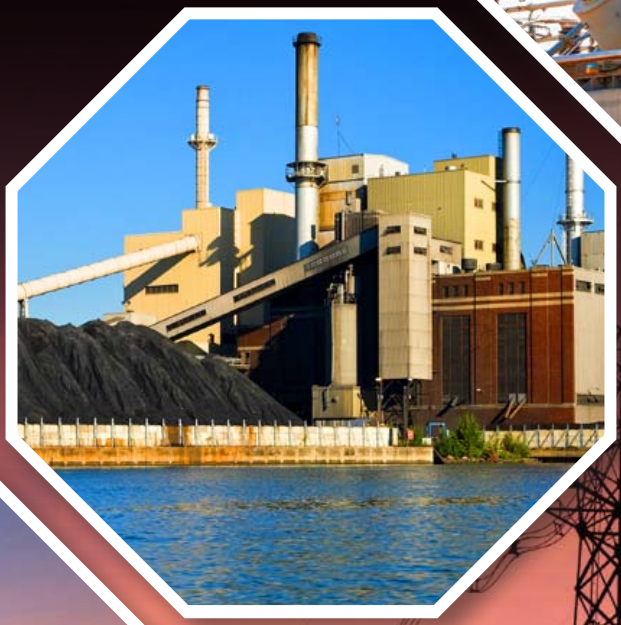
ICS for Electric Utilities



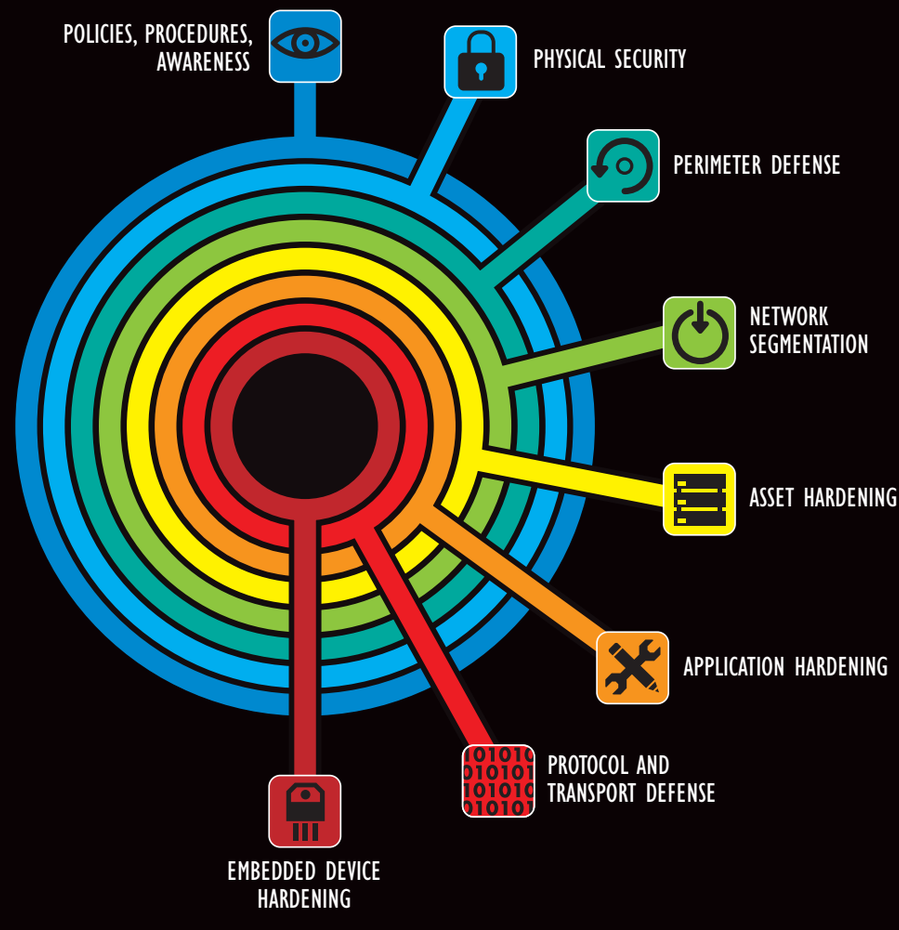
SANS ICS Industrial Control Systems

www.sans.org/ics

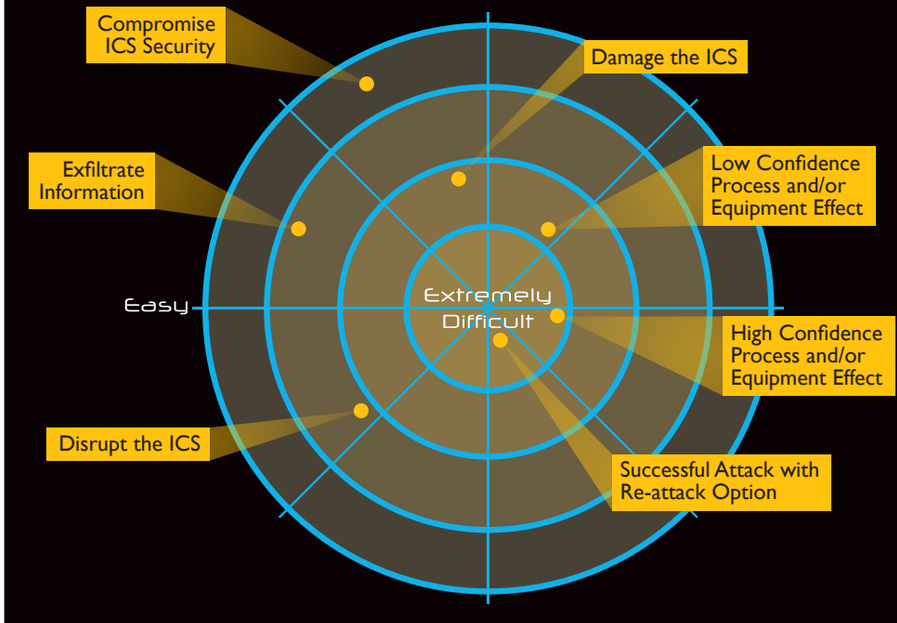
Why ICS?

SANS has joined forces with industry leaders and experts to strengthen the cybersecurity of Industrial Control Systems (ICS). This initiative equips security professionals and control system engineers with the security awareness, work-specific knowledge, and hands-on technical skills they need to secure automation and control system technology. The SANS team provides ICS-focused curricula and certifications, as well as community resources such as promotional materials, white papers, and security practice application guidance.

Layers of ICS Defense In Depth



ICS Attack Difficulty



Why Is the ICS Initiative Important?

- Tremendous gains are being achieved in industrial applications by sharing and analyzing data, but we need professionals who can address the security challenges.
- Preparation is critical because targeted ICS attacks are emerging with increasing frequency and damaging systems.
- Control systems are widely deployed and need your attention – there is no such thing as a system that is too small.
- Up-to-date ICS knowledge and security skills help keep our critical systems safe.
- Effective security requires the integration of cybersecurity professional, ICS support staff, and engineers through shared learning and a common vocabulary.

www.sans.org/ics

CIP V5 Cybersecurity Training

SANS CIP V5 Program (STH.CIPv5) is a cybersecurity training program tailored specifically to help electric system asset owners and operators meet their training responsibilities for ensuring the security of the cyber systems critical to the opearation of the Bulk Electric System. It specifically addresses the requirements part of the NERC Reliability Standards CIP-004-5.1 R2.

The CIP V5 program consists of 12 computer-based modules addressing the 49 topic areas identified in the NERC CIP V5 training requirements plus an additional module covering CIP-014-1. By combining with the SANS Securing The Human End User Awareness program, your organization will have the tools needed to address all of CIP-004-5.1 R1, CIP-004-5.1 R2, and CIP-003-5 R2.1.

The CIP V5 training can be customized by adding direct links to your organization's security policies following each module. Every module also includes a five-question online quiz to verify the student's comprehension of the CBT video content.

Keeping training content updated and relevant is critical to the success of any security awareness program. STH.CIPv5 addresses this by updating the training content as needed and delivers these updates free of charge to all CBT license holders.

The training was developed by SANS team members working with an Advisory Board consisting of fifteen CIP practitioners from electric utilities, Independent System Operators and a former NERC auditor. The Advisory Board participated throughout the development process beginning with defining what the training should include, and provided feedback on module scripts, video imagery, and end-of-module quiz questions. The result is a training program that is consistent, technically accurate, highly engaging, and backed by the SANS reputation for quality.

Training can be hosted on the SANS Virtual Learning Environment (VLE) or your SCORM-compliant LMS and is U.S. Federal 508/ADA compliant.

Optional purchase: Each of the R1 security awareness video modules also has an associated newsletter, poster, and screen saver to help reinforce the CBT training. The support materials package is customized with your organization's name, logo, and security team contact information. It is delivered in electronic format ready for printing or other distribution channels.

If your organization is interested in reviewing this training program, please visit us at www.securingthehuman.org/cipv5

www.sans.org/ics

Join us for the 11th Annual SANS ICS Summit in Orlando, Florida and learn the latest in achieving security in your ICS with presentations and training.

This year's Summit theme is "Defense is Doable" and promises to showcase the strengths defenders can take advantage of to ensure the safety and reliability of operations even in the face of advanced adversaries. With presentations from accomplished speakers and multiple SANS ICS classes, this year will show that defenders have an upper hand against attackers.

At the Summit, you will learn:

- Updates in the cyber threat landscape over the past year
- The latest in security and vulnerability research
- Incident response and network security monitoring tradecraft
- Methods to achieve compliance while enhancing security
- How to build and manage effective security teams

Six reasons to attend:

1. Choose from a variety of exciting classes including two brand new classes:
   ICS515 will teach you how to identify and respond to attackers while
   ICS456 will teach you how to meet NERC CIP regulations
2. Two days of presentations from leading ICS security researchers and experts in the field
3. Network with peers to learn industry-best practices in a friendly environment
4. Identify approaches to security that are NOT working from peers to minimize resource expenditures
5. CyberCity: Take part in or watch the highly rated ICS Mission Night where Summit participants take place in Red vs Blue team operations in an ICS-lab environment
6. Take away lessons and knowledge of where and how defense has worked, even against determined adversaries, to reinforce the theme that "Defense is Doable"

Follow us on Twitter @SANSICS for all the latest updates.

NEW COURSE – COMING SOON

ICS456

Essentials for NERC Critical Infrastructure Protection

The Essentials for NERC CIP five-day course empowers students with knowledge of the "What" and the "How" of the Version 5/6 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 to specific implementations. Additionally, the course covers implementation strategies for the Version 5/6 requirements with a balanced practitioner approach to both cybersecurity benefits as well as regulatory compliance.

Author Statement

The **SANS ICS456: Essentials for NERC Critical Infrastructure Protection** course was developed by SANS ICS team members with extensive electric industry experience including former Registered Entity Primary Contacts, a former NERC officer, and a Co-Chair of the NERC CIP Interpretation Drafting Team. Together the authors bring real-world, practitioner experience gained from developing and maintaining NERC CIP and NERC 693 compliance programs and actively participating in the standards development process.

www.sans.org/ics

ICS410: ICS/SCADA Security Essentials

Hands-On | Five Days | Laptop Required | 30 CPEs

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 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.

The course will provide you with:

- An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

With the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. In addition, IT support personnel who provide the communications paths and network defenses do not always grasp the systems' operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle.

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

www.giac.org

When these different groups of professionals complete this course, they will have developed an appreciation, understanding, and common language enabling them to work effectively together to secure their industrial control system environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world.

Course Day Topics

Day 1 ICS Overview

- Overview of ICS
- Field components
- Network components
- Communications
- ICS Application Overview
- Industry models
- ICS drivers and constraints
- Physical Security & Safety Systems

"The knowledge and tools obtained over the past 5 days are more than what I have gotten throughout my entire career."

–Khang Vodinh, Southwest Generation

Day 2 ICS Attack Surface

- Overview of ICS Attack Surface
- Attacks on HMIs and User Interfaces
- Attacks on Control Servers
- Attacks on Network Communications
- Attacks on Remote Devices

Day 3 Defending ICS Servers and Workstations

- ICS Server and Workstation Technologies
- ICS Server Operating Systems
- System and Security Updates
- Enforcing Security Policy
- Automation, Auditing, and Forensics
- System Processes and Services
- Logs and Log Management
- ICS System Hardening
- Databases and Historians

Day 4 Defending ICS Networks and Devices

- Network Fundamentals
- OSI Layers 1 & 2 Ethernet
- OSI Layers 3-4 IP, UDP, and TCP
- TCP/IP Based ICS Protocols
- Network Defenses
- Wireless Network Security
- Controller and Field Device Security
- Cryptography Fundamentals

Day 5 ICS Governance and Resources

- Information assurance foundations
- Computer Security Policies
- Contingency and Continuity Planning
- Risk assessment and auditing
- Password management
- Incident Handling
- Resources

ICS515: ICS Active Defense and Incident Response

Hands-On | Five Days | Laptop Required | 30 CPEs

ICS515: 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. This process of monitoring, responding to, and learning from threats is known as "active defense." It is the approach needed to appropriately counter advanced adversaries targeting ICS, as has been seen with malware such as Stuxnet, HAVEX, and BlackEnergy2. Students can expect to come out of this course fully understanding how to to deconstruct targeted ICS attacks, with a focus on delivery methods and observable attributes. This knowledge demystifies adversary capabilities and gives actionable recommendations to defenders. The course uses a hands-on approach that shows real-world malware and breaks down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of concepts such as generating and using threat intelligence, performing network security monitoring, and executing threat triage and incident response to ensure the safety and reliability of operations. The strategy presented in the course serves as a basis for ICS organizations looking to show that defense is doable.

Author Statement

"This class was developed from my experiences in the U.S. intelligence community and within the control system community dealing with advanced adversaries targeting industrial control systems. It is the class I wish I would have had available to me while protecting infrastructure against these adversaries. It is exactly what you'll need to maintain secure and reliable operations in the face of determined threats. ICS515 will empower you to prove that defense is doable." -Robert M. Lee

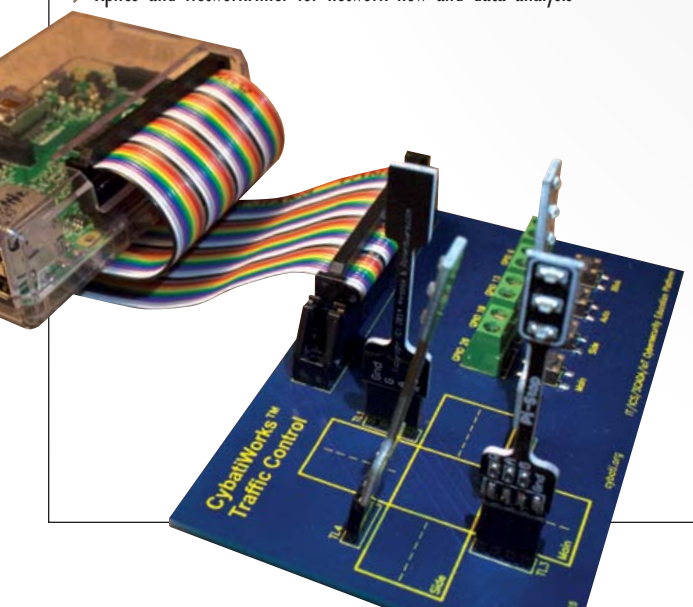
You Will Be Able To

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 operational technology (IT and OT) personnel
- Cybersecurity personnel
- IT- and OT-support personnel
- ICS incident responders
- ICS engineers
- Security Operations Center personnel



What You Will Receive

A fully functioning ICS515 CYBATIWorks Mini-Kit that students take with them after the class. The kit includes a Raspberry PI that functions as a PLC, physical components and attachments for I/O, a virtual machine with commercial control system demonstration software from Rex Controls and PeakHMI, and industrial protocols and software including OPC, ModbusTCP, DNP3, and more.

Course Day Topics

Day 1 Threat Intelligence

Today you will learn how threat intelligence is generated and how to critically analyze reports to determine what is and is not useful for ICS security. These analytical skills are useful in day-to-day operations and will enable you to approach problems in new and unique ways. We will set up the CYBATI Kit, review threat intelligence reports, and discover information available to adversaries about your ICS so that you can better prioritize network defenses.

Topics: Case Study: HAVEX; Introduction to Active Defense and Incident Response; Lab: CYBATI Kit Setup; Intelligence Life Cycle and Threat Intelligence; ICS Information Attack Surface; Lab: Pattern and Information Mapping; External Threat Intelligence; Internal Threat Intelligence; Lab: ICS Honeypot and Analysis of Competing Hypotheses; Sharing and Consuming Threat Intelligence; Lab: Consuming Threat Intelligence

Day 2 Asset Identification and Network Security Monitoring

Understanding the networked environment is the only way to fully defend it: you cannot defend what you do not know. This course section will teach you to use network tools to discover assets and visualize the network. This will then enable you to perform network security monitoring to identify threats to the ICS through the recognition of abnormalities and adversary tactics.

Topics: ICS Asset and Network Visibility; Lab: Asset Discovery and Network Visualization; Identifying and Reducing the Threat landscape; ICS Network Security Monitoring – Collection; Lab: Collecting the Right Data; ICS Network Security Monitoring – Detection; Lab: Detecting the Bad Data; ICS Network Security Monitoring – Analysis; Lab: Analyzing and Responding

Day 3 Incident Response

The ability to prepare for and perform incident response is vital to the safety and reliability of control systems. Incident response in the ICS environment is a young field with many challenges, but today you will learn effective tactics to collect and preserve quality forensic data. You will use this data to perform timely forensic analysis to verify that threats exist in the environment and make actionable recommendations to decision makers.

Topics: Incident Response and Digital Forensics Overview; Incident Response Fundamentals; Building an ICS Incident Response Team; Preparing Ahead of Time; Lab: Acquisition and Verification Part 1; Sources of Forensic Data in ICS Networks; Remote and Local Systems; Lab: Acquisition and Verification Part 2; Time-Critical Incident Response; Lab: Indicators in Action; Maintaining and Restoring Operations; Lab: Capturing the Malware

Day 4 Threat and Environment Manipulation

Understanding the threat is key to discovering its capabilities and the potential impact to the ICS. This information is also critical to making network changes for the purpose of security and sharing threat data internal and external to the organization. Today you will learn how to analyze initial attack vectors such as spearphishing emails, perform malware analysis techniques with memory forensics and dynamic malware analysis, and share threat data.

Topics: ICS Threat and Environment Manipulation Goals and Considerations; Establishing a Safe Working Environment; Initial Attack Vectors; Lab: Spearphishing Analysis; Memory Forensics; Lab: Memory Forensics; Malware Analysis Methodologies; ICS Malware Analysis Essentials; Lab: Dynamic Malware Analysis; Indicators of Compromise; Lab: Indicators of Compromise Development; Uncovering Ongoing Campaigns; Environment Manipulation and Lessons Learned

Day 5 Active Defense and Incident Response Challenge

Today focuses on reinforcing the strategy, methodologies, and skillsets that were introduced through the first four days of the course. This entirely hands-on session will present you with two scenarios to demonstrate different types of threats that affect ICS operations and will challenge you to respond to them appropriately.

Topics: Scenario One will present data from a complex ICS environment and require you to: Map the environment; Perform network security monitoring to identify abnormalities; Identify the adversary's capability in the network data and on the HMI; Analyze the malicious capability

Scenario Two will present a real-world advanced persistent threat capability and challenge you to: Analyze abnormal data in network captures; Perform forensic techniques on incident response captures; Identify the malicious capability and its functionality; Seek out and utilize threat intelligence to understand the adversary campaign

ICS Resources

SANS ICS Homepage

www.sans.org/ics

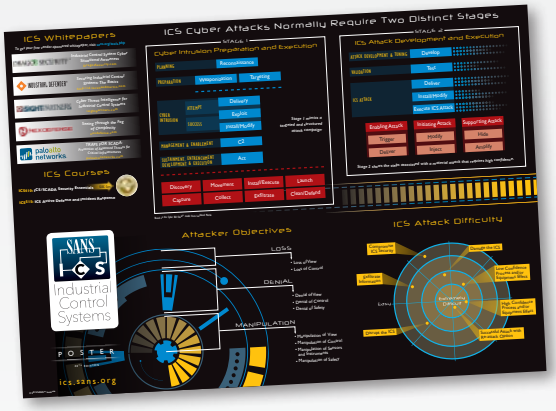
Twitter

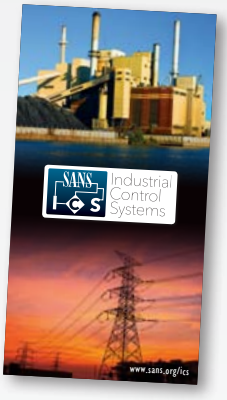
@sansics

Michael Assante: @assante_michael
Ted Gutierrez: @gutierrez_ted
Derek Harp: @Derek_Harp
Robert M. Lee: @RobertMLee

LinkedIn

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





ICS Posters and Brochures

https://ics.sans.org/resources/ics-security-resource-poster

SANS ICS Webcasts

https://ics.sans.org/resources/webcasts

SANS Analyst Surveys

https://ics.sans.org/resources/surveys

SANS Analyst Whitepapers

https://ics.sans.org/resources/whitepapers

ICS Resources

DHS Cybersecurity Evaluation Tool

http://ics-cert.us-cert.gov/Assessments

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

DHS ICS-CERT

(Industrial Control Systems Cyber Emergency Response Team)

http://ics-cert.us-cert.gov

ES-ISAC
ELECTRICITY SECTOR INFORMATION SHARING AND ANALYSIS CENTER
OPERATED BY NERC

NERC ES-ISAC

(Electricity Sector Information Sharing and Analysis Center)

www.esisac.com/SitePages/Home.aspx

ICS-ISAC

ICS-ISAC

(Industrial Control System Information Sharing and Analysis Center)

http://ics-isac.org

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST SP 800-82 Guide to ICS Security

http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

ISA

ISA99 Control System Security Committee

http://isa99.isa.org/ISA99%20Wiki/Home.aspx

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC CIP Standards

www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

HOSTED: Critical Infrastructure and Control System Cybersecurity

Hands-On | Five Days | Laptop Required | 30 CPEs

This is an intermediate-to-advanced course covering control system cybersecurity vulnerabilities, threats and mitigating controls. The course will provide hands-on analysis of control system environments, allowing students to understand the environmental, operational and economic impacts of attacks like Stuxnet and supporting mitigating controls.

What are the security risks of control system components, communication protocols, and operations?

Whether the control system is automating an industrial facility or a local amusement park roller coaster, the system was designed to operate in a physically, cyber and operationally secure domain. This domain extends throughout the facility using a combination of Programmable Logic Controllers, Programmable Automation Controllers, Embedded Logic Controllers, Remote Terminal Units, and Human Machine Interfaces interlinked with one or a variety of SCADA systems and communication protocols across local and long-distance geographic regions. The risks vary from simple eavesdropping or electronic denial of service to more sophisticated asset misuse and destruction. To further compound the challenge, today there are not enough professionals with security skills to sufficiently deter, detect and defend against active threats to our critical infrastructure's control systems.

How can you progress from control system security policy development to design, deployment, and assessment?

This course was designed to help organizations struggling with control system cybersecurity by equipping personnel with the skills needed to design, deploy, operate, and assess a control system's cybersecurity architecture. The course begins by quickly describing the risks and then introducing the participants to a customizable actuator and sensor control system trainer and programmable logic environment. This automation programming analysis creates the platform to identify logic flaws that, combined with active cyber, physical, and operational procedures, may lead to increased risk. The participants then use this knowledge to analyze the cyber, physical, and operational risks to control system architecture through:

- Control system component engineered, programmed and firmware logic flaws
- Wired and wireless communication protocol analysis
- Physical, cyber and operational procedures
- Deterrence, detection and response to threats

The participant's knowledge is challenged through non-kinetic and kinetic analysis associated with common industry components as well as red team/blue team exercises of both physical and simulated control system environments such as traffic lights, chemical storage and mixing, pipelines, robotic arms, heavy rail, and power grids.

Who Should Attend:

- Security personnel whose job involves assessing, deploying, or securing control system components, communications and operations
- Programmers and network and system administrators supporting control systems
- Process engineers and field technicians
- Operations and plant management personnel
- Control system vendor personnel
- Penetration testers
- NERC CIP, DHS CFATS and other auditors who need to build deeper technical skills
- Computer emergency response teams

HOSTED: Assessing and Exploiting Control Systems

Hands-On | Five Days | Laptop Required | 30 CPEs

This is not your traditional SCADA security course! This course teaches hands-on penetration testing techniques used to test embedded electronic field devices, network protocols, RF communications, and controlling servers of ICS and Smart Grid systems like PLCs, RTUs, smart meters, Home Area Networks (HAN), smart appliances, SCADA, substation automation, and synchrophasors. The course is structured around the formal penetration testing methodology created by the National Energy Sector Cybersecurity Organization Resource (NESCOR), a U.S. Department of Energy project.

Using this methodology and SamuraiSTFU (Security Testing Framework for Utilities), an open-source Linux distribution for pentesting energy sector systems and other critical infrastructure, we'll perform hands-on penetration testing tasks on embedded electronic field devices, their RF communications, and the myriad of user interfaces used throughout smart grid systems. We'll tie these techniques and exercises back to the smart grid devices that can be tested using these techniques. We will also do exercises on dissecting and fuzzing smart grid protocols like modbus, DNP3, IEC 61850, ICCP, ZigBee, C37.118, and C12.22. The course exercises will be performed on a mixture of real-world and simulated devices to give students the most realistic experience possible in a portable classroom setting.

"Very practical. An outstanding course!"

–Terry Ingoldsby, Amenaza Tech

What You Will Receive

- Latest version of SamuraiSTFU (Security Testing Framework for Utilities)
- A PDF version of the course slide deck
- Student hardware kits to use in class that must be returned at the end of class
- List of hardware items in the student kits and links to where students can purchase their own kits

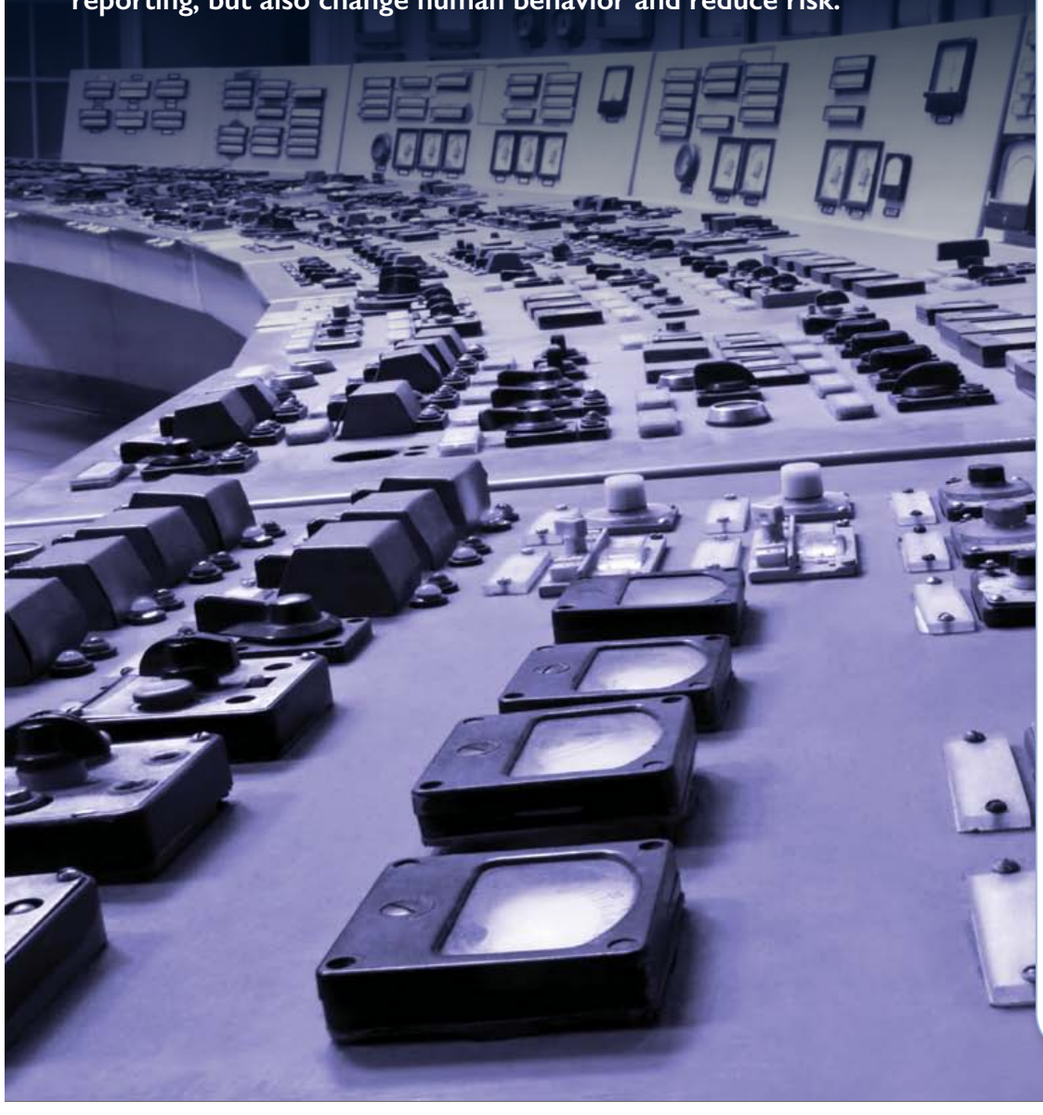
You Will Be Able To:

- Explain the steps and methodology used in performing penetration tests on Industrial Control and Smart Grid systems
- Use the free and open-source tools in SamuraiSTFU to discover and identify vulnerabilities in web applications
- Exploit several hardware, network, user interface, and server-side vulnerabilities

Securing The Human for Engineers

For additional information, please visit
www.securingthehuman.org/engineer

STH.Engineer focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems. This computer-based training solution provides an introduction to ICS, details types of ICS attacks, covers basic system and network defense approaches, and reviews ICS governance and policy best practices. These modules were developed to not only assist your organization in meeting compliance requirements through continued training and standard reporting, but also change human behavior and reduce risk.



This training consists of 10 modules and covers the following topics:

- **Overview of ICS** – Provides a brief history of ICS, regulation, and the need for ICS-focused security behavior training
- **ICS Drivers and Constraints** – Details the cybersecurity principle drivers and constraints that impact how a control system needs to be engineered, managed, supported, and interfaced with
- **Overview of ICS Attacks** – Provides an overview of ICS threat actors and examples of ICS-based attacks and trends
- **ICS Attack Surfaces** – Details specific attack approaches that target various layers of the ICS system
- **ICS Server Security** – Presents concepts specific to defending ICS environments at the server layer
- **ICS Network Security** – Presents concepts specific to defending ICS environments at the network layer
- **ICS System Maintenance** – Details ICS system maintenance tasks such as patching, backups, change management, monitoring, and logging
- **ICS Information Assurance** – Details 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
- **Attack Scenario** – Provides a detailed walkthrough of a cyber attack against an organization from the unique perspective of the attacker's actions

Author & Instructor Bios

Dr. Eric Cole

Dr. Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole has experience in information technology with a focus on helping customers address the right areas of security by building out a dynamic defense. Dr. Cole has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. He served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is the author of several books, including *Advanced Persistent Threat*, *Hackers Beware*, *Hiding in Plain Sight*, *Network Security Bible* 2nd Edition, and *Insider Threat*. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is the founder and an executive leader at Secure Anchor Consulting, where he provides leading-edge cybersecurity consulting services, expert witness work, and leads research and development initiatives to advance the state of the art in information systems security. Dr. Cole is actively involved with the SANS Technology Institute (STI) and is a SANS faculty Fellow and course author who works with students, teaches, and develops and maintains courseware.

Eric Cornelius

Eric Cornelius is currently a Technical Director at Cylance, Inc. and has recently served as the Chief Technical Analyst for DHS CSSP. As an active researcher in the field of cybersecurity since 2002, Mr. Cornelius supported many "boots-on-the-ground" engagements involving penetration testing, forensics, and malware analysis. Through these engagements, Mr. Cornelius aided multiple government, military, and private-sector organizations in protecting their networks and industrial control systems.

Paul A. Henry

Paul Henry is one of the world's foremost global information security and computer forensic experts, with more than 20 years of experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principal at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. Throughout his career, Paul has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. Paul also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the U.S. Department of Defense's Satellite Data Project, and both government as well as telecommunications projects throughout Southeast Asia. Paul is frequently cited by major and trade print publications as an expert in computer forensics, technical security topics, and general security trends and serves as an expert commentator for network broadcast outlets such as FOX, NBC, CNN, and CNBC. In addition, Paul regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications, such as the *Information Security Management Handbook*, to which he is a consistent contributor. Paul serves as a featured and keynote speaker at seminars and conferences worldwide, delivering presentations on diverse topics including anti-forensics, network access control, cyber crime, DDoS attack risk mitigation, firewall architectures, security architectures, and managed security services.

Robert M. Lee

Robert M. Lee is a co-founder at the critical infrastructure cybersecurity company Dragos Security LLC where he has a passion for control system traffic analysis, incident response, and threat intelligence research. He is a SANS Certified Instructor and the course author of SANS ICS515: Active Defense and Incident Response and the co-author of SANS FOR578: Cyber Threat Intelligence. He is a passionate educator although he should not be confused with the other Rob Lee at SANS – that Rob Lee is cooler but has less hair. Robert obtained his start in cybersecurity in the U.S. Intelligence Community where he served as an Air Force Cyber Warfare Operations Officer. He has performed defense, intelligence, and attack missions in various government organizations and established a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles and journals in publications such as Control Engineering, Wired, and Passcode and is a frequent speaker at conferences around the world. He is a non-resident National Cyber Security Fellow at the New America think tank and is currently pursuing his PhD at Kings College London with research into the cybersecurity of control systems. Lastly, Robert is the author of the book *SCADA and Me* and the weekly web-comic www.LittleBobbyComic.com.

Author & Instructor Bios

Matthew Luallen

Matthew E. Luallen is a well-respected information professional, researcher, instructor, and author. Mr. Luallen serves as the president and co-founder of CYBATI, a strategic and practical educational and consulting company. CYBATI provides critical infrastructure and control system cybersecurity consulting, education, and awareness. Prior to incorporating CYBATI, Matthew served as a co-founder of Encari and provided strategic guidance for the Argonne National Laboratory, U.S. Department of Energy, within the Information Architecture and Cyber Security Program Office. In an effort to promote education and collaboration in information security, Matthew is an instructor and faculty member at several institutions. Mr. Luallen is adjunct faculty for DePaul University, teaching the Computer Information and Network Security master's degree capstone course. He is also a certified instructor and CCIE for Cisco Systems, covering security technologies, such as firewalls, intrusion prevention, virtual private networks, and general secure information architecture. As a certified instructor for the SANS Institute, Matthew teaches infrastructure architecture, wireless security, web application security, regulatory and standards compliance, and security essentials. Mr. Luallen is a graduate of National Technological University with a master's degree in computer science, and he also holds a bachelor of science degree in industrial engineering from the University of Illinois, Urbana.

Billy Rios

Billy is an accomplished author and speaker. Billy is recognized as one of the world's most respected experts on emerging threats related to Industrial Control Systems (ICS), Critical Infrastructure (CI), and, medical devices. He discovered thousands of security vulnerabilities in hardware and software supporting ICS and critical infrastructure. He has been publically credited by the Department of Homeland Security (DHS) over 50 times for his support to the DHS ICS Cyber Emergency Response Team (ICS-CERT). Previously, Billy was a Lead at Google where he led the front line response for externally reported security issues and incidents. Prior to Google, Billy was the Security Program Manager at Internet Explorer (Microsoft). During his time at Microsoft, Billy led the company's response for several high profile incidents, including the response for Operation Aurora. Before Microsoft, Billy worked as a penetration tester, an intrusion detection analyst, and served as an active duty Marine Corps Officer. Billy currently holds an MBA and a Master of Science in Information Systems. He was a contributing author for several publications including: Hacking, the Next Generation (O'Reilly), Inside Cyber Warfare (O'Reilly), and The Virtual Battle Field (IOS Press).

Justin Searle

Justin Searle is a Managing Partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. Mr. Searle led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and played key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG). He currently leads the testing group at the National Electric Sector Cybersecurity Organization Resources (NESCOR). He has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences. Justin is currently a certified instructor for the SANS Institute. In addition to electric power industry conferences, he frequently presents at top international security conferences such as Black Hat, DEFCON, OWASP, Nullcon, and AusCERT. Mr. Searle co-leads prominent open-source projects including the Samurai Web Testing Framework (SamuraiWTF), the Samurai Security Testing Framework for Utilities (SamuraiSTFU), Middler, Yokoso!, and Laudanum. He has an MBA in International Technology and is a CISSP and SANS GIAC certified Incident Handler (GCIH), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT).

Graham Speake

Graham Speake is Vice President and Chief Product Architect at NexDefense. Previously to NexDefense, he was Principal Systems Architect for Yokogawa Electric Corporation, ISCI Marketing Chair, and an IEC62443 editor. Graham is an engineer with over 30 years' experience, the last 16 of which have been in the industrial cyber security arena for both end user companies and vendors. Graham has spent 10 years in BP looking at control systems security in both upstream and downstream business areas. Additionally, he has 5 years' experience in designing safety systems at Industrial Control Services. Graham is the author of a number of books and frequent contributor to magazine articles.

ICS Team Bios

Michael J. Assante

Michael Assante is currently the SANS lead for Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) security and Co-founder of NexDefense an Atlanta-based ICS security company. He served as Vice President and Chief Security Officer of the North American Electric Reliability (NERC) Corporation, where he oversaw industry-wide implementation of cyber security standards across the continent. Prior to joining NERC, Mr. Assante held a number of high-level positions at Idaho National Labs and served and as Vice President and Chief Security Officer for American Electric Power. Mr. Assante's work in ICS security has been widely recognized and was selected by his peers as the winner of Information Security Magazine's security leadership award for his efforts as a strategic thinker. The RSA 2005 Conference awarded him its outstanding achievement award in the practice of security within an organization. He has testified before the U.S. Senate and House and was an initial member of the member of the Commission on Cyber Security for the 44th Presidency. Before his career in security served in various naval intelligence and information warfare roles, he developed and gave presentations on the latest technology and security threats to the Chairman of the Joint Chiefs of Staff, Director of the National Security Agency, and other leading government officials. In 1997, he was honored as a Naval Intelligence Officer of the Year.

Tim Conway

Tim Conway is Technical Director of ICS and SCADA programs at SANS. He is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. He formerly served as the Director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO). He was responsible for Operations Technology, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric. He also served as an EMS Computer Systems Engineer at NIPSCO for eight years, with responsibility over the control system servers and the supporting network infrastructure. Mr. Conway is the former Chair of the RFC CIPC, Chair of the NERC CIP Interpretation Drafting Team, member of the NESCO advisory board, current Chair of the NERC CIPC GridEx Working Group, and Chair of the NBISE Smart Grid Cyber Security panel.

Ted Guitierrez

Ted Gutierrez, CISSP, GICSP, and GCIH, is the ICS & NERC CIP Product Manager at the SANS Institute. Mr. Gutierrez was most recently the Director of Operations Technology & NERC Compliance at Northern Indiana Public Service Company (NIPSCO) where he was responsible for compliance to NERC 693 and CIP standards and the support of the related operations technology systems. Mr. Gutierrez has over twenty-five years of experience working in the electric utility, information technology and manufacturing industries.

Derek Harp

Derek Harp is currently the Director for ICS Global Programs at SANS and the GICSP Steering Committee Chair. He is responsible for organizing events, resources and initiatives that educate and enable increased collaboration within the entire ICS security community. Mr. Harp has served as a founder, CEO, or advisor of early-stage companies for the last 16 years with a focus on cybersecurity. Derek is also a co-founder and a board member of NexDefense, Inc., a company focused on the security technology needs of ICS asset owners. Previously, he was the CEO and co-founder of LogiKeep, Inc., where he was the co-inventor of Intellishield,™ a pioneer IT security product which was subsequently acquired. Mr. Harp is a former U.S. Navy Officer with experience in combat information management, communications security, and intelligence.

GIAC Global Industrial Cyber Security Professional (GICSP)

The GICSP exam has 115 questions and a time limit of three hours. Once achieved, the GICSP certification is valid for four years.

The GICSP certification focuses on the knowledge of securing critical infrastructure assets. The GICSP bridges together IT, engineering and cybersecurity to achieve security for industrial control systems from design through retirement.

This unique vendor-neutral, practitioner-focused industrial control system certification is a collaborative effort between GIAC and representatives from a global industry consortium involving organizations that design, deploy, operate and/or maintain industrial automation and control system infrastructure. GICSP will assess a base level of knowledge and understanding across a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments.

This certification will be leveraged across industries to ensure a minimum set of knowledge and capabilities that IT, engineering, and security professionals must know if they are in a role that could impact the cybersecurity of an ICS environment.

GICSP Certification Objectives

- ICS Architecture
- ICS Security Assessments
- Industrial Control Systems
- ICS Modules and Elements Hardening
- Cybersecurity Essentials for ICS
- Configuration/Change Management
- ICS Security Governance and Risk Management

For a complete list of GICSP certification objectives, visit www.giac.org

The GIAC Certification Process

GIAC has the most technical certifications in the information security field. A GIAC certification demonstrates that holders have the skills and knowledge associated with the certifications they hold. The development of the GIAC exams involves a team of dedicated subject-matter experts (SMEs), volunteers who are leaders in the information security field, and a rigorous validation process. The GIAC certification process is also used to develop other exams, including eight ANSI ISO/IEC 17024:2003 accredited exams. The ANSI-approved certifications are GSEC, GCIA, GCIH, GCFA, GPEN, GSLC, and GSNA.

The certification process includes 12 steps and takes about 16 months from conception to completion.

Test Development/Assessment Certification Process

Identify Content

GIAC researches information security topics and collaborates with SMEs to determine the topics and contents of new exams.

Develop Specifications

GIAC technical directors and SMEs develop the exam specifications.

Write Items

SMEs write all of the GIAC exam items and each item is reviewed across three levels, using a minimum of three SMEs.

Level 1: Reviewed by another SME

Level 2: Reviewed by a second SME

Level 3: Reviewed by a GIAC technical director who is also a SME.

The GIAC Certification Exam Review Process:

- Review format, clarity, style, grammar, and spelling
- Properly cite and use appropriate references
- Provide rationale
- Assign the proper certification objective
- Determine cognitive level
- Verify key as the correct answer among the other options
- Develop plausible and attractive distractors
- Avoid negative phrasing of stem (e.g., NOT)
- Avoid trivial information in the stem and options

Review Items

At each review level, SMEs determine if each item should be accepted, revised or rejected. All items are banked and maintained in GIAC's Exam Management System (EMS). The GIAC EMS also maintains exam and item performance criteria and statistical information for quality measures and metrics.

Assemble Exam

Items are assembled into an exam format.

Administer Beta Exam

Once the exam is assembled, GIAC recruits beta testers. These beta testers take the exam and provide feedback. The GIAC technical directors review the feedback and make any necessary adjustments to the exam to assure that it meets test performance criteria and metrics.

Item Analysis

GIAC also conducts item analysis reviews at least once a year. Three indices are used when assessing item performance.

1. **Item Difficulty** – The percentage of candidates who answer the item correctly
2. **Item Discrimination** – Measured using the point-biserial correlations (RPBi). The RPBI suggests whether candidates with high scores are answering the questions correctly and vice versa.
3. **Distractor Response Distributions** – Distribution of the items, which includes the number of candidates answering for each option and the point-biserial correlations.

Standard Setting and Passing Point

A standard setting study using SMEs determines a recommended cut score or passing score. GIAC's scheme committee determines the passing point for the certification exam.

Equate Forms

GIAC employs an equating methodology to assure all candidates receive an exam form of equivalent difficulty.

Exam Goes Live!

GIAC exams are delivered in a proctored examination center. GIAC's partner for exam delivery is Pearson VUE, which has over 3,500 global examination centers for GIAC certification exams.

SANS ICS Industrial Control Systems

Upcoming ICS Events

Community SANS Long Beach
ICS410 | Long Beach, CA | Nov 2-6

SANS Sydney 2015
ICS410 | Sydney, Australia | Nov 9-21

SANS London 2015
ICS410 | London, United Kingdom | Nov 14-23

Community SANS Houston
ICS515 | Houston, TX | Nov 16-20

SANS Hyderabad 2015
ICS410 | Hyderabad, India | Nov 24 - Dec 4

Community SANS Denver
ICS515 | Denver, CO | Dec 7-11

SANS Cyber Defense Initiative 2015
ICS410 & ICS515 | Washington, DC | Dec 12-19

SANS Las Vegas 2016
ICS410 | Las Vegas, NV | Jan 9-14

SANS Security East 2016
ICS515 | New Orleans, LA | Jan 25-30

ICS Security training events will be added throughout the year.
Please check www.sans.org/ics for a complete listing of locations and dates.

Simulcast
ICS410 | Dec 14-18
sans.org/simulcast

OnDemand
E-learning Available Anytime, Anywhere, at Your Own Pace
sans.org/ondemand