SANS EMEA

Hands On | Five Days | Laptop Required | 30 CPEs

ICS 410

ICS/SCADA SECURITY ESSENTIALS

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 standardised 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.

#SANSDubai

Take ICS410 at SANS Dubai 2016

Dubai 9 - 14 Jan, 2016
Register online at **www.sans.org/event/dubai-2016**

Ben Kaintoch, ICS Director, SANS Institute. UK +44 779 118 8469 , UAE +971 564 878 027
Ned Baltagi, Director Middle East, SANS Institute. UAE +971 55 336 1943

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

Hands-on training

- Introduction to Samurai STFU
- Architect a secure DCS
- Information Leakage
- Password Fuzzing
- Bypassing Authentication with SQLi
- Spoofing Modbus-TCP control signals
- Finding Passwords in EEPROM dumps
- Host Based Firewalls
- Linux Hardening
- ICS Network Capture Analysis
- Network Capture Forensics
- Attack Tree Analysis
- Incident response exercise

You will receive

- Software tools
- Virtual Machine environments will be utilized throughout the labs
- MP3 audio files of the complete course lecture

For more information see our course catalogue or visit **www.sans.org/emea**

WORLD-CLASS INFORMATION SECURITY TRAINING

Course Syllabus

410.1 ICS Overview

Students will develop and reinforce a common language and understanding of Industrial Control System (ICS) cybersecurity as well as the important considerations that come with cyber-to-physical operations within these environments.

Topics: Global Industrial Cybersecurity Professional (GICSP) Overview, Overview of ICS, Field Components, Programming Controllers, Types of ICS Systems, IT & ICS Differences, Physical Security, ICS Network Architecture

410.2 ICS Attack Surface

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.

Topics: ICS Attack Surface, Attacks on HMIs and UIs, Attacks on Control Servers, Attacks on Network Communications, Attacks on Remote Devices

410.3 Defending ICS Servers and Workstations

Students will learn essential ICS-related server and workstation operating system capabilities, implementation approaches, and system management practices. Students will receive and work with both Windows- and Linux-based virtual machines in order to understand how to monitor and harden these hosts from attack.

Topics: Windows in ICS, Linux/Unix in ICS, Updates and Patching, Processes and Services, Configuration Hardening, Endpoint Defences, Automation and Auditing, Log Management, Databases and Historians

410.4 Defending ICS Networks and Devices

With an understanding of the ICS environment, the attack vectors that exist, and the defender-specific capabilities available on servers, workstations, and applications, students will now learn network-specific defence approaches.

Topics: Network Fundamentals, Ethernet, TCP/IP Protocol Suite, ICS Protocols over TCP/IP, Enforcement Zone Devices, Honeypots, Wireless in Control Systems, Field and Plant Floor Equipment, Cryptography Fundamentals

410.5 ICS Security Governance

Students will learn about the various models, methodologies, and industry-specific regulations that are used to govern what must be done to protect critical ICS systems. Key business processes that consider risk assessments, disaster recovery, business impact analysis, and contingency planning will be examined from the perspective of ICS environments.

Topics: Information Assurance Foundations, Security Policies, Contingency and Continuity Planning, Risk Assessment and Auditing, Password Management, Incident Handling, Resources

#SANSDubai

Take ICS410 at SANS Dubai 2016

Dubai 9 - 14 Jan, 2016
Register online at:
www.sans.org/event/dubai-2016

Ben Kaintoch
ICS Director, SANS Institute.
UK +44 779 118 8469
UAE +971 564 878 027

Ned Baltagi,
Director Middle East,
SANS Institute.
UAE +971 55 336 1943

You will be able to

- Run Windows command line tools to analyse the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, ect) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems
- Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Work with network infrastructure design (network architecture concepts, including topology, protocols, and components)
- Better understand the systems' security lifecycle
- Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)
- Use your skills in computer network defence (detecting host and network-based intrusions via intrusion detection technologies)
- Implement incident response and handling methodologies

SANS EMEA

www.sans.org/emea

Email: emea@sans.org • **Tel:** +44 20 3384 3470
Address: SANS EMEA,
PO Box 124, Swansea, SA3 9BB, UK