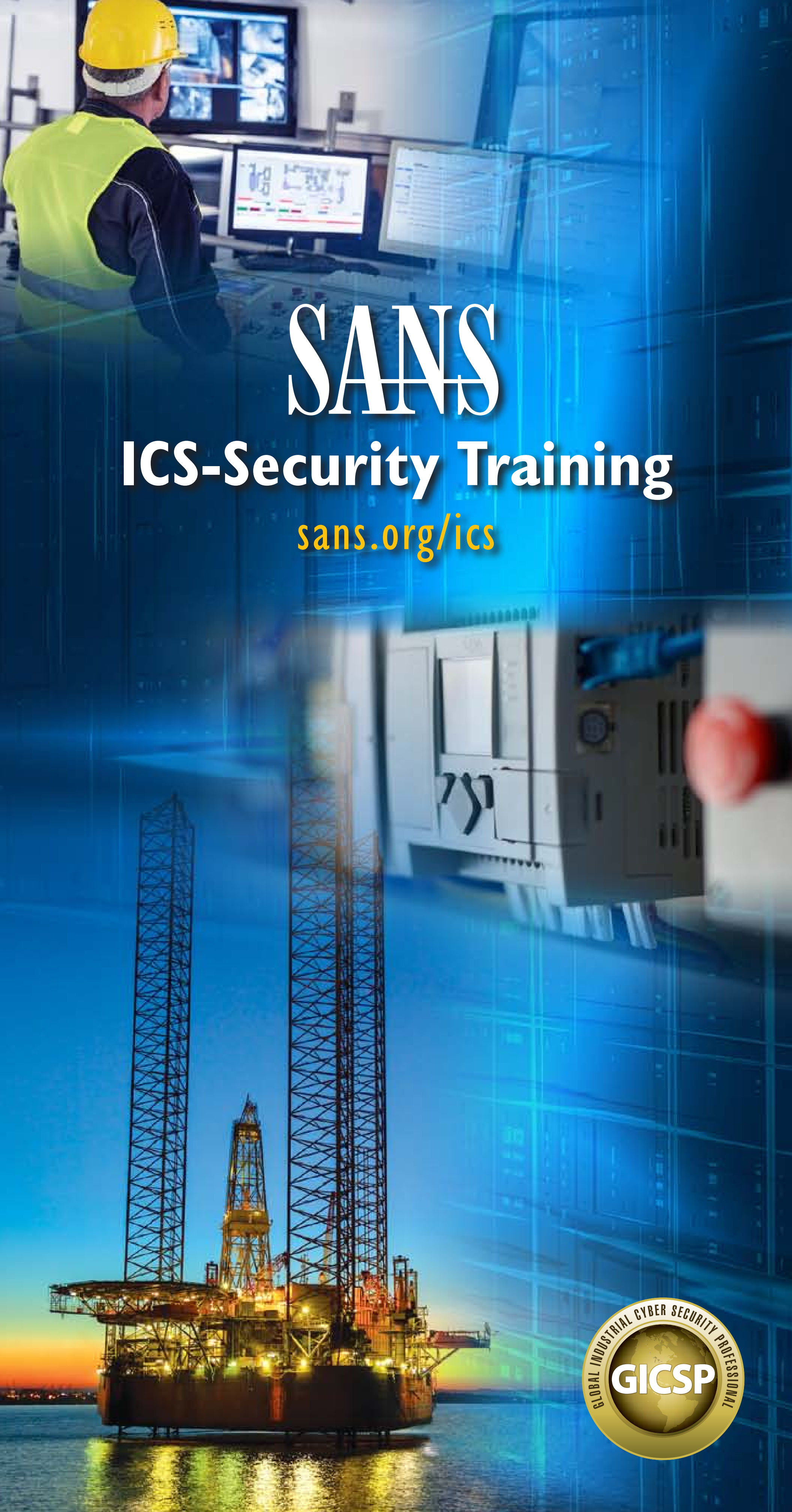


SANS

ICS-Security Training

sans.org/ics

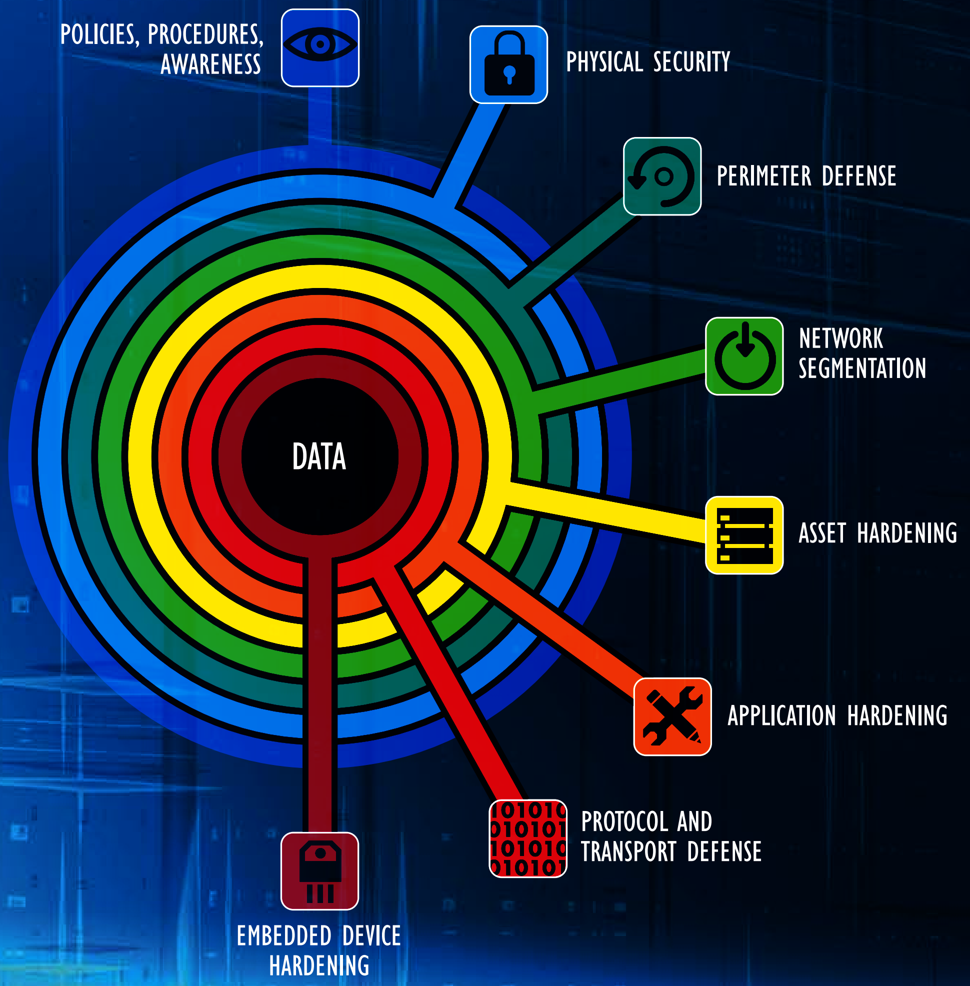
GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL

GICSP

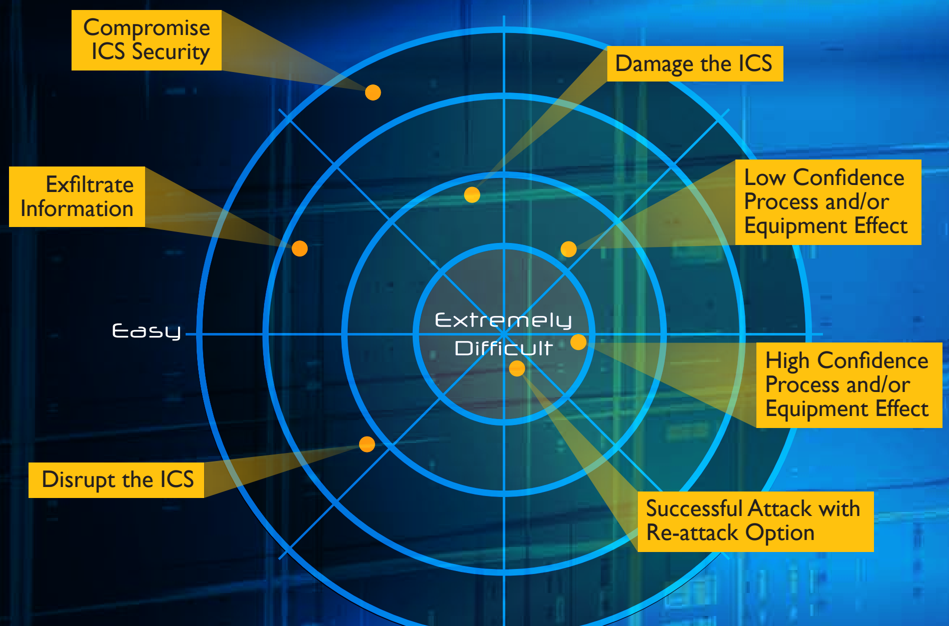
Why ICS?

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


Compromise ICS Security
Damage the ICS
Exfiltrate Information
Low Confidence Process and/or Equipment Effect
Easy
Extremely Difficult
High Confidence Process and/or Equipment Effect
Disrupt the ICS
Successful Attack with Re-attack Option

ICS Security is Critical Now

- 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 automate critical infrastructure operations at all levels.
- 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.

ICS410
ICS/SCADA Security Essentials

Hands-On | Five Days | Laptop Required | 30 CPEs | GIAC Cert: GICSP

sans.org/ics410

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
- A license to Windows 10 and a hardware PLC for students to use in class and take home with them.

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). CONTINUED ON PAGE 22

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

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.

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.

GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL
GICSP

Global Industrial Cyber Security Professional (GICSP)

The GICSP bridges together IT, engineering and cyber security 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.

www.giac.org

SANS ICS Industrial Control Systems
www.sans.org/ics

410.1 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. Each student will receive programmable logic controller (PLC) hardware to keep. The PLC contains physical inputs and outputs that will be programmed in class and mapped to an operator interface, or HMI, also created in class. This improved hardware-enabled approach provides the necessary cyber-to-physical knowledge that allows students to better understand important ICS operational drivers and constraints that require specific safety protection, communications needs, system management approaches, and cybersecurity implementations. Essential terms, architectures, methodologies, and devices are all covered to build a common language for students from a variety of different roles.

Topics: Global Industrial Cybersecurity Professional (GICSP) Overview; Overview of ICS; Field Components; Programming Controllers; Supervisory Components; 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. 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.

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. Students will examine concepts that benefit ICS systems such as system hardening, log management, monitoring, alerting, and audit approaches, then look at some of the more common applications and databases used in ICS environments across multiple industries.

Topics: Windows in ICS; Linux/Unix in ICS; Updates and Patching; Processes and Services; Configuration Hardening; Endpoint Defenses; 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 defense approaches. We'll first examine common IT protocols and network components used within ICS environments, then discuss ICS-specific protocols and devices. Technologies used to defend ICS networks will be reviewed along with implementation approaches. Students will interact with ICS traffic and develop skills to analyze it, then work through a number of tools to further explore a series of staged adversary actions conducted in a lab environment.

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

410.5 ICS Governance and Resources

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. On this final course day, students will work together on an incident response exercise that places them squarely in an ICS environment that is under attack. This exercise ties together key aspects of what has been learned throughout the course and presents students with a scenario to review with their peers. Specific incident-response roles and responsibilities are considered, and actions available to defenders throughout the incident response cycle are explored. Students will leave with a variety of resources for multiple industries and will be well prepared to pursue the GICSP, an important ICS-focused professional certification.

Topics: Information Assurance Foundations; Security Policies; Contingency and Continuity Planning; Risk Assessment and Auditing; Attack Tree Analysis; Password Management; Incident Handling; Incident Response; Resources

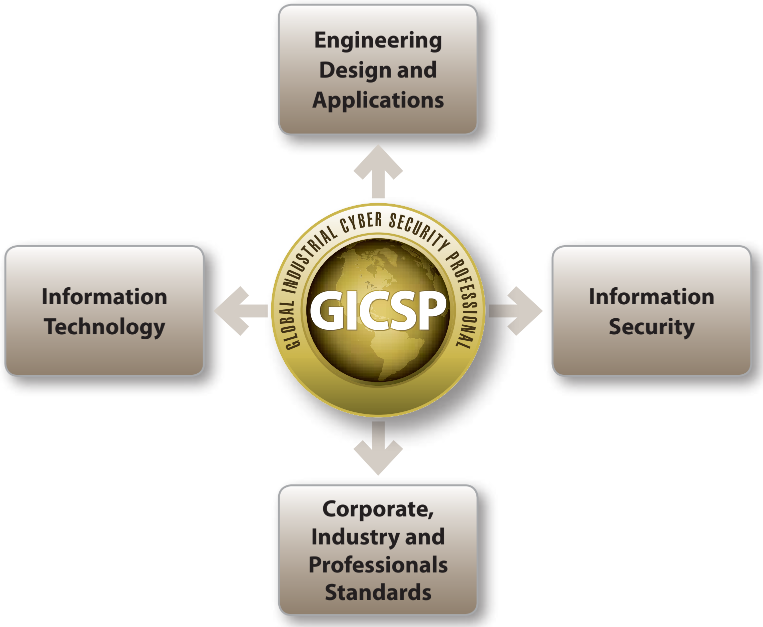
GIAC Global Industrial Cyber Security Professional (GICSP)

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. The GICSP is an important tool in assessing 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 is being 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.


Engineering Design and Applications
Information Technology
GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL
GICSP
Information Security
Corporate, Industry and Professionals Standards

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***

ICS515
ICS Active Defense & Incident Response

sans.org/ics515

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

NEW!

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.

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 the course author of SANS ICS515: Active Defense and Incident Response and the co-author of SANS FOR578: Cyber Threat Intelligence.

CONTINUED ON PAGE 21

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

SANS ICS Industrial Control Systems

www.sans.org/ics

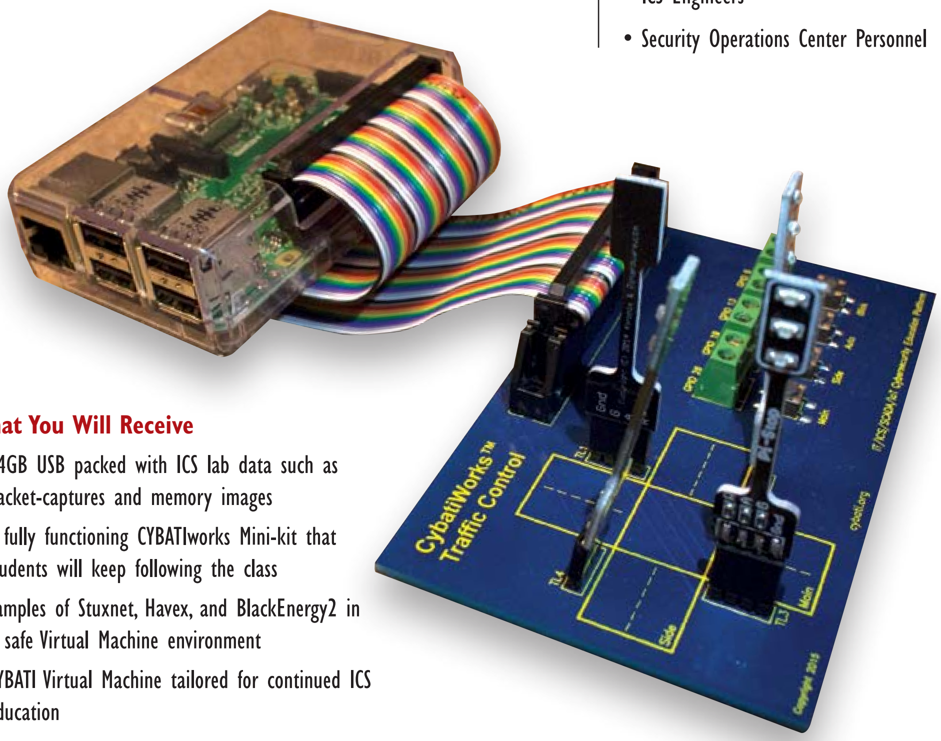
You Will Be Able To

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) Cybersecurity Personnel
- IT and OT Support Personnel
- ICS Incident Responders
- ICS Engineers
- Security Operations Center Personnel



What You Will Receive

- 64GB USB packed with ICS lab data such as packet-captures and memory images
- A fully functioning CYBATIworks Mini-kit that students will keep following the class
- Samples of Stuxnet, Havex, and BlackEnergy2 in a safe Virtual Machine environment
- CYBATI Virtual Machine tailored for continued ICS education
- REMnux Virtual Machine for malware analysis
- Security Onion Virtual Machine for monitoring the network and detecting threats

515.1 HANDS ON: Threat Intelligence

Industrial control system (ICS) security professionals must be able to leverage internal and external threat intelligence to critically analyze threats, extract indicators of compromise (IOCs), and guide security teams to find threats in the environment. Today you will learn how threat intelligence is generated, how to critically analyze reports, and the basic tenets of active defense functions. Students will become better analysts and critical thinkers by learning skills useful in day-to-day operations, regardless of their jobs and roles. This day features four hands-on labs that include building a Programmable Logic Controller (PLC), identifying information available about assets online through Shodan, completing an analysis of competing hypotheses, and ingesting threat intelligence reports to guide their practices over the rest of the labs in the course.

Topics: Case Study: Havex; Introduction to ICS Active Defense and Incident Response; Intelligence Life Cycle and Threat Intelligence; ICS Information Attack Surface; External ICS Threat Intelligence; Internal ICS Threat Intelligence; Sharing and Consuming ICS Threat Intelligence

515.2 HANDS ON: 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 students to use tools such as Wireshark, TCPdump, SGUIL, ELSA, CyberLens, Bro, NetworkMiner, and Snort to map their ICS network, collect data, detect threats, and analyze threats to drive incident response procedures. During this section, students will be introduced to the lab network and an advanced persistent threat (APT) that is present on it. Drawing on threat intelligence from the previous course section, students will have to discover, identify, and leverage the threat using their new active defense skills to guide incident responders to the affected Human Machine Interface (HMI).

Topics: Case Study: BlackEnergy2; ICS Asset and Network Visibility; Identifying and Reducing the Threat Landscape; ICS Network Security Monitoring – Collection; ICS Network Security Monitoring – Detection; ICS Network Security Monitoring - Analysis

515.3 HANDS ON: Incident Response

The ability to prepare for and perform ICS incident response is vital to the safety and reliability of control systems. ICS incident response is a core concept in an ICS active defense and requires that analysts safely acquire digital evidence while scoping the environment for threats and their impact on operations. ICS incident response is a young field with many challenges, but students in this section will learn effective tactics and tools to collect and preserve forensic-quality data. Students will then use these data to perform timely forensic analysis and create IOCs. In the previous section's labs, APT malware was identified in the network. In this section, the labs will focus on identifying which system is impacted and gathering a sample of the threat that can be analyzed.

Topics: Case Study: Stuxnet; Incident Response and Digital Forensics Overview; Preparing an ICS Incident Response Team; Evidence Acquisition; Sources of Forensic Data in ICS Networks; Time-Critical Analysis; Maintaining and Restoring Operations

515.4 HANDS ON: Threat and Environment Manipulation

Understanding the threat is key to discovering its capabilities and its potential to affect the ICS. The information extracted from threats through processes such as malware analysis is also critical to being able to make the necessary changes to the environment to reduce the effectiveness of the threat. The information obtained is vital to an ICS active defense, which requires internal data collection to create and share threat intelligence. In this section, students will learn how to analyze initial attack vectors such as spearphishing emails, perform timely malware analysis techniques, analyze memory images, and create Indicators of Compromise in YARA. The previous section's labs identified the infected HMI and gathered a sample of the APT malware. In this section's labs, students will analyze the malware, extract information, and develop YARA rules to complete the active defense model introduced in the class and maintain operations.

Topics: Case Study: German Steelworks; ICS Threat and Environment Manipulation Goals and Considerations; Establishing a Safe Working Environment; Analyzing Acquired Evidence; Memory Forensics; Malware Analysis Methodologies; Case Study: BlackEnergy2 Automated Analysis; Indicators of Compromise; Environment Manipulation

515.5 HANDS ON: Active Defense and Incident Response Challenge

This section focuses on reinforcing the strategy, methodologies, skillsets, and tools introduced in the first four sections of the course. This entirely hands-on section will present students with two different scenarios. The first involves data collected from an intrusion into SANS Cyber City. The second involves data collected from a Distributed Control System (DCS) infected with malware. This section will truly challenge students to utilize their ICS active defense and incident response skills and test themselves.

Topics: **Scenario One:** Identify the assets and map the ICS networks; Perform ICS network security monitoring to identify the abnormalities; Execute ICS incident response procedures into the SANS Cyber City data files; Analyze the malicious capability and determine if the threat is an insider threat or a targeted external threat
Scenario Two: Identify the software and information present on the DCS; Leverage ICS active defense concepts to identify the real-world malware; Determine the impact on operations and remediation needs

The ICS Cyber Kill Chain

Written by
Michael J. Assante and
Robert M. Lee

The Industrial Control System Cyber Kill Chain

Written by
Michael J. Assante and Robert M. Lee

October 2015

©2015 SANS™ Institute

The ICS Cyber Kill Chain is a model that builds upon the traditional understanding of a cyber kill chain and tailors it to adversary attacks on ICS. The model provides defenders an opportunity to better understand the phases of an adversary's campaign into an ICS to identify opportunities for detection, remediation and defense. These opportunities for success also highlight that ICS networks are more defensible than traditional IT networks and stress the importance of maintaining this defensible architecture through actions such as limiting the integration of safety systems with operations networks and removing ICS components from direct Internet access.

The complete whitepaper can be found at
sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

SANS ICS Industrial Control Systems
www.sans.org/ics

ICS456
Essentials for NERC Critical Infrastructure Protection

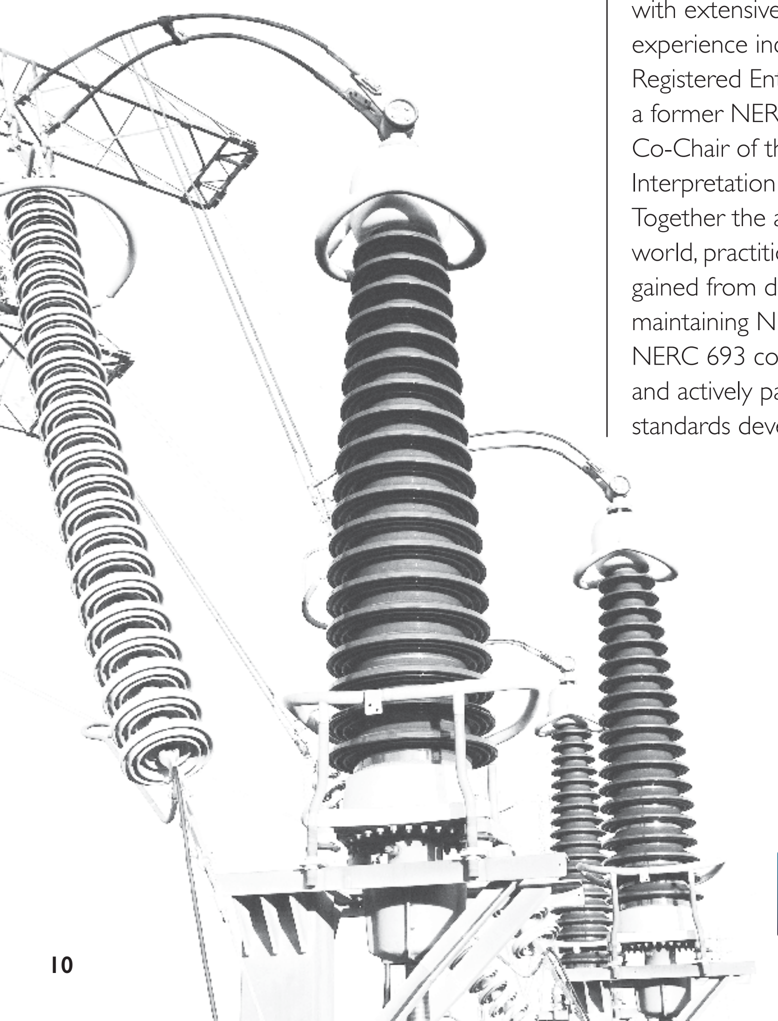
NEW!

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

The Essentials for NERC CIP five-day course empowers students with knowledge of the "What" and the "How" of current and pending versions of the 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 current and pending versions of the standards with a balanced practitioner approach to both cybersecurity benefits as well as regulatory compliance.

About the Authors

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.



SANS ICS Industrial Control Systems

www.sans.org/ics

Day 1 Asset Identification and Governance

A transition is underway from NERC CIP programs that are well defined and understood to a new CIP paradigm that expands its scope into additional environments and adds significant complexity. On Day 1, students will develop an understanding of the electric sector regulatory structure and history as well as an appreciation for how the CIP Standards fit into the overall framework of the reliability standards. Key NERC terms and definitions related to NERC CIP are reviewed using realistic concepts and examples that prepare students to better understand the concepts. We will explore multiple approaches to BES Cyber Asset identification and learn the critical role of strong management and governance controls. The day will examine a series of architectures, strategies, and difficult compliance questions in a way that highlights the reliability and cybersecurity strengths of particular approaches. Unique labs will include a scenario-based competition helping bring the concepts to life and highlight the important role we play in defending "the grid."

Day 2 Access Control and Monitoring

Strong physical and cyber-access controls are at the heart of any good cybersecurity program. During Day 2, we move beyond the "what" of CIP compliance to understanding the "why" and the "how." Firewalls, proxies, gateways, IDS, and more – learn where and when they help and learn practical implementations and designs to avoid. Physical protections include more than fences and you'll learn about the strengths and weaknesses of common physical controls and monitoring schemes. Labs will reinforce the learnings throughout the day and will introduce architecture review and analysis, firewall rules, IDS rules, compliance evidence demonstration, and physical security control reviews.

Day 3 System Management

CIP-007 has been one of the most violated Standards since CIP v1 and through v3. With the CIP Standards moving to a systematic approach with varying requirement applicability based on impact rating, the industry now has new ways to design and architect system management approaches. Throughout day-3, students will dive into CIP-007, various Systems Security Management requirements, with a focus on implementation examples and challenges. This day will also cover the CIP-010 requirements for configuration change management and vulnerability assessments that ensure systems are in a known state and under effective change control. We'll move through a series of labs that reinforce the topics covered from the perspective of the CIP practitioner responsible for implemenation and testing.

Day 4 Information Protection and Response

Education is key to every organization's success with NERC CIP and the students in ICS456 will be knowledgeable advocates for CIP when they return to their workplace. Regardless of their role, each student can be a valued resource to their organization's CIP-004 training program, and their CIP-011 information protection program. Students will be ready with resources for building and running strong programs that reinforce the need for information protection and cybersecurity training. Day 4 also examines CIP-008 and CIP-009 and reviews the various roles and responsibilities needed in an incident response or a disaster recovery event.

Day 5 CIP Process

On the final day, students will learn the key components required to run an effective CIP Compliance program. We will cover recurring and audit-related process tasks that affect everyone involved in CIP Compliance: annual assessments, gap analysis, TFEs, self-reporting, audit management, audit preparation, and after-action processes. We'll also look into the future of CIP, including RAI, lessons learned, FERC directives, committees, guidelines, interpretations, and other industry resources. Students will leave with a strong call-to-action to engage in the on-going development of CIP within their organization and throughout the industry.

sans.org/sec562

SEC562
CyberCity Hands-on Kinetic Cyber Range Exercise

NEW!

Hands-On | Six Days | Laptop Required | 36 CPEs

Computers, networks, and programmable logic controllers operate most of the physical infrastructure of our modern world, ranging from electrical power grids, water systems, and traffic systems all the way down to HVAC systems and industrial automation. Increasingly, security professionals need the skills to assess and defend these important infrastructures. In this innovative and cutting-edge course based on the SANS CyberCity kinetic range, you will learn how to analyze and assess the security of control systems and related infrastructures, finding vulnerabilities that could result in significant kinetic impact.

NETWARS CYBERCITY
www.sans.org/netwars/cybercity

What is NetWars CyberCity?

NetWars CyberCity, our most in-depth and ambitious offering, is designed to teach warriors and infosec pros that cyber action can have significant kinetic impact in the physical world. As computer technology, networks, and industrial control systems permeate nearly every aspect of modern life, military, government, and commercial organizations are realizing an increasing need for skilled defenders of critical infrastructures. We engineered and built CyberCity to help organizations grow these capabilities in their teams.

CyberCity is a 1:87 scale miniaturized physical city that features SCADA-controlled electrical power distribution, as well as water, transit, hospital, bank, retail, and residential infrastructures. CyberCity engages participants to defend the city's components from terrorist cyber attacks, as well as to utilize offensive tactics to retake or maintain control of critical assets.

You Will Learn:

- How to analyze cyber infrastructures that control and impact kinetic infrastructures.
- How to manipulate a variety of key industrial protocols, including Modbus, CIP, DNP3, Profinet, and other SCADA-related protocols.
- How to rapidly prototype computer attack tools against specific vulnerabilities
- How to discover security flaws in a variety of SCADA and Industrial Control Systems (ICSs) and thwart attacks against them.
- How to conduct penetration tests and assessments associated with kinetic infrastructures.

The Main Objectives of CyberCity

- Teach cyber warriors and their leaders the potential kinetic impacts of cyber attacks
- Provide a hands-on, realistic kinetic cyber range with engaging missions to conduct defensive and offensive actions
- Develop capabilities for defending and controlling critical infrastructure components to mitigate or respond to cyber attacks
- Demonstrate to senior leaders and planners the potential impacts of cyber attacks and cyber warfare

Participants engage in missions, with specific operation orders, describing the defensive or offensive goal they need to achieve. In some missions, participants prevent attackers from undermining the CyberCity infrastructure and wreaking havoc, with all the kinetic action captured through streaming video cameras mounted around the physical city. In offensive missions, participants must seize control of CyberCity assets, retaking them from adversaries and using them to achieve a kinetic impact specified in their operation orders. Each mission includes not only a list of goals to be achieved, but also specific sensitive city assets that are out of bounds for the engagement, requiring additional tactical planning to adhere to the rules of engagement.

To achieve mission objectives, participants work as a team, engaging in effective mission planning, devising overall strategies and particular tactics, and exercising detailed technical skills. Furthermore, some participants will be charged as leaders of their teams, helping to build and assess leadership skills, decision making capabilities, and the ability to brief senior leadership. Multiple realistic defensive and offensive missions test the cyberspace engineers ability to thwart the best efforts of a well-funded terrorist organization or other cyber attacker trying to control city assets.

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.

HOSTED

Assessing and Exploiting Control Systems

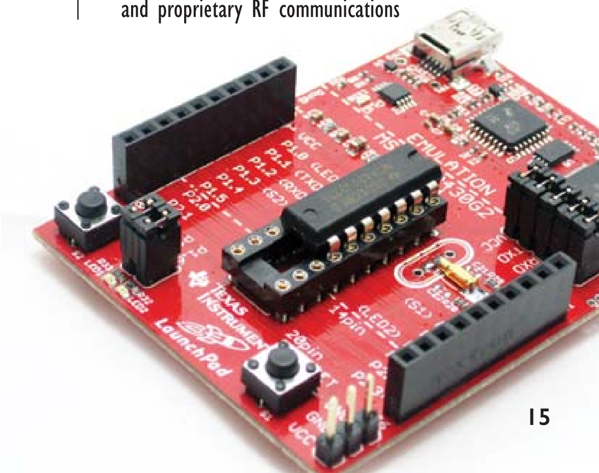
Hands-On | Three/Six Days | Laptop Required | 18/36 CPEs

This is not your traditional SCADA/ICS/IoT security course! How many courses send you home with your own PLC and a set of hardware/RF hacking tools?!? This course teaches hands-on penetration testing techniques used to test individual components of a control system, including embedded electronic field devices, network protocols, RF communications, Human Machine Interfaces (HMIs), and various forms of master servers and their ICS applications. Skills you will learn in this course will apply directly to systems such as the Smart Grid, PLCs, RTUs, smart meters, building management, manufacturing, Home Area Networks (HAN), smart appliances, SCADA, substation automation, and synchrophasors. This course is structured around the formal penetration testing methodology created by UtiliSec for the United States Department of Energy. Using this methodology and Control Things Pentest Platform (previously SamuraiSTFU), an open source Linux distribution for pentesting energy sector systems and other critical infrastructure, we will perform hands-on penetration testing tasks on user interfaces (on master servers and field device maintenance interfaces), control system protocols (modbus, DNP3, IEC 60870-5-104), RF communications (433MHz, 869MHz, 915MHz), and embedded circuit attacks (memory dumping, bus snooping, JTAG, and firmware analysis). We will tie these techniques and exercises back to control system devices that can be tested using these techniques. The course exercises will be performed on a mixture of real world and simulated devices to give students the most realistic experience as possible in a portable classroom setting.

Advances in modern control systems such as the energy sector's Smart Grid has brought great benefits for asset owners/operators and customers alike, however these benefits have often come at a cost from a security perspective. With increased functionality and addition inter-system communication, modern control systems bring a greater risk of compromise that vendors, asset owners/operators, and society in general must accept to realize the desired benefits. To minimize this risk, penetration testing in conjunction with other security assessment types must be performed to minimize vulnerabilities before attackers can exploit critical infrastructures that exist in all countries around the world. Ultimately, this is the goal of this course, to help you know how, when, and where this can be done safely in your control systems.

What You Take Home

- Latest version of the Control Things Pentest Platform on DVD or USB
- PDF version of the course slide deck
- A hardware PLC, programming software, and HMI software
- Hardware pentest kit to test embedded electronics and proprietary RF communications



SANS CIP Cybersecurity Training

SANS CIP Program (STH.CIP) 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 R2.

The CIP program consists of 12 computer-based modules addressing the 49 topic areas identified in the NERC CIP training requirements plus an additional module covering CIP-014. 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 R1, CIP-004 R2, and CIP-003 R2.1.

The CIP 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.CIP 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.ciptraining.org

Securing the Human for Engineers

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.

www.securingthehuman.org/engineer

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

1. **Overview of ICS** – Provides a brief history of ICS, regulation, and the need for ICS-focused security behavior training
2. **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
3. **Overview of ICS Attacks** – Provides an overview of ICS threat actors and examples of ICS-based attacks and trends
4. **ICS Attack Surfaces** – Details specific attack approaches that target various layers of the ICS system
5. **ICS Server Security** – Presents concepts specific to defending ICS environments at the server layer
6. **ICS Network Security** – Presents concepts specific to defending ICS environments at the network layer
7. **ICS System Maintenance** – Details ICS system maintenance tasks such as patching, backups, change management, monitoring, and logging
8. **ICS Information Assurance** – Details ICS-focused information assurance program concepts of risk management, account management, data classification, and defense in depth
9. **ICS Incident Handling** – Covers important ICS incident-response topics for all individuals who interact with ICS environments
10. **Attack Scenario** – Provides a detailed walkthrough of a cyber attack against an organization from the unique perspective of the attacker's actions

SANS Industrial Control Systems

www.sans.org/ics

ICS SECURITY

SUMMIT & TRAINING

ORLANDO, FL | WINTER SUMMIT

For SCADA, Industrial Automation, and Control System Security

Join us for the 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 prepared 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 that "Defense is Doable"

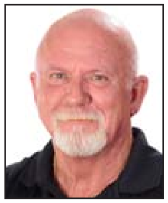
Follow us on Twitter @SANSICS for all the latest updates.

Author & Instructor Bios

At SANS, we are privileged to have an instructor corps considered to be the best in the world. Not only do our instructors meet SANS' stringent requirements for excellence, they are all real-world practitioners. What you learn in class will be up to date and relevant to your job.

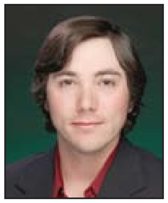
Dr. Eric Cole

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 Cybersecurity 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.



Paul A. Henry

Paul A. 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.



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.

Robert M. Lee

Robert M. Lee is the course author for ICS515 - Active Defense and Incident Response and co-author of FOR578 - Cyber Threat Intelligence. He is also the CEO of Dragos Security and a non-resident national cybersecurity fellow at New America. Robert stood up a first of its kind mission in the U.S. Intelligence Community identifying national adversaries breaking into critical infrastructure and he is also the author of SCADA and Me.

www.LittleBobbyComic.com

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 Cybersecurity 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.

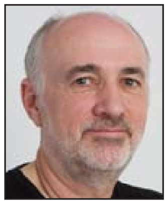
Author & Instructor Bios

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).



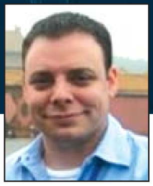
Graham Speake

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 cybersecurity 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 cybersecurity 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 Cybersecurity 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.

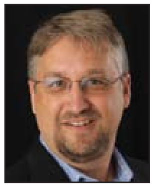


Tim Conway

Tim Conway is the 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 Cybersecurity 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.

ICS Resources

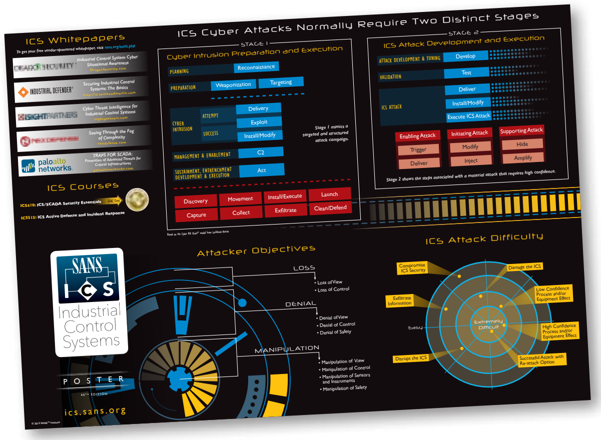
www.sans.org/ics

@sansics

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

Linked in

www.linkedin.com/company/sans-ics


ICS Whitepapers
ICS Cyber Attacks Normally Require Two Distinct Stages
Cyber Intrusion Preparation and Execution
ICS Attack Development and Execution
ICS Courses
Attacker Objectives
ICS Attack Difficulty
LOSS
DENIAL
MANIPULATION
SANS ICS Industrial Control Systems
POSTER
ics.sans.org

ICS Posters and Brochures

http://ics.sans.org/ics_library/ics-sliding-scale-poster-2015

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

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

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

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events

Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers

sans.org/security-training/by-location/all

ONLINE TRAINING

OnDemand

E-learning Available Anytime, Anywhere, at Your Own Pace

sans.org/ondemand

Simulcast

Attend a SANS Training Event without Leaving Home

sans.org/simulcast

SANS ICS SUMMIT

CYBER SECURITY CHALLENGE

sans.org/event/ics-security-summit-2016/ics-challenge

The SANS ICS Summit Cybersecurity Challenge is debuting in 2016 to support continued learning and skill development on ICS security and ever-changing ICS components and processes.