



Cybersecurity Training for Industrial Control Systems (ICS)

Cybersecurity for Industrial Control Systems

Overview: This course provides training on understanding, protecting, and securing Industrial Control Systems (ICS) from cyber-attacks. To understand how to best defend a system, trainees will learn about common vulnerabilities and the importance of understanding the environment they are tasked to protect. Learning the weaknesses of a system will enable trainees to implement the mitigation strategies and institute policies and programs that will provide the defense-in-depth needed to ensure a more secure ICS environment.

Who Should Attend: Members of the industrial control systems community associated with IT and process control network operations and security (Operations Technology, OT), operations or management of critical infrastructure (CI) assets and facilities, as well as those who provide CI components and software development.

Prerequisite: Every student attending the course must bring a laptop computer (no tablets) with wireless capability (to connect to the exercise networks) and a minimum of 8GB of RAM. A modified Kali distribution VM containing additions to support classroom exercises **will be provided** and used during the course. Each student must arrive with a VMware® software virtualization package (Workstation, Player, or Fusion) installed on their laptop. You must have administrator privileges to install the VM player.

There is no fee for attending this workshop. Attendees are responsible for their own travel, food and accommodation during the event.

I Course Description:

Monday, August 31st, 9:00 am – 4:00 pm

Introduction to Control Systems Cybersecurity (101): The purpose of this course is to introduce students to the basics of industrial control systems security. This includes a comparative analysis of IT and control system architecture, security vulnerabilities, and mitigation strategies unique to the control system domain.

Tuesday, September 1st, 8:00 am – 5:00 pm

Intermediate Cybersecurity for Industrial Control Systems, Lecture Part 1 (201): This course provides technical instruction on the protection of industrial control systems using offensive and defensive methods. Students will understand how cyber-attacks could be launched, why they work, and mitigation strategies to increase the

EVENT DETAILS

DATE: Aug 31 – Sept 3rd, 2026

TIME: 9:00/8:00 a.m. – 5:00 p.m

LOCATION:

Ben Clark Training Facility
16902 Bundy Ave,
Riverside, CA
92518

REGISTRATION:

https://ics-training.inl.gov/learn/courses/350/region-9-riverside-registration/lessons?generated_by=49388&hash=8232e107496863ecdbb3fb386e400dc9d447da12

REGISTRATION OPEN

cybersecurity posture of their control system. Demonstrations will include the use of software tools to establish a baseline of your network(s), and to monitor and analyze its traffic.

***The two courses (202 and CyberStrike) will be presented alternately on Thursday and Friday, with 50 seats available for each class, each student will get both courses.**

Wednesday, September 2nd and Thursday September 3rd 8:00 am – 5:00 pm

Intermediate Cybersecurity for Industrial Control Systems, Part 2 (202) Hands-on:

Because this course is hands-on, students will get a deeper understanding of how the various tools work. Accompanying this course is a sample process control network that demonstrates exploits used for unauthorized control of the equipment and mitigation solutions. This network is also used during the course for the many hands-on exercises that will help the students develop control systems cybersecurity skills they can apply when they return to their jobs.

Wednesday, September 2nd and Thursday September 3rd 8:00 am – 5:00 pm

CyberStrike: Hands-on workshop for defending against an OT cyberattack

[No laptop required] This course offers a hands-on, simulated demonstration of a cyberattack, drawing from elements of the 2015 and 2016 cyber incidents in Ukraine. The instruction platform challenges course participants to defend against a cyberattack on the equipment they routinely encounter within their industrial control systems.

A certificate of completion and CEUs will be offered to those who complete each session of the course.

Mon– Room A	Tues– Room A	Wed– Room A	Wed– Room B	Thur– Room A	Thur– Room B
101 – ICS Introduction	201 – Intermediate	202 – Hands on	Cyber Strike	202 – Hands on	Cyber Strike
~100 students	~100 students	~50 Students Track A <u>for ½ of students</u>	~50 Students Track B <u>for ½ of students</u>	~50 Students – Track B <u>for ½ of students</u>	50 Students – Track A <u>for ½ of students</u>
9am – 4pm	8am – 5pm	8am – 5pm	8am – 5pm	8am – 5pm	8am – 5pm

Track A and B are presented at the same time in 2 different rooms to half of the attendees so that everyone gets both courses over the course of the final 2 days.

Questions: For additional information please contact ICSTraining@inl.gov