Training

Industrial Control Systems

	Training Title or Topic	Short Description	Length of Course	Sponsor	Format/ Location	More Information
1	**Web Based OT Training**	There are 13 courses covering introduction to ICS, Risk, Attack Methods, and Defense.	~ 1 hour each	CISA	Online	https://ics-training.inl.gov/learn
2	**Regional Events**	This series of courses provide technical and hands-on instruction on the protection of Industrial Control Systems using offensive and defensive methods	101: 6 hrs 201: 8 hrs 202: 8 hrs CS LO: 8 hrs	CISA	Various locations	https://inl.gov/national-security/ics-cybersecurity-training/#ics-regional
3	**300: Industrial Control Systems (ICS) Cybersecurity**	This course provides hands-on training on understanding, protecting, and securing Industrial Control Systems (ICS) from cyber-attacks. Hands-on exercises include network discovery and mapping, network defense/detection/analysis, and exploitation and attack process.	12-15 hours	CISA	Online	https://inl.gov/national-security/ics-cybersecurity-training/
4	**301: ICS Cybersecurity & Red-Blue Exercise**	This course features wireless communications, ICS architecture, network discovery and mapping, network defense, and an attacker-focused perspective. Escape rooms are used to provide critical thinking exercises on learning objectives. Finally, there is a full day red vs blue exercise, using a complex IT/OT environment.	4 days	CISA	In-person at INL campus	https://inl.gov/national-security/ics-cybersecurity-training/
5	**311 Detect the Attacker**	This scenario-driven course will elevate your threat detection expertise. Participants will master a comprehensive threat detection methodology, and enhance skills in detecting, correlating and analyzing cyberthreats within industrial environments.	4 days	CISA	In-person	https://inl.gov/national-security/ics-cybersecurity-training/

	Training Title or Topic	Short Description	Length of Course	Sponsor	Format/ Location	More Information
6	**401: ICS Cybersecurity Evaluation**	This course provides hands-on training on how to analyze, evaluate, and document the cybersecurity posture of an organization's OT environment for the purpose of identifying recommended changes.	15-20 hrs	CISA	Online	https://inl.gov/national-security/ics-cybersecurity-training/
7	**Cyberstrike**	Cyberstrike workshops are designed to enhance the ability of energy sector owners and operators to prepare for a cyber incident impacting industrial control systems. Each workshop provides hands-on exercises that emulate the topics and attacks being discussed. The various workshops include Lights Out (electric sector), Nemesis (threat brief), Shadow Valve (oil and natural gas), StormCloud (solar and wind generation) and Incident Response (technical analysis).	8 hrs each	DOE	Virtual and in-person/ location varies	https://inl.gov/national-security/cyberstrike/
8	**Accelerate**	Provides participants with a fundamental knowledge of the CCE methodology focused on securing the nation's critical infrastructure systems.	2 days	DOE	In-person at INL campus and various locations	https://inl.gov/national-security/cce
9	**ICS Fundamentals**	Provides a solid foundation of ICS basics and terminology through instruction and hands-on ICS exercises. Includes field trips showing diverse working ICS environments. (This is not an ICS Cybersecurity course)	3 days	DOE	In-person at INL campus	https://inl.gov/national-security/cce
10	**Control Laboratory**	Using a cyber-range that simulates multiple critical infrastructures, it provides an environment for government and private industry partners to experience the possible effects of kinetic cyber-physical attacks.	~ 1 week	CISA	Virtual and in-person at INL campus	https://inl.gov/national-security/ics-celr/

Sponsoring Organizations

Idaho National Laboratory