ENCS

Red Blue

The ENCS Red team Blue team

Training

for Industrial Control Systems and Smart Grid Cyber Security

The ENCS Red Team – Blue Team training teaches anyone working with Industrial Control Systems (ICS) or Smart Grids the essentials of cyber security. In the first two days security specialists from ENCS give an overview of attacks and defensive measures. On the third day participants experience a cyber attack in a realistic Red Team – Blue Team exercise. The Blue Team defends the networks of its company, in particular its core of ICS and Smart Grids components, the Red Team tries to hack it. The training will give particpants:

- **Raised awareness of ICS and Smart Grid cyber security risks**
- **An overview of defensive measures**
- **Strategies to detect attacks and respond to them**

European Network for Cyber Security

Become aware of the risks of cyber-attacks and learn strategies to prevent and detect them.

Red Blue

Awareness of Risks

To secure your ICS and Smart Grid systems, you need to know how hackers work. Anyone can learn the basic methods and tools they use. In the first two days the ENCS Red Team – Blue Team training teaches the entire class:

- **The hacker mindset.** Learn what drives hackers, so that you can discourage them from targeting your organization.
- **The steps in a cyber-attack.** Learn how hackers reach critical systems, so that you see vulnerabilities you missed before.
- **The tools used by hackers.** Learn the technologies hackers use, so that you can judge how hard it is to exploit a vulnerability.

You will learn to see your systems from a new angle, and get a better idea of the risks you face.

Strategies for Defense

In the first two days the ENCS Red Team – Blue Team training teaches you a strategy for defending your systems, based on three principles:

- **Understand your network.** Learn to analyze ICS and Smart Grids for security, so that you can choose security measures that do no harm operations
- **Choose appropriate measures.** Learn how to adapt IT security measures to ICS and Smart Grid, so that you make them work.
- **Monitor your security.** Learn about intrusion detection and incident response, so that you can detect attacks that cannot be prevented.

During the exercise on the third day, you can try different defensive strategies and techniques in a scenario that not only realistically simulates the technical aspects, but also the pressure and communication problems you face during a cyber attack.

On the third day of the training all participants join in an exercise that simulates a cyber attack. Some particpants become the Red Team. They try to hack the Blue Team's ICS and IT infrastructure, and disrupt the Blue Team's production process. The rest of the particpants become the Blue Team. They try to implement the defensive strategy they learned.

The exercise scenario realistically simulates not only the technical aspects, but also the pressure and communication problems during a cyber attack. At the end of the day everyone shares the lessons learned in the exercise, and discusses how to apply these in their own organization. Participants who complete the course can also benefit by earning credits towards CISSP and CISM security certification programs.

ENCS

The European Network for Cyber Security (ENCS) is a non-profit member organization that brings together critical infrastructure stake owners and security experts to deploy secure European critical energy grids and infrastructure. Founded in 2012, ENCS has dedicated researchers and test specialists who work with members and partners on applied research, defining technical security requirements, component and end-to-end testing, as well as education & training.

Register at encs.eu/training or for more information contact training@encs.eu