



# The Cyber-Range Solution

Offering a digital twin environment to support your cybersecurity posture



[nexovagroup.eu](https://nexovagroup.eu)

Nexova's Cyber Integration, Test and Evaluation Field (CITEF) provides an interactive emulation of an organisation's local network, systems, tools and applications. Its highly accurate representation of both information and operational technology assets powers our cyber-range services, which are used across industry and within critical infrastructures for cybersecurity testing, planning and training.



### Why organisations need CITEF

The complexity and frequency of cyberattacks on organisations and individuals continues to escalate at an alarming rate, costing billions of euros every year and creating a challenge for senior management. To help combat this, organisations across all industries are accelerating their digital transformation, introducing new information technology (IT) and operational technology (OT), which is resulting in more complex interconnected systems.

When an attack or breach occurs, it is important to ensure your IT and security teams are ready to respond quickly and mitigate the impact. High-fidelity emulation solutions are a cost-effective way to address cyber vulnerabilities and strengthen an organisation's overall digital resilience. This is where Nexova's cyber-range service and emulation solutions can help your organisation accelerate its digital transformation and strengthen your cybersecurity posture.





## What is a cyber-range?

Cyber-ranges are interactive and simulated platforms that provide digital replicas of networks, systems, tools and applications. They provide a safe and legal environment for acquiring hands-on cyber skills and a secure setting for product development and security posture testing. They also have a crucial role to play in facilitating and promoting cybersecurity education, training and certification.

Our cyber-range solution offers a multi-purpose virtualisation or digital twin environment that supports three main services:

- ✦ Improved system assurance in development (R&D)
- ✦ Knowledge development and dissemination (training)
- ✦ Improved system assurance through evaluation (testing).

When an attack or breach occurs, it is important your IT and security teams are ready to respond quickly.





## Introducing CITEF

The most effective preparation for any cyberattack happens in a real-life environment, but that is not always practical. The most secure infrastructure is one that is fully tested and risk assessed without endangering any live operational setup.

Nexova's CITEF is an interactive emulation of an organisation's local network, system, tools and/or applications.



CITEF supports advanced simulation capabilities, allowing employees and students to engage in realistic and dynamic hands-on exercises. It offers a versatile and customisable platform for R&D and testing environments that can be loaded with pre-built training scenarios, allowing trainers and students to create and modify their own scenarios.

## The CITEF platform

CITEF offers a comprehensive platform that is designed to work the way your business works, with its visual front-end and template-based environment modelling. With its user-friendly interface for scenario development and instantiation, and drag-and-drop functionality, our CITEF cyber-range platform allows you to:

- ✦ Develop and continually enhance your security team's skills
- ✦ Enhance cyber awareness among non-security staff
- ✦ Build a truly realistic emulation of your assets (OT+IT), not just a simple simulation
- ✦ Spin up training and test environments in minutes in a safe, legal environment
- ✦ Generate hybrid scenarios using both digital and physical assets
- ✦ Conduct technical, hands-on, tabletop exercises for your security team
- ✦ Ensure your infrastructure remains secure by running regular, automated tests
- ✦ Prepare and test your incident response plans
- ✦ Design, develop and evaluate new products and services with security in mind – security by design
- ✦ Implement a digital twin for critical infrastructures including Supervisory Control and Data Acquisition (SCADA), industrial control systems (ICS) and Internet of Things (IoT).

## CITEF benefits

CITEF offers a unique combination of features and benefits, allowing you to:

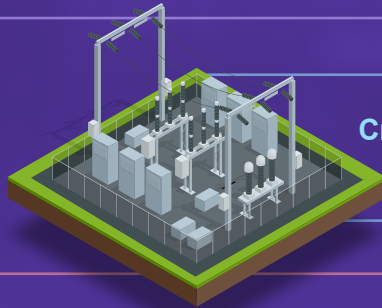
- ✦ Train your security and non-security teams in a 'real-life' environment
- ✦ Be flexible, easily creating diverse scenarios with virtual and physical assets
- ✦ Customise environments with cutting-edge technology and automatic traffic generation
- ✦ Choose from 50+ pre-built scenarios, or customise your own
- ✦ Emulate both OT and IT for realistic training, including running 'red and blue team' scenarios seamlessly.



## Multiple domains

CITEF is being used in many domains internationally:

**Commercial sector** – banking, chemical sector, New Space, unmanned aerial vehicles (UAVs)



**Critical infrastructures** – defence, maritime, space, power grids, hospitals, railways, aviation

**Institutions** – European Commission, NATO, European Defence Agency (EDA), European Defence Fund (EDF), European Space Agency (ESA), police, education, research centres





“ I am passionate about making people aware of cyber threats and cybersecurity. Using the flexible CITEF platform helps bring real-world learning to multiple learners from multiple organisations and backgrounds. I believe this kind of training should be offered by all educational facilities, especially post-secondary institutes where cyber-range training should be added to their curriculum, as well as being implemented by companies that have their own security operation centres and want to enhance their security skillsets. ”

**Trish Dyl** – Director, Corporate Training and Cyber-Range  
at the Rogerson Cybersecure Catalyst

## A cyber-range for digital twins

With modern cyber-range/emulation technology, it is now possible to emulate a real infrastructure with a high degree of affinity, with (near) real-time traffic monitoring, and semi-automatic scan and discovery of the original system.

CITEF is perfectly suited to work as an emulation-based digital twin, acting as a true-life replication that emulates your systems and networks. It allows students to experience dynamic interactions, for real-time testing with different scenario creations. The high-fidelity replication enables users to accurately mirror real-world environments, giving them hands-on, real-life training, as well as providing asset recovery after an attack.

## Using AI in cyber-ranges

Artificial intelligence (AI) is being used increasingly to enhance specialised applications, including cyber-ranges. Its versatility can support cyber-range training by providing simulated attacks and fostering realistic and varied attack scenarios. AI is part of the CITEF roadmap moving forward where we are looking to identify how it can best be adapted to react to trainee actions and simulate potential human user behaviour.

## Nexova Cyber Centre of Excellence

The Nexova Cyber Centre of Excellence in the Galaxia Business Park in Transinne, Belgium, is dedicated to supporting critical infrastructure organisations in the secure design, operation and use of their IT and OT



systems. This 3,300m<sup>2</sup> state-of-the-art infrastructure is a centre for cybersecurity protection and training, including a cyber-range and security operations centre (SOC).

The facility provides R&D labs, radio frequency (RF) cybersecurity and incident response services, and is specially designed to enable us to provide an array of tailored cybersecurity services and support. This includes comprehensive cybersecurity training and certification for professionals

and students, a SOC staffed with highly qualified security experts, cyber training rooms to enable dynamic live and virtual classrooms and a technology lab dedicated to research.



Nexova Group SA, Rue des Etoiles 140, 6890 Libin, Belgium

✉ [info@nexovagroup.eu](mailto:info@nexovagroup.eu)  [nexovagroup.eu](http://nexovagroup.eu)