Industrial Control Systems Cyber Security Emergency Response Team (ICS-CERT)

Pre-Approved for CompTIA CEUs

You can earn 1 CEU for each hour of training. Follow these requirements to earn and receive CEUs.

All training durations less than 1 hour are not valid for CEUs.

Timing: You must complete the training course during your three-year renewal cycle, and the same course can only be submitted once.
Relevance: At least 50 percent of the training course content must relate to one or more of the exam objectives for the certification you're renewing.
Documentation: Submit the following documentation to receive CEUs for a training course:

1. Detailed description/outline of the training content
2. Completion certificate containing the following:
   - Your name
   - Name of the course
   - Name of the training provider
   - Date the course was completed
   - Number of hours

Training approved in this document is based on the exam objectives:

- A+ 220-1001 and 220-1001
- Network+ N10-007
- Security+ SY0-501
- Linux+ XK0-004
- Cloud+ CV0-002
- PenTest+ PT0-001
- CySA+ CS0-001
- CASP+ CAS-003

Note: Approved training courses in this document are subject to change without prior notification. Training submitted based on prior approval will remain valid.

CompTIA Continuing Education
PRE-APPROVED FOR CEUs

ICS-CERT

Pre-Approved for CompTIA CEUs

ICS-CERT	A+	Network+	Security+	Linux+	Cloud+	PenTest+	CySA+	CASP+
101 Introduction to Control Systems Cybersecurity (8 hrs.)	Valid	Valid	N/A	Valid	Valid	N/A	N/A	N/A
201 Intermediate Cybersecurity for Industrial Control Systems (8 hrs.)	Valid	Valid	Valid	Valid	Valid	N/A	N/A	N/A
202 Intermediate Cybersecurity for Industrial Control Systems (8 hrs.)	Valid	Valid	Valid	Valid	Valid	N/A	N/A	N/A
301 ICS Cybersecurity (5 days)	Valid	Valid	Valid	Valid	Valid	N/A	N/A	N/A
100W Operational Security (OPSEC) for Control Systems (1hr)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
210W Cyber Security Industrial Control Systems (15 hrs.)	Valid	Valid	Valid	Valid	Valid	N/A	N/A	N/A
210W-01 Differences in Deployments of ICS (1.5 hrs.)	Valid	Valid	Valid	Valid	Valid	N/A	N/A	N/A
210W-02 Influence of Common IT Components on ICS (1.5 hrs.)	Valid	Valid	Valid	Valid	Valid	N/A	N/A	N/A
210W-03 Common ICS Components (1.5 hrs.)	Valid	Valid	N/A	Valid	Valid	N/A	N/A	N/A
210W-04 Cybersecurity within IT & ICS Domains (1.5 hrs.)	Valid	Valid	N/A	Valid	Valid	N/A	N/A	N/A
210W-05 Cybersecurity Risk (1.5 hrs.)	Valid	Valid	N/A	Valid	Valid	N/A	N/A	N/A

ICS-CERT	A+	Network+	Security+	Linux+	Cloud+	PenTest+	CySA+	CASP+
210W-06 - Current Trends (Threats) (1.5 hrs.)	Valid	Valid	N/A	Valid	Valid	N/A	N/A	N/A
210W-07 Current Trends (Vulnerabilities) (1.5 hrs.)	Valid	Valid	N/A	Valid	Valid	N/A	N/A	N/A
210W-08 Determining the Impacts of a Cybersecurity Incident (1.5 hrs.)	Valid	Valid	Valid	Valid	Valid	N/A	N/A	N/A
210W-09 Attack Methodologies in IT & ICS (1.5 hrs.)	Valid	Valid	N/A	Valid	Valid	N/A	N/A	N/A
210W-10 Mapping IT Defense-In-Depth Security Solutions to ICS (1.5 hrs.)	Valid	Valid	Valid	Valid	Valid	N/A	N/A	N/A