

## CYBERSECURITY SIMULATION EXERCISES

This competency provides realistic, risk-free cybersecurity training through cyber range simulations that improve organisational preparedness, resilience, and incident response. It delivers guided scenarios, red/blue team exercises, and Capture the Flag (CTF) challenges tailored to technical maturity and sector needs. The activity supports NIS2-aligned capability development while strengthening security awareness across technical teams and decision-makers.



### ACHIEVEMENTS

- Deployed cyber range-based simulation platforms for organisations of different sizes.
- Organised CTF competitions and cybersecurity bootcamps for students and professionals.
- Executed guided cyber-attack and response simulations to test organisational resilience.
- Supported NIS2-related training through simulation-based security programmes.



### INFRASTRUCTURE

- Customisable cyber range simulation environments.
- Red/blue team operational and exercise platforms.
- CTF infrastructure with user simulation and reporting workflows.
- SOC-style, OS-independent training environments.
- Remote and on-site deployment capability.



### REFERENCES

- Industrial Cyber Defence Exercise delivered with BOSCH.
- Cyber range development and training collaboration with the National Security Service (NBSZ).
- Cyber awareness and simulation programme with the Ministry of Defence (HM).
- Collaborative cyber exercise framework with the University of Public Service (NKE).