



# Las Vegas 2016

Las Vegas, NV | Sat, Jan 9 - Thu, Jan 14, 2016



## ICS410: ICS/SCADA Security Essentials

- ▶ [Contents](#) | [Schedule](#) | [Additional Info](#)
- ▶ Instructor: [Paul A. Henry](#)
- ▶ 5,185 USD

- ▶ [GICSP Certification](#)
- ▶ [Affiliate Pricing](#)
- ▶ 30 CPEs
- ▶ [Laptop Required](#)

*This is a great course that distinguishes the challenges and integration points for ICS and Traditional IT security posture. The instructors provide in-depth real world knowledge and experience to the material to make it actionable within the attendee's corporate environment.*  
Rob Oates, GDIT

*Good comprehensive content with dynamic instructor really made this course good. This is the best training course I've taken in 25+ years.*  
Curt Imanse, Accenture

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. ICS410: ICS/SCADA Security Essentials provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.



[More](#) ▼



**Course Content Overlap Notice:** Please note that some course material for SEC401 may overlap with ICS410. We recommend ICS410 for those interested in security for an ICS/SCADA environment as it is approached from this viewpoint, and SEC401 for those primarily interested in a general information security course.

### Course Syllabus

+ Expand All

Course Contents	Instructors	Schedule
+ <a href="#">ICS410.1: ICS Overview</a>	<a href="#">Paul A. Henry</a>	Sat Jan 9th, 2016 9:00 AM - 5:00 PM
- <a href="#">ICS410.2: ICS Attack Surface</a>	<a href="#">Paul A.</a>	Sun Jan 10th, 2016

Event starts  
in 25 Days

[Register Now](#)



[Free Excerpt](#)

[Event Home](#)

[Location](#)

[Courses / Prices](#)

[Schedule](#)

[Instructors](#)

[Bonus Sessions](#)

[Exhibitors](#)

[Attendee Info](#)

[Downloads](#)



- [Event Brochure](#)
- [Winter Training 2016](#)

[Share](#)



[g+](#) [Tweet](#) [Like](#)  
[in](#) [Share](#)

*SANS training is like a catalyst. It not only boosts your knowledge but also*

[Henry](#)

9:00 AM - 5:00 PM

*inspires you to learn  
more.  
Tan Koon Yaw*

## Overview

**Takeaway:** If you know the adversary's approaches to attacking an ICS environment, you will be better prepared to defend that environment. Numerous attack vectors exist within an ICS environment. Some are similar to traditional IT systems, while others are more specific to ICS. During Day 2 defenders will develop a better understanding of where these specific attack vectors exist, as well as the tools to use to discover vulnerabilities and exploit them. Each student will use a vulnerable target virtual machine to further understand attacks targeting the types of web servers used on many ICS devices for management purposes. Simulators will be configured to allow students to conduct attacks against unauthenticated ICS protocols. A variety of data samples are used to examine additional attack vectors on remote devices.

CPE/CMU Credits: 6

## Topics

### Day 2: ICS Attack Surface

- ICS Attack Surface
  - *Exercise: Information Leakage*
- Attacks on HMI and UIs
  - Intro to SamuraiSTFU
  - *Exercise: Password Fuzzing*
  - Web Attacks
  - *Exercise: Authentication Bypass with SQL Injection*
- Attacks on Control Servers
- Attacks on Network Communications
  - *Exercise: Spoofing Modbus*
- Attacks on Remote Devices
  - *Exercise: Analyzing Firmware*
  - Firmware Attacks

+ [ICS410.3: Defending ICS Servers and Workstations](#)

[Paul A.  
Henry](#)

Mon Jan 11th, 2016  
9:00 AM - 5:00 PM

+ [ICS410.4: Defending ICS Networks and Devices](#)

[Paul A.  
Henry](#)

Tue Jan 12th, 2016  
9:00 AM - 5:00 PM

+ [ICS410.5: ICS Security Governance](#)

[Paul A.  
Henry](#)

Wed Jan 13th, 2016  
9:00 AM - 5:00 PM

## Additional Information

! [Laptop Required](#)

+ [Who Should Attend](#)

+ [Prerequisites](#)

+ [What You Will Receive](#)

+ [You Will Be Able To](#)

+ [Hands-on Training](#)

+ [What To Take Next?](#)

# Author Statement

Eric Cole, Eric Cornelius, and Justin Searle

This course provides students with the essentials for conducting cybersecurity work in industrial control system environments. After spending years working with industry, we believe there is a gap in the skill sets of industrial control system personnel, whether it be cybersecurity skills for engineers or engineering principles for cybersecurity experts. In addition, both information technology and operational technology roles have converged in today's industrial control system environments, so there is a greater need than ever for a common understanding between the various groups who support or rely on these systems. Students in ICS410 will learn the language, the underlying theory, and the basic tools for industrial control system security in settings across a wide range of industry sectors and applications.

## Latest Whitepapers

[Cleaning Up After a Breach Post-Breach Impact: A Cost Compendium](#)

By Barbara Filkins

[Infrastructure Security Architecture for Effective Security Monitoring](#)

By Luciana Obregon

[Advancing Endpoint Protection and Compliance with Promisec Endpoint Manager](#)

By Jake Williams

[Last 25 Papers »](#)

## Latest Tweets @SANSInstitute

[Threat Hunters: how long does it take you to proactively unc \[...\]](#)

December 15, 2015 - 12:20 AM

[In your org, what types of systems are considered endpoints? \[...\]](#)

December 14, 2015 - 8:30 PM

[Tip of the Day #SANS Tip: Leaving your seat? Ctrl--Alt--Delet \[...\]](#)

December 14, 2015 - 3:02 PM

## Contact Us

Tel +65 69 339 540

[asiapacific@sans.org](mailto:asiapacific@sans.org)

"As a security professional, this info is foundational to do a competent job, let alone be successful."  
- Michael Foster, Providence Health and Security

"The perfect balance of theory and hands-on experience."  
- James D. Perry II, University of Tennessee

"SANS is a great place to enhance your technical and hands-on skills and tools. I thoroughly recommend it."  
- Aaron Waugh, Datacom NZ Ltd



[Find Training](#) | [Live Training](#) | [Online Training](#) | [Programs](#) | [Resources](#) | [Vendor](#) | [About](#)  
[Privacy Policy](#) | [Trademark Usage Policy](#) | [Credits](#) | © 2000-2015 SANS™ Institute