TRAINING

Industrial Control Systems Emergency Response Team (ICS-CERT) training courses and workshops share in-depth defense strategies and up-to-date information on cyber threats and mitigations for vulnerabilities with the goal of improving cybersecurity preparedness in the control systems community. All training options are presented with no cost to the student. A certificate of completion is available after each course.

WEB BASED TRAINING

Operational Security for Control Systems (100W)—1 hour

This training will provide an overview of operational security for industrial control systems (ICSs). It will provide information on how to recognize potential weaknesses in your daily operations and suggest techniques for mitigating those weaknesses.

Cybersecurity for Industrial Control Systems (210W)—15 hours

This Course is a web based version of our 101 and 201 instructor led courses. It will introduce students to the basics of ICS security, including a comparative analysis of IT and ICS architecture, security vulnerabilities, and defensive techniques unique to the control system domain. Students will learn how cyber attacks could be launched, why they work, and mitigation strategies to increase the cybersecurity posture of their control system.

INSTRUCTOR LED TRAINING

The ICS-CERT program provides instructor-led training courses and workshops at venues associated with regional events. Refer to the ICS-CERT calendar for a schedule of these training sessions.

Introduction to Industrial Control Systems Cybersecurity (101)—8 Hours

Students learn the basics of ICS security, including information on security vulnerabilities and mitigation strategies unique to the control system domain, and a comparative analysis of IT and ICS system architecture.

The course is split into four sessions:
(1) Cybersecurity Landscape: Understanding the Risks; (2) ICS Applications; (3) Current State of Cybersecurity in Control Systems; and (4) Practical Applications of Cybersecurity.

Intermediate Cybersecurity for Industrial Control Systems (201) Lecture Only—8 Hours

This course provides intermediate-level technical instruction on the protection of control systems using both offensive and defensive methods. It helps students understand how cyber attacks are launched and why they work. The session also covers mitigation strategies that can be used to increase the cybersecurity posture of ICS.

This course is split into four sessions: (1) Current Security in ICS; (2) Strategies Used Against ICS; (3) Defending the ICS; and (4) Preparation and Further Reading for 202.

Intermediate Cybersecurity for Industrial Control Systems (202) With Lab and Exercises—8 Hours

Throughout this hands-on class, a sample ICS network is used to demonstrate various exploits that can be used to gain unauthorized control of a system. Working with the sample network during class exercises helps students understand mitigation techniques and develop ICS cybersecurity skills they can apply to their work environments.

This course is split into six sessions: (1) ICS overview; (2) Risk to ICS; (3) Exploit Demonstration; (4) Basic Control Security Considerations; (5) Network Security, Identification, and Remediation; and (6) Network: Defense, Detection, and Analysis.

ICS Advanced Cybersecurity (301)—5 Days

This course provides Intensive hands-on training in protecting and securing ICS from cyber attacks. It includes a Red Team/Blue Team exercise conducted within an actual control systems environment. The exercise presents an opportunity to network and collaborate with other colleagues involved in operating and protecting control systems networks.

Prerequisites:

Each attendee should have practical knowledge of ICS networks, software, and components; have basic coding skills; and a fairly deep understanding of IT network details, such as the difference between UDP and TCP protocols, and MAC and IP addresses.

Every student attending this course should bring a laptop computer (with a DVD drive) on which they have "administrator" privileges allowing them to configure and load software.

DAY 1—Welcome, overview of the ICS-CERT Program, a brief review of cybersecurity for Control Systems, a demonstration showing how a control system can be attacked from the internet, and hands-on training on Network Discovery techniques and practices.

DAY 2—Hands-on classroom training on Network Discovery and Metasploit; separating into Red and Blue Teams.

DAY 3—Hands-on classroom training on Network Exploitation and Network Defense techniques and practices; Red and Blue team strategy meetings.

DAY 4—An 8-hour Red Team/Blue Team exercise. The Blue Team is tasked with providing the cyber defense for a corporate environment and with maintaining operations for a batch mixing plant and an electrical distribution SCADA system. The Red Team attempts to attack the Blue Team's systems.

DAY 5—Red and Blue team discussion of lessons learned and roundtable discussion.

LEARN MORE

To learn more about these training sessions, visit:

https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

For a list of upcoming training events, visit:

https://ics-cert.us-cert.gov/Calendar

About ICS-CERT

ICS-CERT works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors.

https://ics-cert.us-cert.gov

About NCCIC

The National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

http://www.dhs.gov/national-cybersecurity-communications-integration-center