INFOSEC Skills
LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

OT/ICS Certified Security Professional (ICSP) Boot Camp

Learn the best practices for securing Operational Technologies (OT) including Industrial Control Systems (ICS) and SCADA networks. This boot camp teaches you how to defend against both internal and external attackers to provide holistic security for critical industrial automation systems.

Course description

From the power grid to water treatment facilities, ICS and SCADA OT controls are essentials for many of today's most critical infrastructures. Infosec's OT/ICSP Boot Camp builds your security skills by teaching you how to assess, administer, and secure these critical systems while gaining hands-on experience via our applied learning ICS/SCADA Cyber Range activities.

You'll learn everything from field-based attacks to automated vulnerability assessments for OT. This boot camp also prepares you to become an OT/ICS Certified Security Professional and pass the ICSP certification exam.

Who should attend

- OT, ICS, and SCADA system operators or analysts
- Operations Technology Cybersecurity or Threat Intelligence professionals
- Control systems engineers
- Industrial Control System Engineers and consultants
- IT and security professionals with a desire to learn how to protect critical infrastructure and Operational Technologies

Boot camp at a glance

Hands-on training

- ✓ Practice your skills in the ICS/SCADA Cyber Range
- ✓ Learn OT/ICS access control, authentication and authorization
- ✓ Assess OT/ICS vulnerabilities, detect cyber-attacks and more!

Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 5-day boot camp
- ✓ 90-day extended access to all boot camp materials

The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to hundreds of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

700+ IT and security courses

Earn CPEs and build new skills with hundreds of additional training courses.

What's included

- Five days of expert, live security training for ICS, SCADA, and OT
- Exam Pass Guarantee
- Exam voucher
- Unlimited practice exam attempts
- 100% Satisfaction Guarantee
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- 90-day extended access to all boot camp video replays and materials
- Onsite proctoring of exam
- Pre-study learning path
- Hands-on cyber ranges and labs
- Knowledge Transfer Guarantee

Prerequisites

- Understanding of computer hardware and operating systems
- Basic knowledge of OT, ICS or SCADA systems

Hands-on labs

Dozens of exercises in the ICS/SCADA Cyber Range bring you up to speed with the latest threats. Take the knowledge you learn and apply it to real-world scenarios to build your ICS security skills.

What you'll learn

- OT/ICS security policy development
- OT/ICS security standards and best practices
- Access control methods and strategy
- OT/ICS protocol security issues
- strategiesfor securing field communications
- User authentication and authorization
- Detecting cyberattacks
- Vulnerability assessment

Learn from experts

We don't just have great instructors. Our instructors have years of industry experience and are recognized as experts. Over the past 15 years, we've helped tens of thousands of students get certified and advance their careers.

Industry-leading exam pass rates

Infosec's courseware materials are always up to date and synchronized with the latest exam objectives. Our industry-leading curriculum and expert instructors have led to the highest pass rates in the industry. More than 93% of Infosec students pass their certification exams on their first attempt.

Skill up and get certified, guaranteed

Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.

100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

What our students are saying

I really appreciate that our instructor was extremely knowledgeable and was able to provide the information in a way that it could be understood. He also provided valuable test-taking strategies that I know not only helped me with this exam, but will help in all exams I take in the future.

Michelle Jemmott
Pentagon

Excellent! Our instructor had a vast background and related the materials to real life. Much better than just teaching the materials to pass an exam … but he did that as well. He went out of his way in class. The extra materials really benefited us when we returned to our real jobs! Great experience!

John Peck
EPA

Very impressed with Infosec. My instructor did a great job delivering the information strategically and in a way for all to understand. I would definitely take another class/certification prep course.

Sylvia Swinson
Texeltek

The instructor was able to take material that prior to the class had made no sense, and explained it in real world scenarios that were able to be understood.

Erik Heiss
United States Air Force

The course was extremely helpful and provided exactly what we needed to know in order to successfully navigate the exam. Without this I am not confident I would have passed.

Robert Caldwell
Salient Federal Solutions

OT/ICS Security Boot Camp details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

	Day 1	Day 2	Day 3	Day 4	Day 5
Morning session	Introduction to class and ICS	ICS security governance	Pentesting ICS	ICS security controls	ICSP review
Afternoon session	ICS & SCADA overview	ICS security governance	Pentesting ICS	ICS security controls	Take the ICSP exam
Evening session	Optional group & individual study	Optional group & individual study	Optional group & individual study	Optional group & individual study	

Schedule may vary from class to class

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

During your boot camp

OT security controls

- Introduction to ICSP
- Industrial control systems (ICS)
- Types of ICS
- OT and ICS components
- BPCS & SIS
- Control system strengths and weaknesses
- ICS PCN & protocols
- PCN evolution
- Modbus / DNP3 / HART
- Lab: Modbus PLC
- IT vs. ICS
- RS-232 and RS-485
- TASE 2.0 / ICCP
- CIP
- PROFIBUS / PROFINET
- FOUNDATION fieldbus
- Open vs. proprietary protocols
- HMI applications
- HMI/OIT implementations
- OPC and OPC UA
- Data historians
- Integration software (ERP/MES)

OT security governance

- Threat to OT, ISC, & SCADA
- OT attacks and threats case studies
- Lab: Attacking the infrastructure
- ICS security challenges
- Security frameworks, strategy, policies
- Standards, procedures and guidelines
- OT & SCADA security standards bodies (NIST / ISA / CFATS / NERC CIP)
- Risk management process
- Lab: "Theoretical" assessment with CSET
- ICS security assessment methodology
- NESCOR guide to vulnerability assessment

Pentesting OT systems

- Security assessment strategy
- Pentesting steps
- Safety and security considerations
- Information gathering
- Architecture analysis
- Host, application and platform fingerprinting
- DNS and SNMP recon
- Lab: SNMP recon
- Host and port scanning
- Security considerations
- Scanning tools and techniques
- Lab: Scanning ICS/SCADA networks
- Network communications capture and analysis
- RF signal capture
- Sniffing network traffic
- Device functionality analysis
- Lab: Datasheet analysis
- Vulnerability identification
- Common OT vulnerabilities
- Finding vulnerabilities
- Physical access
- Vulnerability scanning
- Server OS testing
- Patch levels
- Default and insecure configurations
- Authentication and remote access
- Firmware analysis
- Attacking ICS
- Attacking standard services (HTTP, FTP)
- Attacking server OS
- Lab: Exploiting OS-level vulnerabilities (Shellshock exploit)
- Attacking ISC protocols
- Lab: Capturing and manipulating protocol data
- Attacking wireless communications
- Lab: Recovering ZigBee network keys
- Lab: WEP/WPA2 password cracking

Crucial security controls

- Categorization of system controls
- Physical security & safety
- Identification, authentication & authorization (IA&A)
- IA&A and access control
- Remote access security
- Encryption
- Logical security
- Lab: Firewall rule design
- Monitoring, detection and protection
- Secure OT architecture
- Lab: Security architecture (group discussion)
- IDS/IPS (Introduction to Snort)
- Log monitoring and management
- Lab: SCADA honeypot (Conpot)
- Lab: Snort SCADA rules (Quickdraw)
- Incident response
- Anti-malware
- Application whitelisting
- Patch management
- Active Directory & group policy
- Summary of good security practices

ICSP exam

- ICSP review
- Take the ICSP exam

After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.

INFOSEC