Realistic Environment for IT Security Training

CYBER RANGES

In the event of cyberattacks, experts must be able to act without delay.

The increasing number of IT security incidents worldwide makes well-trained and field-tested professionals highly demanded experts. In order to be able to defend more efficiently against sophisticated attacks, IT security teams have to be trained on realistic scenarios. Cyber Ranges create a unique virtualized training environment in which a variety of security incidents and real-life attacks can be simulated. At the Research Institute CODE, the Cyber Range ICE & T (IT Competence Education & Training) is the central laboratory for realistic training in cybersecurity and for testing new cybersecurity products.

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, Pasko Maksim / Shutterstock; Creation: M. Berwanger / Tausendblauwerk, www.tausendblauwerk.de

Universität der Bundeswehr München

ICE T
IT Competence
Education & Training

CYBER RANGE

CODE RI Research Institute Cyber Defence
Universität der Bundeswehr München

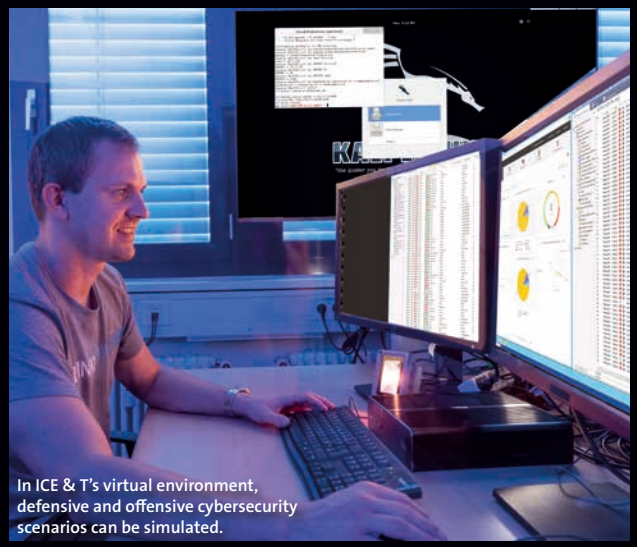
ICE & T Cyber Range

The Cyber Range IT Competence Education & Training (ICE & T) is a comprehensive and flexible solution for real-world cybersecurity trainings.

It offers a platform for learning and deepening of Cyber Network Operations competences with a strong focus on teamwork. ICE & T also enables the evaluation of novel cybersecurity products and approaches. During the trainings, defensive and offensive cybersecurity scenarios are simulated in a virtual environment. Trainees learn to investigate, analyze and mitigate attacks or use offensive techniques on their own in real-world scenarios.

Training Types

- Basic Training: Investigate cybersecurity incidents as a team
- Advanced Training: Improve a team's efficiency
- Individual Training: Focus on personal needs



In ICE & T's virtual environment, defensive and offensive cybersecurity scenarios can be simulated.

Teamwork takes the center stage:
The trainees analyze and mitigate incidents together as a team.

How Our Trainings Work

At RI CODE, we focus on a realistic training experience that is tailored to personal needs.

- **Our trainers give** an introduction in the virtual environment and the tools used, e.g., Firewall and Open Source Security Information Management (OSSIM).
- The initial situation is presented to the trainees. Every scenario has its own story.
- Trainees investigate, analyze, and mitigate incidents or use offensive techniques to achieve the scenario's mission goals through teamwork (usually 4–6 trainees per team).
- At the end, the scenario and the team's performance is discussed and evaluated in a debriefing session.

The scenarios currently available at ICE & T are grouped into the categories Cyber Incident & Response Management (CIRM) Level 0–2, Supervisory Control and Data Acquisition (SCADA), and Penetration Testing (PT). Beyond that, the Cyber Range offers a variety of self-learning modules and more than 80 individual exercises from nine different cybersecurity domains.

Infrastructure and Setup

RI CODE's Cyber Range has two fully equipped classrooms for teams with up to six trainees.

Our trainers monitor team progress, manage scenarios and enable a unique learning experience.

Connections into the virtual environments are established via remote desktop session. In each classroom, teams have whiteboards, TV screens, and a touchboard to summarize and visualize their findings and to plan their next steps. The trainer room is equipped with three workstations: Each remote session of a trainee can be supervised via a multi-platform remote control software to analyze the teams' activities during a training.

Scenarios are played out on predefined virtualized network topologies. The modular architecture keeps the design and implementation of new scenarios from different cybersecurity domains simple. Furthermore, it enables the integration of novel network topologies, hardware components or software solutions. Consequently, ICE & T is in a permanent evolution and its features are constantly developed and extended.