

# (301) ICS Cybersecurity Lab Training

Including the Red-Blue Exercise

Imagine delving into a world where digital landscapes intertwine with intricate networks, and every click and command holds the weight of safeguarding critical infrastructure. Participants will navigate through a meticulously designed cyber terrain, encountering scenarios that mirror real-world threats and cyber-attack simulations. The immersive environments are crafted to provide a comprehensive understanding of the complexities in cybersecurity, ensuring that each challenge not only tests their current skills but also pushes them to innovate and adapt. The cyber escape rooms, themed with advanced technological aesthetics and realistic control systems, create a captivating backdrop that enhances the learning experience, making every moment in the course a thrilling exploration of the digital frontier. The final challenge will be a unique face-off - red team vs. blue team. An unscripted battle between two teams, blue team trying to maintain a fully operational company while under full cyber-assault of the red team! Unlike any tabletop or CTF that you have ever tried!

## Course Overview

This course builds on the concepts presented in the online 300 course and provides instruction, hands-on exercises, and immersive environments to facilitate understanding, protecting, and securing Industrial Control Systems (ICS) from cyber-attacks.

## Key Features

- Hands-on exercises
- Immersive environments
- Cyber escape rooms to challenge participants' problem-solving, communication, and cyber skills
- Red Team/Blue Team exercise conducted in a cyber range encompassing four actual live Control Systems

## Course Benefits

- Learn intermediate and advanced ICS cybersecurity techniques
- Improve problem-solving and communication skills
- Gain practical experience in a realistic environment

## Course Dates and Registration

For a calendar of course dates and to register, visit [<https://cisa.gov/ics-training-calendar>]