

Why CCS?

Cybersecurity resilience isn't just about technology — it's about people, processes, and decisions made under pressure. CCS provides a safe, realistic environment to rehearse incident response, validate procedures, and build organizational confidence.

Key Benefits



REALISTIC SCENARIOS

Tailored to your infrastructure, risks, and threat landscape.



WHOLE-TEAM ENGAGEMENT

From IT staff to executives, everyone trains in their actual role.



EFFICIENT TRAINING

Multi-day incidents can be simulated in just hours.



STRONGER CAPABILITIES

Teams become faster, more coordinated, and more resilient.



LONG-TERM VALUE

Reusable cyber landscape enables continuous training across a wide range of scenarios.



ATTACKER INSIGHTS

Understand adversary tactics, techniques, and procedures (TTPs).

Become a CCS partner

We are building a network of trusted partners - consultants, system integrators, and training providers - who want to deliver advanced cyber exercises with CCS.

WHAT WE OFFER

- Partner Training – Learn to design Cyber Landscape, scenarios and conduct exercises.
- Ongoing Support – Assistance tailoring exercises to end users' needs and requirements.
- Scalable Engagement – Use CCS for projects or as part of services.

WHY PARTNER WITH US

- Add high-value services
- Differentiate your offering
- Strengthen client relationships
- Expand your capabilities
- Deliver cutting-edge cyber incident response training

+385 (1) 36 35 666

info@utilis.biz



Utilis Ltd. | www.utilis.biz | ccs.utilis.biz



Co-funded by
the European Union

Scan for other
languages



CCS Cyber Conflict
Simulator

Train your organization to command a cyber crisis

A cyber wargaming platform
to strengthen **your organization's**
cyber resilience.

Cyber Security Context

In today's hyper-connected world, cybersecurity has become a critical concern for individuals, businesses, and governments. State-sponsored attacks, financially motivated crime, and hacktivist movements evolve faster than defenses.

Frameworks such as the EU's DORA and NIS2 demand stronger cyber resilience. Organizations must ensure not just data protection, but continuity of essential services during and after incidents.



CYBER INCIDENTS

For several years in a row, cyber incidents are the top global business risk. Organizations invest significant resources in prevention measures, both technical and organizational. It is equally important to invest in preparedness.

WHY PREPAREDNESS MATTERS?

Tested incident response plans and a well-trained incident response team can significantly reduce data breach costs, according to IBM research.

Preparedness means having:

- **A Solid Plan** – Customized IR plans, tested in realistic scenarios, reveal gaps and define roles.
- **A Trained Team** – Practice under pressure builds coordination.



CCS Cyber Conflict Simulator

CCS is a cyber wargaming platform that simulates realistic attack and defence scenarios. It enables modelling of a digital twin of IT/OT systems, business processes, and people, helping organizations strengthen their incident response readiness and decision-making under pressure.

How It Works

CYBER LANDSCAPE

CCS Cyber Landscape (CL) is a digital twin that mirrors your IT/OT systems and business processes as they exist in the real world. Business processes depend on the underlying IT/OT systems, so technical events can disrupt operations and lead to financial losses, reputational damage or even threats to human life.

People are part of the model, too — administrators, analysts, technicians, and other roles, each represented by their skills, awareness, and habits.

Realistic adversaries and attack behaviours can be simulated, representing a wide range of threat sources, from state-sponsored actors and cybercriminal groups to individual attackers. Their actions are based on intelligence-driven tactics, techniques, and procedures (TTPs). Once the Cyber landscape is set up, you can run unlimited exercises with diverse attack scenarios.

SCENARIO

Each exercise scenario is tailored to its objectives and can be based on threat intelligence or risk assessments. CCS supports a wide range of attacks and can simulate vulnerabilities across hardware and software. Scenarios can be recorded and replayed or saved as starting points for future exercises.

Participants are assigned realistic roles — Incident Commander, Technical Lead, IT Operations and Network Administrators, Management, Business Owners, CISO, Domain Experts, PR Lead, Legal Counsel, and HR — mirroring real-world responsibilities and cross-functional coordination.

SIMULATION

CCS simulates both technical events and their business impacts. Exercises can follow predefined attack sequences or live Red Team activity, starting at an early detection stage or later escalation. Participants interact with virtual team members whose actions reflect their skills and capabilities. Time scaling compresses days of activity into hours, enabling realistic, time-efficient exercises.

AFTER-ACTION REVIEW

Every action, decision, and message is recorded with verbose information. After the exercise, CCS provides detailed reports to evaluate effectiveness, coordination, and IR procedures - helping teams learn, adapt, and continuously improve IR processes.

Review Insights

- Effectiveness of actions to detect, verify & triage, scope, contain, eradicate and recover
- Communication and collaboration among roles and stakeholders under pressure
- Strengths and gaps in existing IR procedures and playbooks
- Effectiveness of firewalls, EPP, EDR, DLP, and other security controls
- Attacker Tactics, Techniques, and Procedures (TTPs) observed
- Priority areas for improving technical defenses and organizational procedures.