2017 ISA Water/Wastewater and Automatic Controls Symposium

August 8 to 10, 2017 • Wyndham Lake Buena Vista Resort • Orlando, Florida, USA
Presented by the ISA Water/Wastewater Industries Division – ***www.isawwsymposium.com***
Technical co-sponsors: Florida AWWA Section, the WEF Automation and Info Tech Committee , Florida Water Environment Association, Instrumentation Testing Association, and ISA Tampa Bay Section

August 7-8, 2017 – Optional Short Course

IACS Cybersecurity Operations and Maintenance

ISA Course IC37. Version 1.7

Course Description

Length: 2 days
Date: Mon-Tue, August 7-8, 2017
CEU Credits: 1.4
Course Hours: 8:00 a.m. – 4:00 p.m., includes lunch both days
Price: $2,000 for ISA Members, $2,500 List

Description:

The third phase in the IACS Cybersecurity Lifecycle (defined in ISA 62443-1-1) focuses on the activities associated with the ongoing operations and maintenance of IACS cybersecurity. This involves network diagnostics and troubleshooting, security monitoring and incident response, and maintenance of cybersecurity countermeasures implemented in the Design & Implementation phase. This phase also includes security management of change, backup, and recovery procedures and periodic cybersecurity audits.

This course will provide students with the information and skills to detect and troubleshoot potential cybersecurity events as well as the skills to maintain the security level of an operating system throughout its lifecycle despite the challenges of an ever-changing threat environment.

You will be able to:

- Perform basic network diagnostics and troubleshooting
- Interpret the results of IACS device diagnostic alarms and event logs
- Develop and follow IACS backup and restoration procedures
- Understand the IACS patch management lifecycle
- Develop and follow an IACS patch management procedure
- Develop and follow an antivirus management procedure
- Define the basics of application control and whitelisting tools
- Define the basics of network and host intrusion detection
- Define the basics of security incident and event monitoring tools
- Develop and follow an incident response plan
- Develop and follow an IACS management of change procedure
- Conduct a basic IACS cybersecurity audit

You will cover:

- Introduction to the IACS Cybersecurity Lifecycle
  - Identification & Assessment phase
  - Design & Implementation phase
  - Operations & Maintenance phase
- Network Diagnostics and Troubleshooting
  - Interpreting device alarms and event logs
  - Early indicators
  - Network intrusion detection systems
  - Network management tools
- Application Diagnostics and Troubleshooting
  - Interpreting OS and application alarms and event logs
  - Early indicators
  - Application management and whitelisting tools
  - Antivirus and endpoint protection tools
  - Security Incident and Event Monitoring (SIEM) tools
- IACS Cybersecurity Operating Procedures & Tools
  - Developing and following an IACS management of change procedure
  - Developing and following an IACS backup procedure
  - IACS configuration management tools
  - Developing and following an IACS patch management procedure
  - Patch management tools
  - Developing and following an IACS antivirus management procedure
  - Antivirus and whitelisting tools
  - Developing and following an IACS cybersecurity audit procedure
  - Auditing tools
- IACS incident response
  - Developing and following and IACS incident response plan
  - Incident investigation
  - System recovery

Classroom/Laboratory Exercises:

- Network diagnostics and troubleshooting
- Intrusion detection alarm
- Event monitoring
- Configuration management
- Patch management
- Antivirus management
- Whitelisting
- Vulnerability scanning tools
- Incident response
- Backup and recovery

Who Should Attend?:

- Operations and maintenance personnel
- Control systems engineers and managers
- System integrators
- IT engineers and managers of industrial facilities
- Plant Safety and Risk Management

Recommended Prerequisites:

- ISA Courses TS06, TS12, TS20, IC32, IC33, and IC34 or equivalent knowledge/experience

About the Instructor

Bryan Singer is a Director of Industrial Cybersecurity Services and Sales for IOActive, overseeing service engagements and staff. Bryan has over twenty years of experience in security research and consulting across a variety of enterprises including industrial automation, critical infrastructure, manufacturing, US Department of Defense, healthcare, telecommunications, and others.

His proven professional skills include system architecture and design, software project management, application development, system administration, with extensive recent experience in cyber vulnerability assessments and penetration testing. His professional industrial cybersecurity experience spans over 4,000 plants globally and nearly every process type including oil and gas, power generation, transmission/distribution, nuclear, food and beverage, water, pharmaceutical, automotive, and others.

Course Schedule

DAY	Topics, Exercises, Etc.	Time
Day 1	Welcome and Pre-Instructional Survey	0.50 hour
A.M.	Introduction to the ICS Cybersecurity Lifecycle	0.25 hour
	Section 1: Review of the Assess Phase	0.25 hour
	Section 2: Review of the Design Phase	0.25 hour
	Section 3: IACS Asset Management	0.25 hour
	Exercise #1: Asset Inventory	0.25 hour
	Section 3: System Hardening	0.50 hour
	Exercise #2: ICS Device Hardening	0.50 hour
	Exercise #3: Disabling USB Storage Devices	0.50 hour
Day 1	Exercise #4: Whitelisting	0.50 hour
P.M.	Section 3: Access Control & Remote Access	0.25 hour
	Section 3: Patch Management	0.25 hour
	Exercise #5: WSUS demo	0.25 hour
	Section 3: Malware Management	0.50 hour
	Exercise #6: PLC backup and configuration management	0.50 hour
	Exercise #7: Complete a MOC form	0.50 hour
	Section 3: Information & Documentation Management	0.25 hour

Day 2 A.M.	Daily Progress Reviews & Overview of Day 2 Objectives Section 3: Change Management Section 3: Physical Security Exercise #8: What's wrong with this picture Section 4: Detecting Abnormal Activity Section 4: Network and Host Intrusion Detection Section 4: Monitoring Logs Exercise #9: Event Detection, Tracking, and Log Monitoring Section 4: Periodic testing / auditing Exercise #10: Vulnerability scanning	0.25 hour 0.50 hour 0.25 hour 0.25 hour 0.25 hour 0.25 hour 0.50 hour 0.25 hour 0.25 hour 0.25 hour
Day 2 P.M.	Daily Progress Reviews & Overview of Day 3 Objectives Section 5: Incident Response Lifecycle Section 5: Incident Response Planning Section 5: Incident Management Section 5: Post Incident Analysis & Forensics Exercise #11: Network packet capture analysis Exercise #12: Troubleshooting and Forensics Review of Overall Course Objectives Post-Instructional Survey Final Course Evaluation	0.25 hour 0.25 hour 0.25 hour 0.25 hour 0.25 hour 0.50 hour 0.50 hour 0.25 hour 0.50 hour
		14 hours = 1.4 CEUs