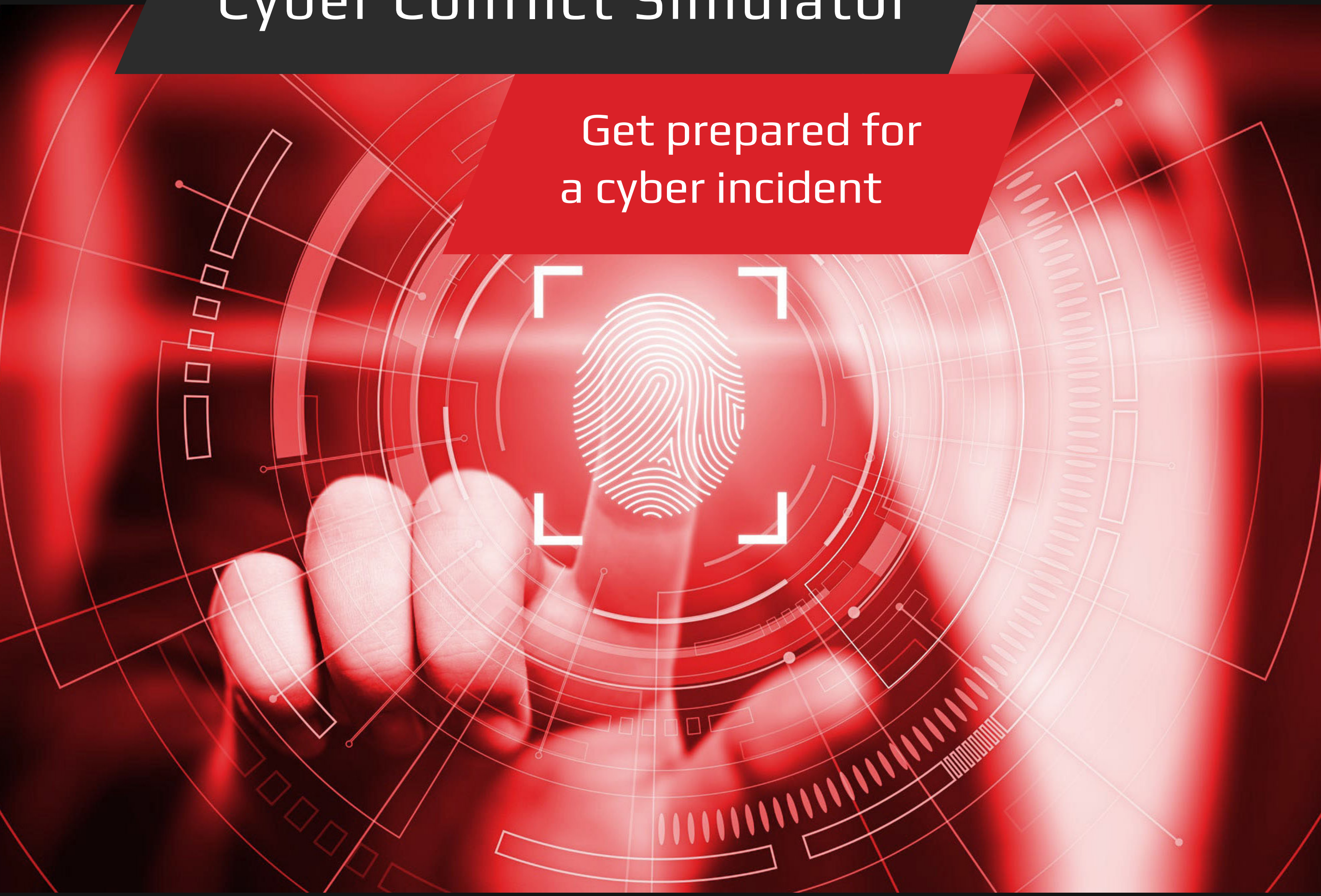
CCS

Cyber Conflict Simulator



Get prepared for
a cyber incident

Carry out a realistic cyber incident response exercise with the participation of all incident response team members.

The Context

Society's reliance on cyberspace is constantly increasing. Cyberspace is recognised as the fifth operational domain of military activity. Therefore, the preparedness of military forces through appropriate training is mandatory.

In the civilian domain, cybercriminals are becoming more skilled and daring, and their methods and vectors of attack are getting more sophisticated. Aside from the obvious and well-reported huge financial losses, cyber adversaries can cause damage that threatens critical infrastructure, utilities, services and even lives.

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

- Are you able to properly detect its cause?
- How good are you in incident containment and cause eradication?
- Can you recover your information system and business quickly?
- Have you practiced cyber incident scenarios to improve your defensive tactics, techniques and procedures based on the lessons learned?

Many organisations invest significant financial resources in cyber-attack prevention measures, both technical and organisational. It is reasonable to assume that the organisations that fall victims to cyber-attacks are the ones with lower level of cyber security maturity.

The 2022 State of Operational Technology and Cybersecurity Report from Fortinet reports that even organisations with a high level of security maturity face data breaches. Most of them had more than one such breach in the past year.

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

Cyber incidents take first place as the most significant global business risks for 2022 according to Allianz Risk Barometer.

Unlike other types of threats to organisations such as fires, earthquakes or even pandemics, cyber-attacks have an active attacker who can adapt his steps to defensive actions. That is why the course of the incident is unpredictable. There is a high level of uncertainty about the scale of the incident and how or when is started. The affected organisation is often alone in facing the incident and is therefore in the spotlight. Time is a critical factor.

The Cost of a Data Breach Report 2022 from IBM Security shows that the average cost of a data breach is higher than $4.35 million. Of the organisations studied for the report, 83% experienced more than one data breach. The report highlights one very important fact – **The average savings (reduced financial impact) in organisations with an IR team that tested their plan versus those who didn't is $2.66 million! That is a 60% cost reduction!**

This should not come as a surprise, though. In many professions people exercise for events we all hope will never happen. Airline pilots exercise regularly for emergency situations that fortunately rarely occur. Firefighters reduce response time and increase efficiency through regular emergency exercises. They all get prepared for an event in which their skills and performance can make a big difference.

When a cyber security incident happens, who would you rather have at the helm? A team that tested and proved their skills, or a team that is facing it for the first time? A team that tried different approaches and plans and learned from their mistakes or the one that didn't?

When a cyber security incident happens, who would you rather have at the helm? A team that tested and proved their skills, or a team that is facing it for the first time? A team that tried different approaches and plans and learned from their mistakes or the one that didn't?

A Good Exercise

The importance of exercises has also been recognised by regulators. Exercises are now often required for organisations of particular importance such as critical infrastructure. EU NIS and NIS2 directives state that exercises are one of the ways to effectively prepare for a possible incident.

Military professionals say, exercise the way you fight. A good exercise is the one that puts the organisation into a situation setting as close to a real-life incident as possible.

The team should be trained in an environment that is very close to the real one – including all the aspects – IT infrastructure, business services and processes, resources but also skills and expertise available to the organisation. It should allow the organisation to see the consequences of decisions made during an incident. It should engage trainees into the exercise as well.

The two most common approaches to cyber exercises are cyber range and table-top exercises.

Cyber range is aimed at technical staff: analysts, digital forensics, reversing engineers, sysadmins, etc. It is a virtualised environment running in real time in which technical tasks are performed. However, re-creating a real environment of an organisation is not an easy task here. It is difficult to take business processes into account since cyber range is not meant to do that. Therefore, it is hard to engage the management level of incident response teams.

In table-top exercises trainees discuss a given situation and make decisions. They are primarily targeting senior management. The challenge for that kind of exercise is to include the technical level since table-top exercise lack technical details. The time component of the incident is only vaguely represented as are the limitations on resources. The course of the exercise does not always depend on the trainees' actions.

Each of these approaches has its place, but involves only a part of incident response teams, not the entire teams.

Responding to a cyber incident is a coordinated effort of people in different roles. It is a demanding task that involves managing many people and activities.

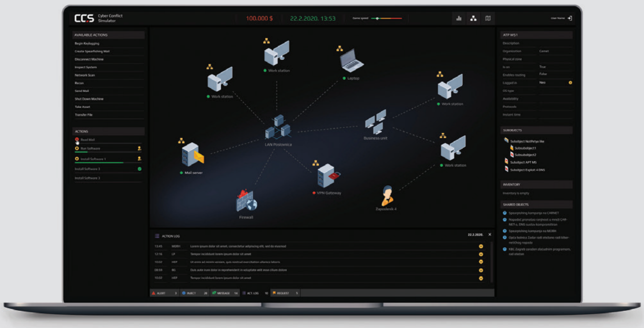
Some of the activities may take a long time but their outcome is important for decisions about the next steps. In real life, incidents can last for days or weeks, and sometimes even longer. That is a real challenge for exercises if conducted in real time. Some members of IRT might be able to take part in an exercise that lasts that long, but it is hard to single out key people from an organisation for a long period of time. During the incident, some decisions often go beyond the IT domain and enter the business sphere, so the people in key business roles are also involved.

With all this in mind, preparing, organising and conducting an exercise becomes a challenging endeavour. It’s unlikely organisations can carry out such exercises often enough to gain experience in a reasonable time.

Cyber Conflict Simulator

All of these challenges led to the development of Cyber Conflict Simulator (CCS), an interactive simulator that tackles the response to a cyber incident in a different way. CCS is a software system designed for cyber security incident response teams, in both civil and military sectors, to help them get prepared for an incident.

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



```
13:45  MORH  Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod
12:16  LP    Tempor incididunt lorem ipsum dolor sit amet
10:02  HEP   Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris
08:59  BG    Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore
10:02  HEP   Tempor incididunt lorem ipsum dolor sit amet
```

CCS is a software system designed for cyber security incident response teams, in both civil and military sectors, to help them get prepared for an incident.

Simulation Environment

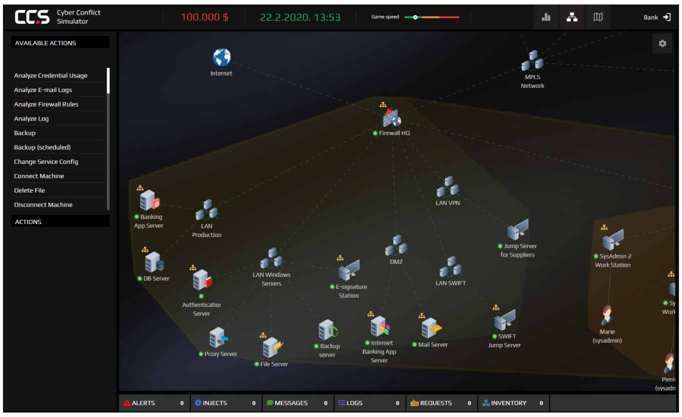
Imagine having a simulation environment that models your IT/OT systems and business processes and services the way they are in real world. IT/OT systems are described with computers, servers, networks, software, data, SCADA systems, etc. Implemented security controls (AV, Firewalls, SIEM, Logs, AAA, etc) are also added.

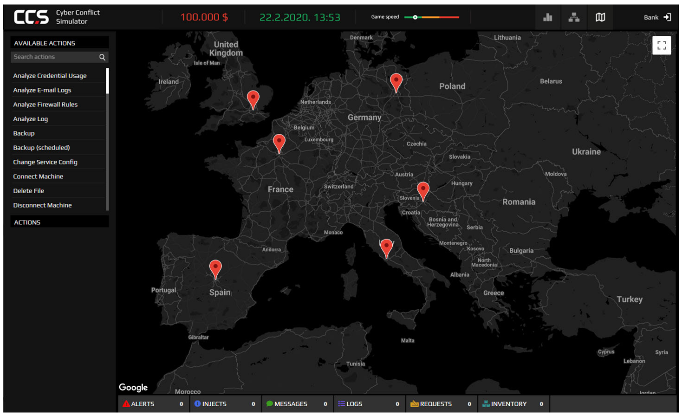
Business processes and services are modelled with their dependence on IT/OT systems - events on the IT level may impact business processes. Possible consequences of an attack like damages or losses are also described. Consequences may range from financial and reputation losses to loss of human lives.

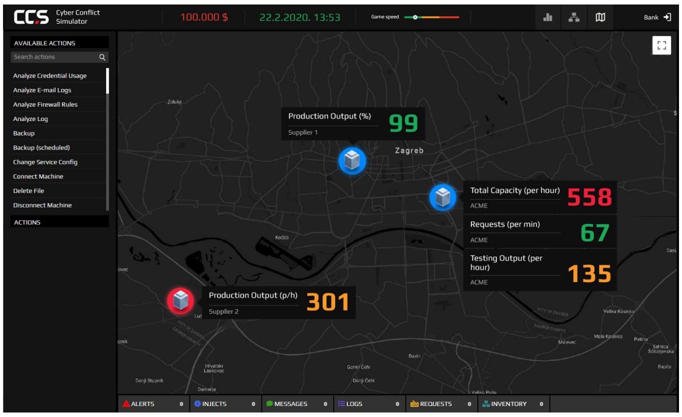
People are an important part of any organisation: system administrators, digital forensics, technicians, analysts and all other staff. They are modelled with their skills, security awareness, public exposure and habits, and managed by the participants of an exercise during simulation.

To simulate the attacker there are a variety of sources of threats to choose from: states, criminal groups, or individuals, based on threat intelligence sources or risk assessment. Different attack groups can be easily mimicked, along with their tactics, techniques, and procedures.

Simulation







The simulation can be carried out according to predefined scenarios and prepared steps or with the active participation of a red team. Attack steps are simulated respecting all limitations due to network architecture and implemented security controls.

The exercise may start when offensive activities begin, or it can start later when the attackers has already achieved some of their goals. This is left up to the author of the scenario.

Participants may be in one group or separated into different roles, depending on the goals and objectives of the exercise. These roles correspond to the typical roles of an incident response team: IT team, OT team, incident response manager, technical lead, recovery manager, business process owners, management, etc.

Participants assign tasks to members of their virtual team, we call them actors. What tasks an actor can perform and how long it will take depends on his skills, just like in real life. During the task execution, the actor reports on his work and results. Based on this information, participants decide on the next steps to take to resolve the incident.

Business oriented roles need to make business decisions (i.e. stopping or restoring processes or services, allocating resources, etc), take care of regulatory or legal aspects of the incident, communication with stakeholders, etc.

During the exercise, simulation time can be sped up or slowed down so that trainees are fully engaged and the exercise can finish in a reasonable amount of time. An incident that would last for days or weeks can, with the use of CCS, unfold in just a few hours.
Several organisations can be involved in an exercise and each of them will see only part of the information that would be available to them in a real situation.
The simulation is interactive, realistic and immersive.

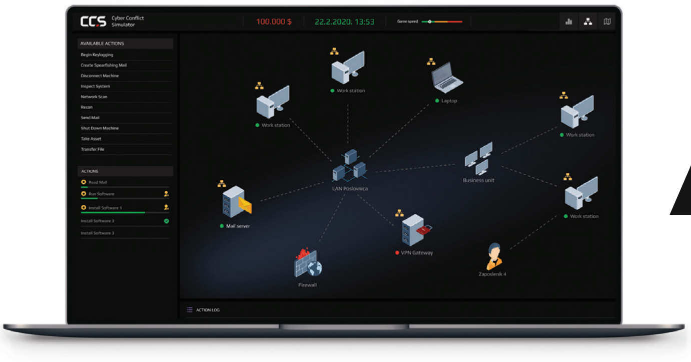
All steps and events in the exercise are logged and are available in the simulation report. This allows the improvement of defense strategy, tactics, techniques, procedures and the entire system.

Once the simulation environment 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 used. This allows for many possibilities when creating exercise scenarios.

All steps and events in the exercise are recorded and are available in the simulation report. This enables an analysis of the effectiveness and efficiency of defensive activities and the communication between roles and stakeholders. It helps verifying if the team follows playbooks and procedures during an incident. An analysis of the effectiveness of technical measures can also be performed.

CCS provides the option to analyse attack steps. Get to know your enemy. Different APT groups use different tactics, techniques and procedures (TTPs) for attack. Recurring exercises using different TTPs increase the organisation’s capabilities in incident response. All of this provides the content of the lessons to be learned after an exercise.

Conclusion



CCS

Cyber Conflict Simulator

Get prepared for
a cyber incident

CCS can be used to assess the level of readiness of the organisation to respond to cyber incidents. It helps to test how robust the IT system is and to prepare the most important part of defence, the people.

There are many benefits of exercises using CCS, to name just a few:

- testing incident response playbooks and procedures, evaluating whether they need to be amended and observing how they are followed by the IRT
- verification of communication procedures
- investigation skills training
- performing what-if analysis
- testing BCP plans
- understanding the longer-term consequences of the incident
- increasing confidence in making decisions with limited information
- preparing to defend decisions to the media, shareholders and regulators

One should learn from mistakes, the old wisdom says. Mistakes in real cyber incidents are very costly, it's always better to make them in a controlled simulation environment.

CCS is very easy to use. It enables exercises to be organised more often and be performed in a way that really makes a difference. A complete solution with less effort.

Get prepared for a cyber incident!

Arrange an Exercise

Everything needed to conduct the exercise can be prepared by our team or our partner's team of experts with minimal involvement from your organisation. Contact us with additional questions, request a presentation or arrange an exercise tailored to your organisation.

utilis

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

diverto

Ulica Filipa Vukasovića 1
10000 Zagreb
Hrvatska
www.diverto.hr
diverto@diverto.hr
sales@diverto.hr

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"