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 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.

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.