

# Protecting Europe's Heartbeat

We maximise our clients' cyber resilience and foster digital trust through our advanced technologies and solutions



Nexova 

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

# Introducing Nexova

Nexova is a privately-owned Belgian company that combines engineering solutions and cybersecurity services for critical infrastructures and operations across Europe. Our passion lies in enabling organisations to embrace digital transformation while building trust and resilience to shape a more secure tomorrow.

## Our vision

At Nexova, we have a bold vision: to secure the vital assets of critical infrastructures, enhancing resilience to ensure sustainable growth in an increasingly digital economy.

We help clients protect their operations and support them in driving competitiveness and gaining customers' trust.

We also assist our clients as they navigate the changing legislative landscape, enabling them to understand what it means to their organisation, and identify and set up the right tools and processes to comply with all relevant acts and directives. We make sure they are aware of all their responsibilities and their accountability for cybersecurity governance and risk decisions defined by new European regulations. These include the Network and Information Security 2 (NIS2) Directive, the Artificial Intelligence Act (AI Act), the Cyber Resilience Act (CRA) and the Digital Operational Resilience Act (DORA).

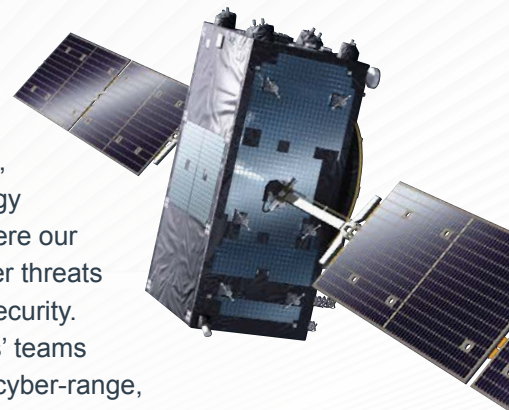
**Nexova – your trusted partner through the entire cybersecurity value chain.**

## Our DNA

With our roots in securing the most complex space missions, we are pioneering new technologies to help protect European space, defence and other critical infrastructures from cyber threats and make them more resilient in the future.

Innovation is at the heart of our organisation. Our cybersecurity specialists work with multiple custom-built solutions to take care of every aspect of our clients' cybersecurity needs. Our capacity to innovate is demonstrated in our brand new,

Nexova Cyber Centre of Excellence, a marvel of technology and architecture, where our experts mitigate cyber threats with a high level of security. Here, we train clients' teams using our advanced cyber-range, we manage any crisis with the highest levels of secrecy and we help our clients recover their critical data.



# 30%

of organisations deploying AI have experienced AI-related security breaches.

Source: [Gartner \(2024\) AI in the Enterprise Survey](#)

# Our Cyber Centre of Excellence

The Nexova Cyber Centre of Excellence is a unique, highly secure, self-sustaining facility located in Europe's newest Cyber Valley in the Belgian Ardennes. Hidden in the wide open, it is the beating heart of our company.

The Centre offers state-of-the-art training facilities, ultra-secure security operations centres (SOCs), a technology lab, office space and secluded data centres in a unique setting designed to serve the needs of European critical infrastructures and defence organisations. Its classified environments enable service delivery up to SECRET level.

In an era marked by evolving threats and interconnected vulnerabilities, safeguarding defence assets and critical infrastructures is paramount. Our unified approach, with all facilities and services sited in one place, offers a comprehensive solution to fortify organisations against the complexities of modern security challenges.

## Facilities

Our modular building features six distinct zones across two floors tailored to specific needs:



**Ground floor** – Reception, conference rooms, cyber-range and laboratories; all designed to facilitate daily operations while maintaining a robust defence posture.

**Lower level** – Classified zone, SOCs, incident management, post-incident management; this is the nerve centre of our operations, housing critical systems and resources, hidden from view.

# 89%

of organisations will require more cybersecurity staff to comply with NIS2.

Source: [NIS Investments 2024](#), ENISA



# Deter Detect Delay Respond

## Maximum security

Our Centre is designed to provide maximum security where it's needed most, making it ideal for organisations providing sensitive and classified services, especially critical infrastructures. Its self-sustaining features include its power supply, network infrastructure, data centres and network providers, and it is designed to meet all relevant European security standards.

Multiple layers of defence and security technologies are strategically implemented to create overlapping barriers against threats, including access control and intrusion detection and response.

Our 'Defence in Depth' system:

**Deter** adversary attempts

**Detect** unauthorised access as early as possible

**Delay** adversarial action sufficiently to allow effective response

**Respond** before harmful actions can start

## A centre for innovation

Our Centre is designed to enable continuous pursuit of innovation and technological leadership in cybersecurity.

Our investment in R&D at the Centre includes: quantum-safe communication solutions; application of artificial intelligence (AI) and machine learning for cybersecurity; radio frequency (RF) lab for space and drone-related applications; cyber-range development; digital twin technology; and security in industrial control systems and operational technology.

Our innovation and development at the Centre take full account of all European regulations and directives, including the AI Act, which will pave the way towards a safer and more transparent AI ecosystem. The Centre's R&D facilities and cyber-range are available for our customers to use, as well as our in-house cybersecurity experts.

The average cost of a data breach has risen to

**€4.4 million**

Source: [IBM. 2024 Data Breach Report](#)

## Our Service Offering

Operating from a central European location, we offer a comprehensive range of advanced cybersecurity services and solutions. We solidify our clients' cybersecurity posture and build trust through our advanced technologies and solutions.



Our services include:

- \* Cybersecurity training for IT and non-IT staff, up to and including C-suite executives
- \* Cyber-range and emulation services, maximising security by using digital twins
- \* Cybersecurity managed detection and response services
- \* Tailored engineering services
- \* Consulting services
- \* Cybersecurity facilities at our Cyber Centre of Excellence.

### Meeting regulatory obligations

In the context of a strengthened European regulatory framework for cybersecurity, organisations – especially their CEOs and Board members – face increasing obligations to safeguard their activities against cyber threats. Our mission is to support organisations in implementing tools and processes that enable them to prevent, detect and respond swiftly to cyberattacks with tailored solutions while meeting their regulatory obligations.



EU regulations aim to elevate the level of cybersecurity across the Union, but they present substantial challenges for cybersecurity teams. Our cyber experts help our clients achieve compliance with current rules and anticipate future changes, ensuring they stay ahead in this evolving landscape. This includes those using disruptive technologies powered by AI and/or machine learning, which present both opportunities and threats in terms of cybersecurity.

We help organisations and senior management understand the implications of new regulations and support them in meeting their obligations in aspects such as:

- \* Risk analysis and management
- \* Developing and updating information system security policies
- \* Incident handling
- \* Business continuity planning and crisis management
- \* Supply chain security analysis
- \* Training for management, Board members and staff.

## Cybersecurity training

Nexova's cybersecurity training is powered by our cyber-range platform (CITEF), which uses our proprietary emulation technology to create a realistic digital replica of any IT/OT infrastructure. Using our cyber-range, your teams will receive cybersecurity training based on real-life cyberattack scenarios presented in an emulation of your business environment.

This unique approach to cyber training maximises the learning value for your teams. Being highly flexible and customisable, our digital emulation platform allows us to tailor a training environment that meets specific educational needs. Training can be provided remotely or in our state-of-the-art cybersecurity classroom located at our Cyber Centre of Excellence in Transinne, Belgium.





## Cyber-range and emulation services

Nexova's advanced digital twin platform, CITEF, can easily create a virtual replica of your IT/OT environment that can be used for a wide range of purposes:

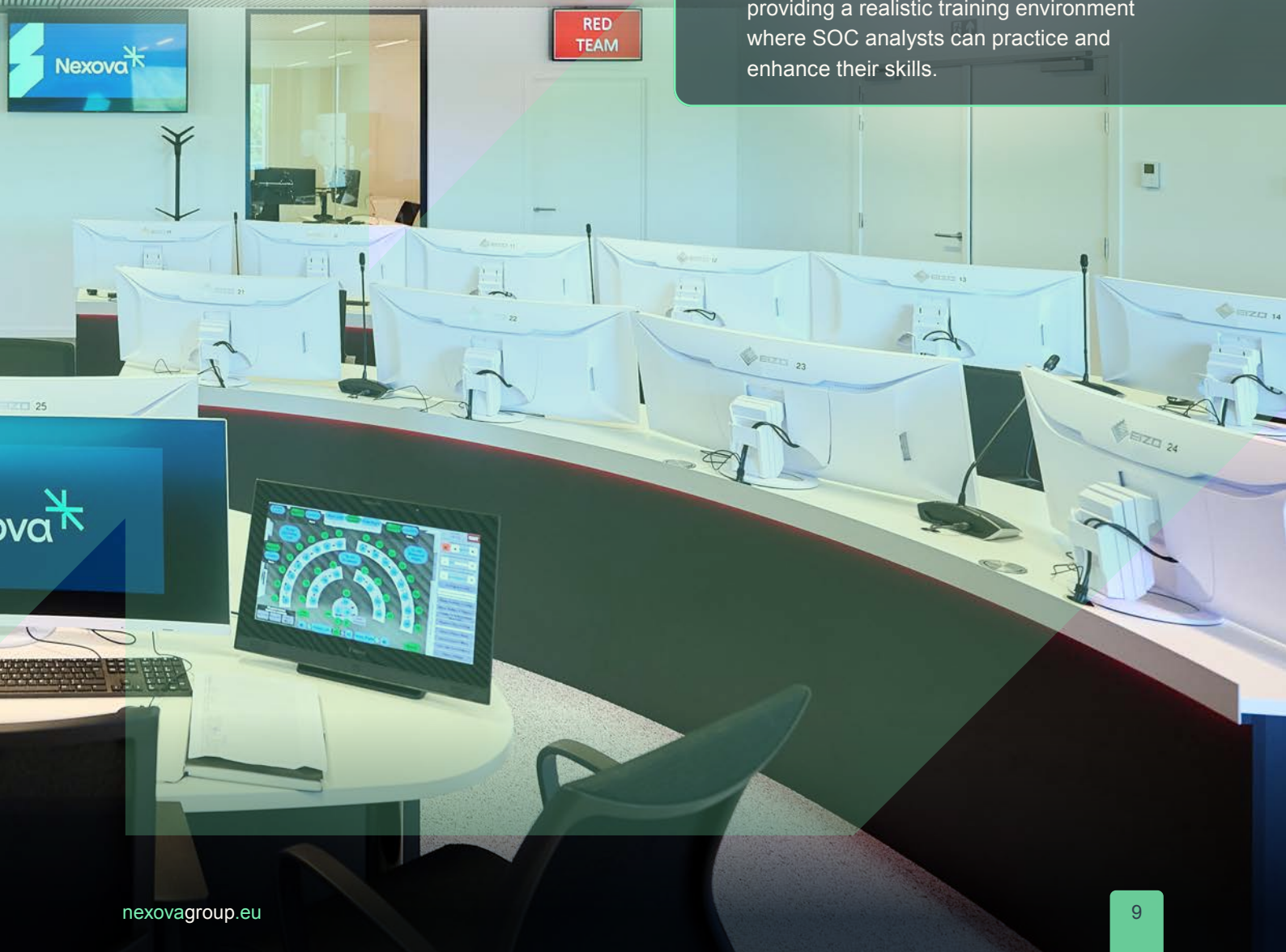
- \* Prepare for the integration of new complex systems or additional IT/OT elements in your operational infrastructure
- \* Assess the security vulnerabilities of your operational environment in a safe manner
- \* Validate new versions of architectures, software and operating systems
- \* Rehearse and improve incident response plans through table-top exercises
- \* Train operators of your security systems.

Our solution can be adapted to your needs and delivered on premise or as a service. In the latter case, our platform is hosted on our multi-tenant, secure private cloud.

### Why use a digital twin with a SOC?

Combining our digital twin solution with SOC services offers unique synergies that can help with many different scenarios. These include:

- \* Enhancing SOC monitoring and detection and identifying potential threats in a controlled, virtual space before they impact operational systems
- \* Improving SOC incident responses
- \* Enabling SOC threat hunting, providing a sandbox environment to test and validate techniques in a safe environment
- \* Delivering comprehensive security training, providing a realistic training environment where SOC analysts can practice and enhance their skills.



## Cybersecurity managed detection and response services

Our cybersecurity managed services combine a multidisciplinary team with extensive cybersecurity expertise and knowledge of advanced European technology, together with our purpose-built SOC located at our Cyber Centre of Excellence. This enables us to continuously monitor your connected systems, proactively detect cyber incidents and help you act when needed.

In addition to providing continuous monitoring and alerts, our services include vulnerability management, endpoint detection and response (EDR), network detection and response (NDR), built-in threat-hunting intelligence and incident response.

## Tailored engineering solutions

At Nexova, we provide tailored engineering solutions that we adapt to your organisation's unique requirements. Our teams of highly qualified engineers can support you in the design, build, maintenance and continuous improvement of your cybersecurity infrastructures, systems and processes.

Whether it is for precise cyber monitoring and alerting services, training, R&D or complex systems integration and testing, all our advanced engineering solutions are customisable. Our portfolio includes, but is not limited to, custom-designed SOCs, cyber training labs and digital twin solutions, all created and developed to fit the needs of your organisation and market sector.

“ Cybercrime is the greatest threat to every company in the world. ”

Ginni Rometty – Former CEO of IBM

## Consulting services

Our dedicated cybersecurity experts and analysts provide a range of service offerings tailored for critical infrastructure sectors, influenced by strong European Union regulations and in response to complex cyber threats. These services are aimed at guiding organisations to obtain an objective view of their current cybersecurity posture and in setting up their cyber resilience and business continuity strategy.

Our tailored approach towards strengthening defence against cyber threats carefully considers the triad of people–processes–technologies, with an emphasis on the human factor that is crucial for business operations. As experts in EU regulations and directives, we can help you make sure your organisation is compliant, saving you time and effort.



## Cybersecurity facilities

Our Cyber Centre of Excellence offers state-of-the-art workspaces designed to foster collaboration while meeting the highest security standards. These secure environments are complemented by secluded data centres, ensuring the integrity and confidentiality of sensitive information. By combining a modern infrastructure with advanced security measures, we provide a trusted space for organisations to address their most critical cybersecurity challenges.

**We are Nexova. Protecting Europe's heartbeat.**



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

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