is facing it for the first time?
Since the number of people who have experienced an incident is relatively small, the only way to gain experience is through exercise.

For many demanding jobs it is necessary to train people. Firefighters achieve speed and efficiency through regular emergency exercises. Surgeons start by assisting in operations, then work under supervision before performing the operations on their own. Flight controllers are trained in simulators where “pseudo-pilots” simulate air traffic.
Training generals is even more complex and expensive.
A similar challenge is training cyber incident response teams.

Responding to a cyber incident is a demanding job that involves managing many people and activities. Some of those activities may take a long time and their outcome is important for decisions about the next steps. Incidents can last for days, weeks, sometimes longer. The decisions that need to be made typically go beyond the IT domain and enter the business sphere. People who have key roles in the business are involved.

All this makes organizing and conducting the exercise a demanding task. It’s hard to single out key people from an organization for long periods of time for exercise. With that in mind, it is not to be expected that such an exercise could be carried out often enough to gain experience in a reasonable time.

The importance of exercises has also been recognized by regulators. Exercises are now often required for organizations of particular importance - i.e. critical infrastructure. EU NIS and NIS2 directives state the exercises are one of the ways to effectively prepare for a possible incident.

Cyber Conflict Simulator

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

Cyber Conflict Simulator (CCS) is a software system intended for persons in charge of managing cyber incidents in both civil and military sectors.

How it works?

Cyber Landscape

Imagine being able to transfer your IT and business system to a virtual environment. You can configure it to work just the way it works in the real world.
CCS makes it possible to describe how business services or production processes depend on the IT systems that are the target of the attack and the consequences of their disruption.

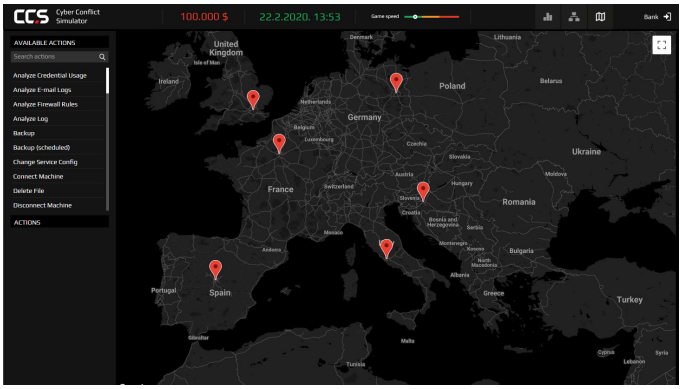
The IT system is described by objects such as computers, servers, mobile devices, networks, operating systems, software, services, files, databases, SCADA systems, etc.
CCS makes it possible to define dependencies on external services. They can be disrupted by a cyber incident or be an input vector to an attacker.

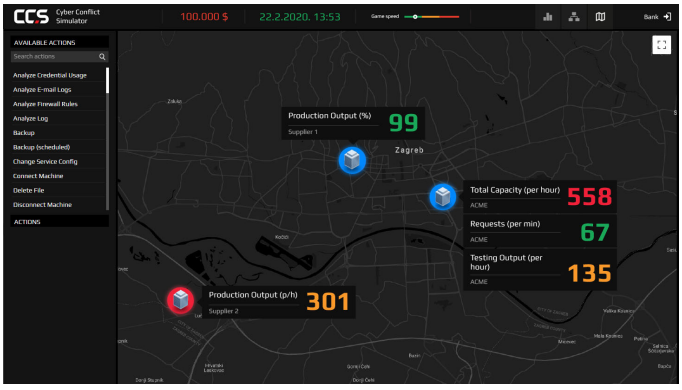
People are an important part of any organization - system administrators, digital forensics, technicians, analysts and all other staff. They are a virtual team that is managed during stimulation.

For the attacker it is possible to place different sources of threats - states, criminal groups or individuals.

Simulation

The exercise needs to be realistic so it needs to model the events on the IT infrastructure accurately, because that is the source of the problem. On the other hand, business impacts need to be modelled as they measure the actual damage or loss that can occur.





The simulation can be carried out according to predefined scenarios and prepared steps or with the active participation of a red team. The exercise itself can begin when offensive activities begin, or it can begin later, at the time of incident detection when the attacker has already achieved some of his goals. It is the choice of the author of the exercise scenario.

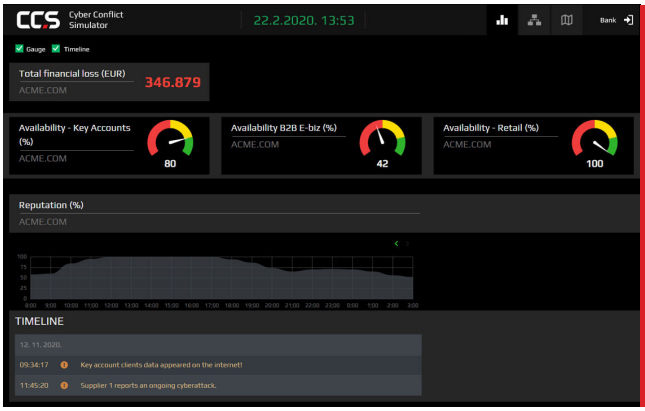
There can be several groups of participants of the simulation. Several organizations can be involved in the exercise and each of them sees only that part of the information that would be available to them in a real situation.

Participants give tasks to members of their virtual team - we call them actors. What tasks an actor can perform and how long it would take depends on his skills. Just like in reality.

The actor reports on his work and results. Based on this information, participants decide what next steps to take to resolve the incident.

During the exercise, one should often wait for the results of the actors' activities. At that point, it is possible to speed up the simulation. It can be slowed down again at any time. This allows you to perform the exercise in a much shorter time than in reality. A cyber attack that would actually last for days or weeks, with the use of CCS, will take place in just a few hours.

When cyberspace is defined it is possible to carry out an unlimited number of exercises with different scenarios. The exercise is largely determined by the resources available to the attacker and the attack techniques he uses. This results in a large number of possibilities in creating exercise scenarios.



All steps and events in the exercise are logged and are available in the simulation report. This allows the improvement of defense strategy, tactics, techniques, procedures and the entire system.

There are a number of questions important for cyber defence. Can an attack be detected early? How easy is it for an attacker to move through the organization to reach the goal? The list goes on.

To know the answers, the best way is to test it. CCS is a valuable tool for testing your IT system. It allows you to simulate various attacks on your organization and find out how easy it is to detect an attack, contain it, and finally understand what really happened.

You can introduce zero-day vulnerabilities for any component of your system and test what it means for your defence in case of attack.

Key Features

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

SCALABILITY
Model complex systems through the option to include all related organizations.

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

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
Improve the defence tactics and techniques of the team by analysing steps taken in after action review.

Conclusion

CCS

Cyber Conflict Simulator

The cyber defence link you are missing

Utilis CCS enables you to check the level of readiness of your organization to respond to cyber incidents. It helps you to test how robust your IT system is and prepare your most important part of defense - people.

CCS is created for those in charge of managing cyber incidents in the civil and military sectors. It simulates various methods of cyber attacks to your information system and allows you to define a virtual cyberspace composed of different objects.

CCS makes it easy to:

- check the reaction and performance of your system and cyber incident response team in case of attack
- test your cyber incident response procedures and communication plans
- save time and other resources needed to prepare exercises so you can do more exercises with less engagement
- simulate cyber incidents that would last for days or weeks in a matter of hours
- gain experience and skills by doing exercises with various scenarios of attack
- raise the level of awareness about the threats aimed against your IT system

Learn from mistakes - wisdom says. Mistakes in real cyber incidents are very costly.
So it is better to do them in the exercises first.
We made CCS to be very easy to use. It can also be easily extended via a plug-in system.

In the initial phase, CCS was recognized by the European Defense Agency (EDA) as an innovative dual (military and civilian) use project and selected to get technical support.

Arrange an Exercise

Everything needed to conduct the exercise can be prepared by a team of Utilis and FER experts with minimal involvement your organization. Contact us with additional questions, request a presentation or 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

Europska unija
Zajedno do fondova EU

EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI

Utilis Ltd and the project partner, Faculty of Electrical Engineering and Computing (FER), signed a Grant Agreement with MINGO and HAMAG BICRO for projects financed from the European Structural and Investment Funds in the financial period 2014-2020 (ESIF). The contract was signed for the Cyber Conflict Simulator project within the instrument "Increasing the development of new products and services arising from research and development activities"