SANS

Industrial Control Systems

November 18, 2015

ABOUT SANS - TRAINING

- SANS provides intensive, hands-on, immersion training
- Highest quality
  - 70+ courses covering basic security skills to cutting edge topics
  - Courses updated 4 times per year to keep current
  - Course material includes very thorough back-up material to provide post training value
- The best practitioner-instructors
- Practical steps for defending systems and applications

The SANS Promise:

"You will be able to apply our information security training the day you get back to the office."

WE'VE BEEN DOING ICS FOR 11 YEARS

This is not your
"another day in the data center"
for IT professionals

This is <u>Industrial</u> Cyber Security:

- ✓ Engineers
- ✓ ICS Security Specialists
- ✓ OT Support Specialists

SANS Industrial Control Systems

CURRICULUM

COMING SOON:

Hosted: Embedded Security

Building Control System Security

CIP Security

ICS Security for Managers

ICS515

Active Defense & Incident Response

- Modifying defense systems
- Intrusion response
- Intrusion prevention

ICS410

Security Essentials

- IT (OT support)
- IT Security
- Engineering
- Corporate, industry & professional

GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL GICSP

ICS410 ICS/SCADA SECURITY ESSENTIALS

Provides an introductory 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.

Who Should Attend

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

Five-day course with hands-on Labs

Day 1 - ICS Overview
Day 2 - ICS Attack Surface
Day 3 – Defending ICS Servers & Workstations
Day 4 – Defending ICS Networks & Devices
Day 5 – ICS Governance & Resources

sans.org/ics410

WHAT STUDENTS ARE SAYING ABOUT ICS410?

- "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 attendees corporate environment." Rob Oates – GDIT

- "Provides good baseline info for both IT and OT SME's." Daryl Haegley – DOD

- "This is a great intro course for anyone taking security seriously in an ICS environment." Shaun Curry – SMSD

GLOBAL INDUSTRIAL CYBERSECURITY PROFESSIONAL (GICSP)

Industries that are helping to develop and shape this certification include:

- **Oil and Gas**
- **Utilities (Power, Water and related)**
- **Manufacturing**
- **OEM**
- **Information Technology**

giac.org/gicsp

NEW! ICS515 ICS ACTIVE DEFENSE AND INCIDENT RESPONSE

ICS Active Defense and Incident Response will empower students to understand their networked industrial control system (ICS) environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security.

Participants will gain hands-on experience with the following tools:

- CYBATIWorks Kit and Virtual Machine with PeakHMI
- Snort and Bro for tailoring and tuning Intrusion Detection System rules
- Wireshark and TCPDump for network traffic capturing and packet analysis
- FTK Imager and MD5Deep for forensic data acquisition and Validation
- OpenIOC and YARA for developing Indicators of Compromise
- Xplico and NetworkMiner for network flow and data analysis

Who should attend:

- Information Technology and Operation Technology (IT and OT) Cybersecurity Personnel
- IT and OT Support Personnel
- ICS Incident Responders
- ICS Engineers
- Security Operations Center Personnel

Five-day course with hands-on Labs

Day 1 –Threat Intelligence
Day 2 – Asset Identification and Network Security Monitoring
Day 3 – Incident Response
Day 4 – Threat and Environment Manipulation
Day 5 – Active Defense and Incident Response Challenge

sans.org/ics515

BETA! ICS456: ESSENTIALS FOR NERC CRITICAL INFRASTRUCTURE PROTECTION

The NERC CIP Essentials 5-day course empowers students with knowledge of the "What" and the "How" of the Version 5 standards. The course addresses the role of FERC, NERC and the Regional Entities, provides multiple approaches for identifying and categorizing BES Cyber Systems and helps asset owners determine the requirements applicable specific implementations. Additionally, the course covers implementation strategies for the Version 5 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance.

Who should attend:

- Individuals with CIP responsibilities in the following areas:
  - IT and OT (ICS) cybersecurity
  - Field support personnel
  - Security operations
  - Incident response
  - Compliance staff
  - Team leaders
  - Governance
  - Vendors / Integrators
  - Auditors

The course will provide students with:

- NERC CIP V 5 Toolkit
- MS Windows VM for hands on components of course
- Variety of tools utilized in labs
- Sample data and numerous scenario worksheets to work together as a class

ICS TRAINING OPPORTUNITIES

Community SANS

Denver, CO| Dec 7-11, 2015

- ICS515 Active Defense and Incident Response

Cyber Defense Initiative 2015

Washington, DC| Dec 12-19, 2015

- ICS410: ICS/SCADA Security Essentials
- ICS515 Active Defense and Incident Response

Las Vegas 2016

Las Vegas, NV | Jan 9-14, 2016

- ICS410: ICS/SCADA Security Essentials

Security East 2016

New Orleans, LA | Jan 25-30, 2016

- ICS515 Active Defense and Incident Response

Security East 2016

Atlanta, GA| Feb 1-5, 2016

- ICS515 Active Defense and Incident Response

https://ics.sans.org/training/courses

ICS SECURITY SUMMIT - ORLANDO, FL

Summit: Feb. 22-23, 2016
Courses: Feb. 16-21, 2016

Training - 9 training classes to choose from.

Certification - Global Industrial Cyber Security Professional (GICSP) certification

Summit - Educational session tracks presented by the best minds in the field of SCADA security.

Networking - Opportunities to make connections in the industry with the most innovative minds in the industry.

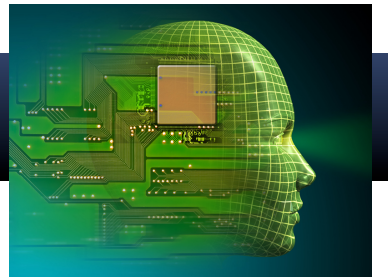
Special Events!! – KIPS Simulation, WOPR, ICS Challenge, ICS Wall

sans.org/event/42402

SANS CIP TRAINING

The SANS Cybersecurity Solution for NERC CIP is a computer-based CIP training program tailored specifically to help electric system asset owners and operators meet their training responsibilities for NERC Reliability Standards CIP-004-5.1 R2 (CIP v5). Our training is designed to meet the needs of the electric industry and the people with responsibility for CIP compliance such as the CIP Senior Manager, system operators, directors of CIP compliance and VPs of operations.

- 12 computer-based modules addressing the 49 topic areas identified in the NERC CIP training requirements plus an additional module covering CIP-014.
- Combine the SANS Securing The Human End User Awareness program, your organization will have the tools needed to address all of CIP-004 R1, CIP-004 R2, and CIP-003 R2.1.



ICS ENGINEER FOCUSED AWARENESS

SANS ENGINEER

SECURING THE HUMAN

Introduction to ICS

- **ICS Overview** – provides a brief history of ICS, regulation, and the need for ICS-focused security behavior training.
- **ICS Drivers & Constraints** – provides detail on the cybersecurity principle drivers and constraints that impact how a control system needs to be engineered, managed, supported and interfaced with.

ICS Attacks Overview

- **Overview of ICS Attacks** – provides an overview of ICS Threat Actors and examples of ICS-based attacks and trends.
- **ICS Attack Surfaces** – provides detail on specific attack approaches that target various layers of the ICS system.
- **Attack Scenario** – this is a detailed walk through of a cyber-attack against an example organization, from the unique perspective of the attacker's actions.

ICS Defense

- **ICS Server Security** – provides concepts specific to defending ICS environments at the server layer.
- **ICS Network Security** – provides concepts specific to defending ICS environments at the network layer.

ICS Governance & Policy

- **ICS System Maintenance** – provides details on ICS system maintenance tasks such as patching, backups, change management, monitoring, and logging.
- **ICS Information Assurance** – details on ICS-focused information assurance program concepts of risk management, account management, data classification, and defense in depth.
- **ICS Incident Handling** – covers important ICS incident-response topics for all individuals who interact with ICS environments.

ICS LIBRARY

Brochures

- ICS Security Training
- Deutsche ICS

Analyst Surveys

- 2015: State of Security in Control Systems
- 2014: ICS Security
- 2013: SCADA Process Control Security

Posters

- 2015: Sliding Scale of Cyber Security
- 2014: Securing an Automated Word
- 2013: Control Systems Are A Target

Whitepapers

- ICS Cyber Kill Chain
- Sliding Scale of Cyber Security
- The Perfect ICS Storm

https://ics.sans.org/ics-library

STAY CONNECTED

https://twitter.com/SANSICS

https://www.linkedin.com/company/sans-ics

https://ics.sans.org/blog

QUESTIONS?

John Pescatore

- jpescatore@sans.org

Brian Correia

- bcorreia@sans.org