ICE & T Cyber Range

The Cyber Range IT Competence Education & Training (ICE & T) is the central laboratory for realistic cybersecurity trainings as well as for the evaluation of novel security products and approaches at the Research Institute CODE. It offers a platform for learning and deepening of Cyber Network Operations competences with a strong focus on teamwork.

How to Find Us

Research Institute Cyber Defence (CODE)
Universität der Bundeswehr München
Carl-Wery-Str. 22
81739 Munich
Germany

code@unibw.de
+49 89 6004-7302 or -7303
www.unibw.de/code

Twitter: @FI_CODE
LinkedIn: Forschungsinstitut Cyber Defence (CODE)
YouTube: Forschungsinstitut Cyber Defence

Further Information

www.unibw.de/code/forschung/zentralabore/cyber-range

 OUR TRAININGS

Basic Training
Investigate cybersecurity incidents in teams (up to six trainees):
• Understand attackers’ intentions
• Analyze heterogeneous systems
• Comprehend incidents
• Take measures
• Create awareness

Advanced Training
Improve your team’s efficiency:
• Detect and investigate complex attacks
• Coordinate your team’s activities
• Document security incidents and countermeasures
• Deepen your knowledge

Individual Training
Focus on your needs:
• Train on customized network topologies
• Test your new cybersecurity solutions
• Use individually defined attack vectors
• Discover various domains (SCADA/IoT)

Details and Infrastructure

Further Information

www.unibw.de/code/forschung/zentralabore/cyber-range
The currently available scenarios at ICE & T are grouped into different categories:

- Cyber Incident & Response Management (CIRM) Level 0–2
- Supervisory Control and Data Acquisition (SCADA)
- Penetration Testing (PT)

In CIRM Level 0, 1, 2, and SCADA, multiple automated attacks are used in three different virtual network infrastructures to simulate cyber incidents. These attacks include Denial of Service, Remote Access Trojan, Ransomware, and others.

For PT Trainings, a virtual network infrastructure with multiple, partly vulnerable systems is available. The missions include Social Engineering, SQL Injection and more. Individual, customer-specific training is possible.

The ICE & T Cyber Range is a comprehensive and adaptive solution. It provides the following options:

- Integration of IT security solutions for testing and/or training purposes
- Hardware component integration
- Creation/import of new, own content
- Customization/creation of training environment topologies

ICE & T is fully virtualized on a server cluster using VMware ESXi hypervisor. More than 400 virtual machines are used to enable multistage scenarios as well as over 80 individual exercises and back-office services.

The modular architecture also enables the integration of hardware components such as IoT and SCADA devices.