CYBER RANGES

OT WORLDS

OT / ICS Cybersecurity

Hands-on scenarios

- 8 Scenarios
- Self-Paced
- Online
- 3-month access
- On-demand



Build practical skills to analyze, defend, and hunt for threats across industrial control environments.

Explore OT attack vectors and defense strategies through expert-curated, self-paced, online scenarios.

BUILD PRACTICAL CAPABILITIES FOR CONNECTED OT ENVIRONMENTS

As Operational Technology (OT) and IT converge, securing industrial systems, PLCs and hybrid networks becomes more complex. Cybersecurity training focused on IT often provides limited exposure to the industrial technologies and protocols that underpin critical infrastructure.

This CYBER RANGES OT / ICS Cybersecurity Labs Playlist helps professionals develop practical skills through self-paced, hands-on scenarios. Participants explore vulnerabilities, examine how attacks affect physical operations, and practice analyzing and detecting threats across OT environments.

FOR PROFESSIONALS SECURING OT SYSTEMS AND INFRASTRUCTURE

For cybersecurity professionals, OT engineers and technical teams seeking to develop the practical competencies needed to secure OT systems and infrastructure. The Playlist supports skills development across industrial communications, PLCs, SCADA and threat detection.

> The foundation of Cyber-Physical Systems security is the workforce that understands the risks and knows how to respond when something goes wrong.
>
> – Gartner
>
> Implement Secure Behavior Management to Secure Your Cyber-Physical Systems (July 2026)

PRACTICAL SKILLS FOR OT CYBER DEFENSE

- Analyze MODBUS communications and identify OT device misconfigurations.
- Investigate network traffic and detect malicious activity using Wireshark and Suricata.
- Explore PLC fundamentals, Phoenix Contact PCWorx and PLC firmware analysis.
- Create Visu+ projects and work with SCADA operations and alarms.
- Explore attacks against OT systems and their impact on physical processes.



CYBER SPACE, ENGAGED.

CYBER RANGES

EXPLORE THE SCENARIOS



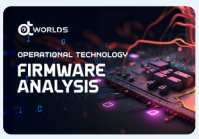
ANALYZING MODBUS
Monitor and analyze MODBUS traffic; identify common OT device misconfigurations.
45 MINUTES



DETECTING ATTACKS
Investigate network packets and MODBUS communications using Wireshark and Suricata.
1 HOUR



ATTACKING OT SYSTEMS
Explore a water-treatment control compromise and its effect on physical operations.
45 MINUTES



FIRMWARE ANALYSIS
Explore PLC firmware reverse engineering.
1 HOUR



PHOENIX CONTACT PCWORX
Build PLC fundamentals, including ladder logic, inputs and outputs, timers and counters.
2 HOURS



SCADA FUNDAMENTALS WITH VISU+ PART 1
Create and structure projects; configure tags, drivers and graphic elements.
2 HOURS



SCADA FUNDAMENTALS WITH VISU+ PART 2
Work with dynamic animations, basic SCADA operations and alarm management.
2 HOURS



OT POWER PLANT ATTACK
Detect and respond to unauthorized ICS manipulation in an OT power plant environment.
2 HOURS

DEVELOPED WITH OT / ICS SECURITY EXPERTS

Developed in collaboration with experts from ICS Village. ICS Village is a non-profit that equips industry experts and policy-makers with the tools to better defend our Nation's critical infrastructure.

> Security teams need to understand how vulnerabilities and weaknesses could be used, which exposed paths an attacker could follow, and whether the result would be a minor security issue or a serious operational disruption. This is where simulation becomes critical. Organizations can safely examine how risks may play out across assets, protocols, remote access routes, vendor connections, and control-system dependencies — without touching live operations.
>
> – Gartner
> Coolest Vendor Innovations in Cyber-Physical Systems Security (Sept. 2026)

Access this CYBER RANGES OT / ICS Cybersecurity Playlist at **app.cyberranges.com**

DEVELOP YOUR ORGANIZATION'S OT/ICS CYBERSECURITY CAPABILITIES

OT WORLDS

OT Worlds by CYBER RANGES offers a broad portfolio of exercises, training programs and physical and virtual environments to help organizations develop and test OT security capabilities, with a focus on resilience and recovery.

Explore instructor-led training and bespoke exercises, including in-person options at the Quantico Cyber Range IT / OT Battle Lab in Stafford, Virginia, USA.



Quantico Cyber Hub
Suite 305, 1010 Corporate Drive
Stafford, VA 22554
1-800-959-0163 (toll-free)
contact@cyberranges.com
www.cyberranges.com

QCR QUANTICO CYBER RANGE