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)

ICE & T Cyber Range

The **C**yber **R**ange **IT** **C**ompetence **E**ducation & **T**raining (ICE & T) is the central laboratory for realistic cybersecurity trainings as well as for the evaluation of novel cybersecurity 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/zentrallabore/cyber-range

Editorial Staff: Lisa Scherbaum, Team Cyber Range / FI CODE; Pictures: C. Siebold, T. Mittermeier / UniBw M, Adobe Stock; Creation: M. Berwanger / Tausendblauwerk, www.tausendblauwerk.de

der Bundeswehr Universität München

CYBER RANGE

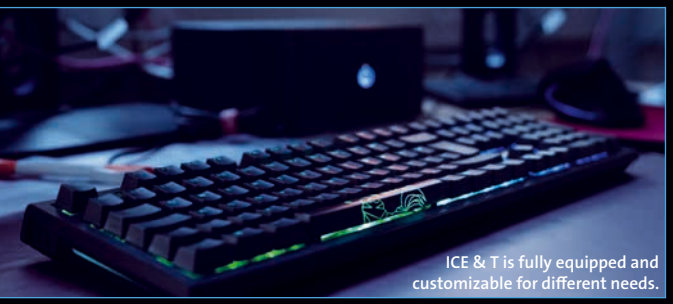
Details and Infrastructure

ICE T

IT Competence
Education & Training

Research Institute
Cyber Defence
Universität der Bundeswehr München

ICE & T



ICE & T is fully equipped and customizable for different needs.

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

Internal Infrastructure

Classrooms

RI CODE has two fully equipped classrooms for teams of up to six participants each. The rooms are designed for collaborative work. Multiple touchscreens, whiteboards and flipcharts help the participants to keep track of the scenario and work as a team. The powerful workstations allow access to the training environments via remote desktop connection and are equipped with multiple monitors to enable parallel research and documentation. Up to six classrooms are supported by now.

Training Environment & Scenarios

The currently available scenarios at ICE & T are grouped into different categories:

- **C**yber **I**ncident & **R**esponse **M**anagement (CIRM) Level 0–2
- **S**upervisory **C**ontrol **a**nd **D**ata **A**cquisition (SCADA)
- **P**enetration **T**esting (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.

Backoffice & Trainer Room

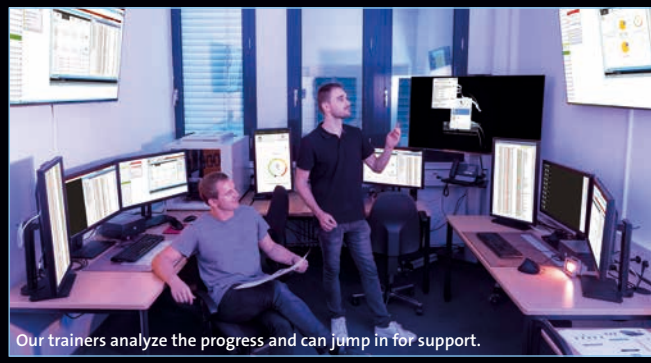
The trainer room is equipped with three workstations, each with three monitors and a TV screen that can mirror the screens of the classrooms. The remote sessions of the trainees can be supervised via a multi-platform remote control software. This enables analyzing the activities of a team during the training session.

ICE & T's classrooms are made for team training.

Core Infrastructure

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 backoffice services.

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



Our trainers analyze the progress and can jump in for support.