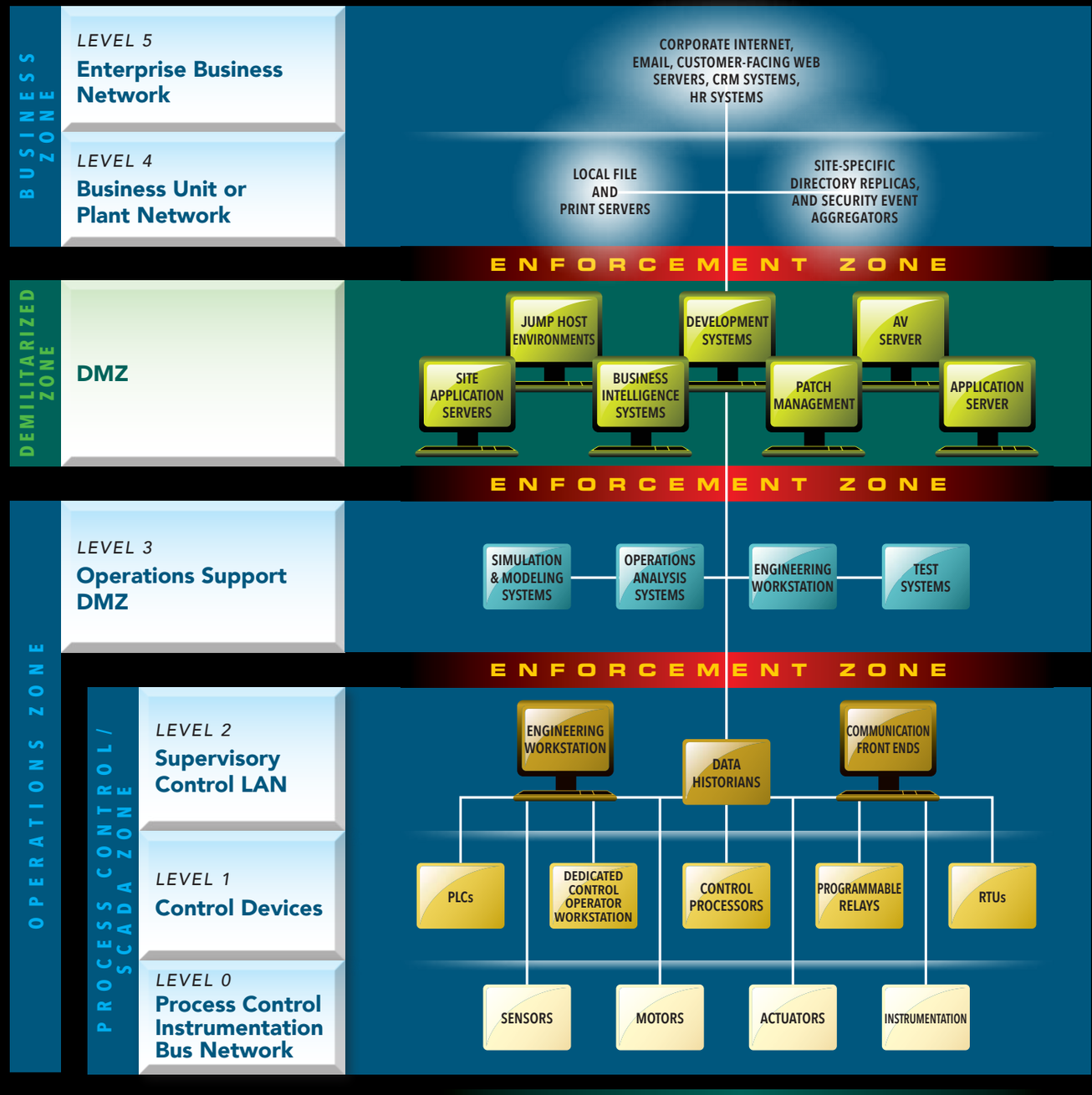

SANS
ICS
Industrial
Control
Systems
InterCity
www.sans.org/ics

Why ICS?

SANS has joined forces with industry leaders and experts to strengthen the cybersecurity of Industrial Control Systems (ICS). The initiative is turning ICS cybersecurity around by equipping both 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 is working to provide ICS-focused curricula and certifications, as well as community resources such as promotional materials, white papers, and security practice application guidance.

Control System Architecture



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 ICS incidents are occurring 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 can help keep our critical systems safe**
- **Shared learning translates into results-effective security requires the integration of cybersecurity professionals, ICS support staff, and engineers**

SAFETY ZONE

Includes safety-specific systems that are engineered for a particular protective function. Items typically found in this zone include all those identified in Level 0 and 1 with a dedicated purpose for a safety control function like; acoustic monitoring, liquid chemistry monitoring, vibration monitoring, and emission monitoring. In most safety systems there is control function that serves to protect the operation and personnel.

ENFORCEMENT ZONE

Includes the functions necessary to segment and protect the various zones within an ICS environment. Items typically found in this zone include Firewalls, Routers (with ACLs), Application Firewalls, Data Guard technology, and Unidirectional Data Diode technology. Technologies implemented may differ in the various enforcement zones within an ICS environment depending on business needs and the level of risk.

ICS410: ICS/SCADA Security Essentials

NEW

Hands-On | Five Days | Laptop Required | 30 CPE/CMU Credits

SANS has joined forces with industry leaders to change the game by equipping both security professionals and control system engineers with necessary cybersecurity skills to defend national critical infrastructure. This course will provide a standardized foundational set of skills, knowledge and abilities for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending Industrial Control Systems (ICS) is trained to perform work in a manner that will keep the operational environment safe, secure and resilient against current and emerging cyber threats.

When the authors of this course examined where the greatest risks exist throughout the critical infrastructure sectors and where the greatest need is, they talked a lot about core security principles that are needed for the various roles that work on or support control systems daily. Where there are available courses for higher level security practitioners who need to develop very specific skill sets like industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and hands on red team training. The issue with these training curricula is that they are not focused on the largest collection of individuals who operate, manage, design, implement, monitor, or integrate the production control systems throughout the critical infrastructure.

Due to the dynamic nature of Industrial Control System components, many engineers do not fully understand the feature sets and risks in many devices, and IT support personnel who provide the communications paths and network defense do not always understand the operational drivers and constraints of the control systems. Efforts need to be undertaken to ensure the traditional IT personnel fully understand the design principles underlying the control systems and how to support the systems in a manner that does not impact availability, and ensures integrity. The need for IT support education is paralleled with the need for control system engineers and operators to further develop an understanding of the important role they play in cybersecurity. This starts with ensuring that a control system is designed and engineered with cybersecurity built in and provided the same level of focus throughout the system lifecycle as is system reliability.

When the students complete the course they should have developed an appreciation, understanding, and a common language that will enable these various important groups to work together to secure their ICS environments. This course will help develop cyber secure aware engineering practices, as well as real-time control system IT / OT support personnel who understand the physical effects of actions in the cyber world.

Who Should Attend:

Individuals who interact with or who could impact Industrial Controls System environments. The roles performed by personnel specific to this field can roughly be divided in 4 domains:

- IT (includes OT support)
- IT Security (includes OT security)
- Engineering
- Corporate, industry, and professional standards

Course Day Topics

Day 1 ICS Overview

- Brief History of ICS
- Overview of ICS
- Field Components
- Network Components
- Communication Paths & Telecommunications
- Applications
- Industry Models
- ICS Drivers and Constraints
- Physical & Safety Security

Day 2 ICS Attacks

- Overview of Attacks
- Attacks on HMIs
- Attacks on Control Servers
- Attacks on Network Communications
- Attacks on Remote Devices

Day 3 System Defense

- The Security Infrastructure
- Security Policies and Templates
- Service Packs, Patches, and Backups
- Auditing and Components Automation
- Linux Landscape
- Linux Command Line
- Linux OS Security
- Linux Security Tools
- Maintenance, Monitoring, and Auditing Linux

Day 4 Network Defense

- IP Behavior
- Firewalls and Perimeters
- Wireless
- Cryptography
- Enbedded Security Defenses

Day 5 Governance and Resources

- Information assurance foundations
- Risk assessment and auditing
- Password management
- Incident Handling
- Resources

Course Includes:

- Understanding of Industrial Control System components, purpose, deployments, significant drivers and constraints
- Hands-on lab learning approach to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident response in a control system environment
- Governance models and resources for ICS professionals

HOSTED: SCADA Security Training

Hands-On | Five Days | Laptop Required | 30 CPE/CMU Credits

This is a hands-on SCADA Security course with more than 20 exercises and labs that are performed on a portable SCADA lab that contains over 15 different PLCs, RTUs, RF, and telemetry devices. The course has already trained more than 1,300 professionals around the world, and has been constantly refined over the past four years. It was designed to bridge the skills sets of Control System Engineers, Technicians, and IT Security professionals. The first day is spent diving deep into teaching how ICS and SCADA Systems work from the ground up. Instrumentation, I/O, control techniques, automation theory, HMI visualization, and data archival systems are broken down at their functional level. Several SCADA protocols are taught, captured, dissected, and then used to hack into the embedded devices. OPC, ModbusTCP, and EthernetIP are some of the ICS protocols that are used in live hands-on exercises and labs.

Everyone in the course builds their own SCADA system by implementing and designing their own OPC servers, data tags, and HMI graphics. RF and telemetry systems used in SCADA, ICS, and Smart Grid applications are covered, and live demonstrations are provided on the following RF systems: 900 MHz Spread Spectrum, Zigbee (802.15.4), WirelessHART, Bluetooth, and WiFi (2.4 and 5.6 GHz). Wireless hacking demonstrations convey the weaknesses and security hardening required when using wireless systems in ICS and SCADA applications.

Once all of the ICS and RF concepts are completely understood, the course shifts into a penetration and exploitation mindset. The students are taught how to find security vulnerabilities in ICS and SCADA system components, how to safely conduct penetration testing against live ICS and SCADA systems, and how to conduct Cyber Vulnerability Assessments that satisfy the NERC CIP and DHS CFATS regulations. The Metasploit framework is taught using the BackTrack environment. The hands-on exercises start with basic Linux commands, and by the end of the course, students are creating their own buffer overflows and other exploits using Metasploit, NETCAT, HPING, and other open-source tools.

After everyone has built their own SCADA system, and spent time learning how to attack these real-time systems, the course rounds out the process by explaining how to defend these systems from similar threats. The defense techniques include how to design secure SCADA architectures, where to place firewalls, how to implement secure remote access into SCADA environments, where to deploy IDS / IPS systems, and tips for implementing centralized log aggregation and network monitoring solutions.

The instructors for this course collectively have more than 20 years of experience conducting Cyber Security Penetration Testing and Vulnerability Assessments on live operational ICS and SCADA Systems. This makes them uniquely qualified to provide the tips and feedback necessary to address the complex problems brought to them by students during the course.

This Course Will Answer the Questions Below – and Many More – Related to SCADA Security

- What are the unique vulnerabilities and security risks of ICS systems?
- What approach should be used to test Internet, Enterprise IT, and ICS systems for security vulnerabilities?
- What are the common security weaknesses in Internet and Enterprise IT Systems that pose the greatest risk to ICS systems?
- Can poorly managed ICS systems pose an even greater risk to Enterprise IT and Internet-connected systems?
- What is a solid approach to testing SCADA systems for security vulnerabilities?
- When and how do you conduct penetration testing on live SCADA equipment?
- How do you use open-source security tools to research and discover unknown vulnerabilities with ICS equipment?
- What are solid techniques for securing SCADA systems that are not vendor-specific, and require low administrative overhead?
- Can social networking information about employees found on sites like Facebook, Linkedin, MySpace, and Twitter be used to compromise critical industrial facilities?
- What is a Red Team or Tiger Team Attack Exercise, and how can these scenarios simulate a targeted attack on a SCADA facility?

HOSTED: Pentesting ICS and Smart Grid

Hands-On | Five Days | Laptop Required | 30 CPE/CMU Credits

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 United States 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

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

What You Will Receive

- Power for your laptop
- Internet connectivity may or may not be available depending on the facility hosting the course
- 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

HOSTED: Critical Infrastructure and Control System Cybersecurity

Hands-On | Five Days | Laptop Required | 30 CPE/CMU Credits

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 we 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 utilize this knowledge to analyze the control system architecture through cyber, physical and operational risks including:

- **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, 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

What is critical infrastructure Control System cybersecurity?

Control systems (Local, Distributed and SCADA systems) are used throughout the world to automate common processes. These systems need to provide reliable and safe automation for such critical infrastructures as the Bulk Electric System (BES), natural gas, oil, transportation, chemical, mining, fresh water/waste water, manufacturing, food, and defense. The critical necessities for both government and its people to survive are automated using Industrial Control Systems. In the past decade, advances in technology have added automation that has intertwined these systems with the Internet, wireless, business networks and traditional hardware and communications protocols. Many control systems are in some way electronically connected to networks of less trust, potentially even a slight distance away from the Internet. These control systems typically use vulnerable communication protocols. Many even use TCP/IP and in specific situations, common off-the-shelf hardware and chipsets. It is paramount to the safety of our society to sufficiently understand the architecture of these critical systems and protect them.

Certification

GIAC Global Industrial Control Systems Professional (GICSP)

The SANS GIAC team, working with industry experts, has developed a vendor-neutral, practitioner-focused Industrial Control System certification.

The Global Industrial Cyber Security Professional Certification (GICSP) assesses 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, engineer, and security professionals should know if they are in a role that could impact the cyber security of an ICS environment.

GICSP Certification Objectives

- Architecture
- Assessments
- Configuration and Change Management
- Log Collection and Management
- Incident Management
- Information Risk and Security Management
- System Hardening
- Cybersecurity Essentials
- Assess Management
- Physical Security
- Industrial Control Systems

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. GIAC's 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, GSNA 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
- Rationales
- 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 the examination 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

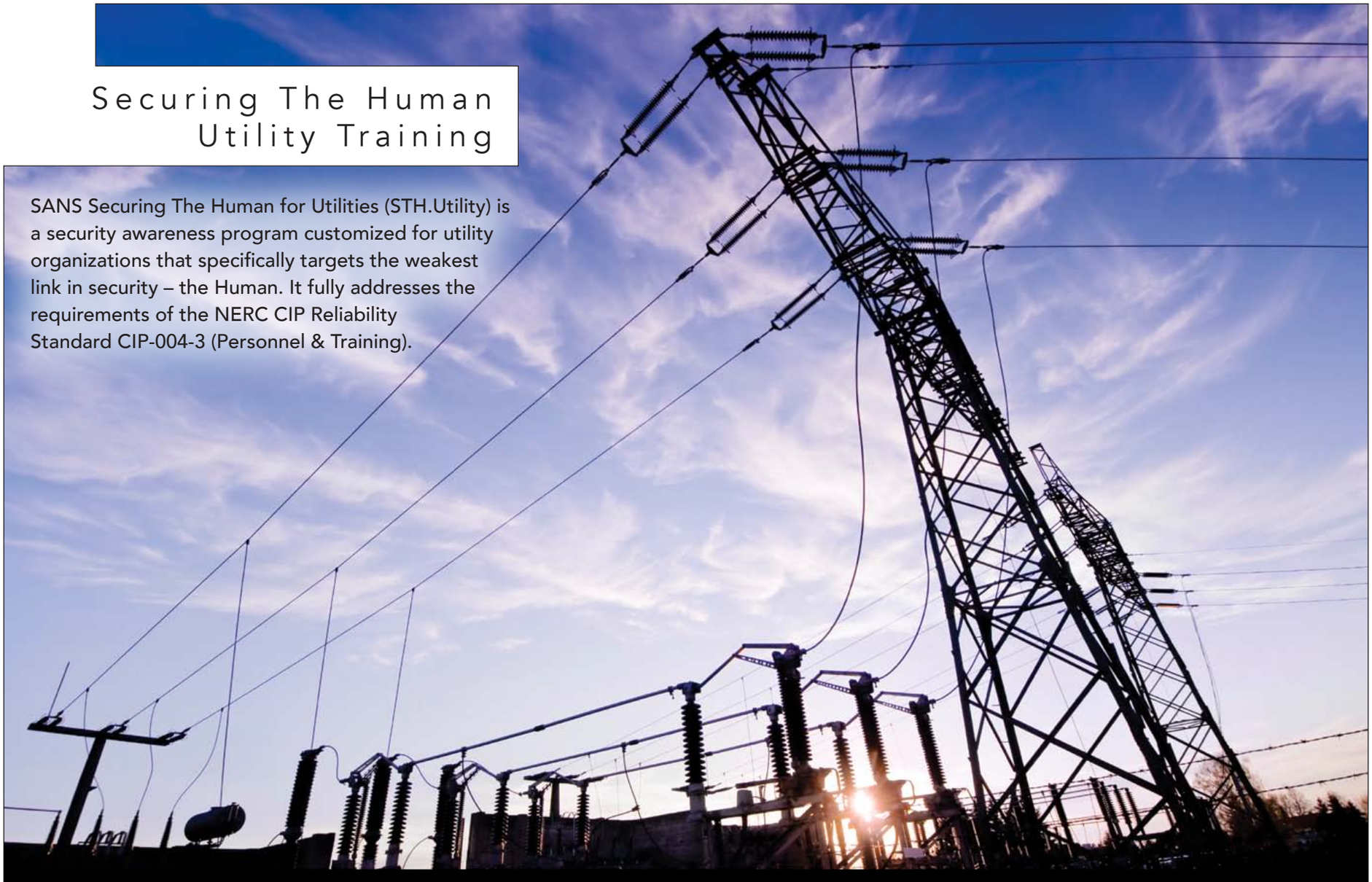
GIAC employs an equating methodology to assure all candidates receive an exam form of equivalent difficulty.

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.

Securing The Human Utility Training

SANS Securing The Human for Utilities (STH.Utility) is a security awareness program customized for utility organizations that specifically targets the weakest link in security – the Human. It fully addresses the requirements of the NERC CIP Reliability Standard CIP-004-3 (Personnel & Training).



Topics include:

- **Overview of NERC and FERC**
- **Introduction to the NERC CIP Standards**
- **Identification and Proper Use of Critical Cyber Assets**
- **Physical Access Controls to Critical Cyber Assets**
- **Electronic Access Controls to Physical Cyber Assets**
- **Proper Handling of Critical Cyber Asset Information**
- **Recovery of Critical Cyber Assets following a Cybersecurity Incident**

In addition to these modules, the Utility package includes the entire suite of SANS Securing The Human Security Awareness modules (23 in total).

www.securingthehuman.org/utility

Coming Soon!

Securing The Human for Engineers

SANS has developed Securing the Human for Engineers, which focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems (ICS). This training consists of 10 core modules and provides an ICS overview, an understanding of ICS attacks, and covers basic system and network defense approaches in an ICS environment, as well as governance and policy resources. The program was developed to not only assist your organization in meeting compliance requirements through continued training and standard reporting, but also to change human behavior and reduce risk.

Author and 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.

Mark Heard

Mark Heard is a native Tennessean and graduate of Auburn University with a degree in electrical engineering. He worked at Eastman Chemical Company in Kingsport, TN, as a control systems engineer for over 30 years. Mr. Heard has experience with a variety of Industrial Control Systems and applications and a continuing interest in computer and network technologies. He has been active in ACC Cybersecurity Program teams and ISA99 standard working groups since 2002. Mr. Heard has also represented the chemical sector on the DHS Process Control Systems Forum and Industrial Control Systems Joint Working Group. He helped write the "Roadmap to Secure Control Systems in the Chemical Sector" and chartered the Roadmap Implementation Working Group for that sector. Mr. Heard spent a year in the IT Security Group at Eastman before working at Red Tiger Security providing ICS cybersecurity assessment, consulting, and training.

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, Mr. Luallen 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, Mr. Luallen is an instructor and faculty member at several institutions. Mr. Luallen is adjunct faculty for DePaul University, teaching the Computer Information and Network Security Masters degree capstone course. He is also a certified instructor and CCIE for Cisco Systems, covering security technologies, such as firewalls, intrusion prevention, and virtual private networks, and general secure information architecture. As a certified instructor for the SANS Institute, Mr. Luallen 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.

Jonathan Pollet

Jonathan Pollet, Founder and Principal Consultant for Red Tiger Security, USA has over 12 years of experience in both Industrial Process Control Systems and Network Security. After graduating from the University of New Orleans with honors and receiving a B.S. degree in Electrical Engineering, he was hired by Chevron and designed and implemented PLC and SCADA systems for onshore and offshore facilities. In 2001 he began to publish several white papers that exposed the need for security for Industrial Control Systems (ICS), and is still active in the research of vulnerabilities within real-time ICS systems. Throughout his career, he has been involved with SANS, IEEE, ISA, ISSA, UTC, CSIA, and other professional organizations. Mr. Pollet has developed and presented workshops on SCADA Security to the FBI, Department of Homeland Security, and Utility Telecom Council, and has spoken at many conferences and workshops around the world.

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. Mr. Searle 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).

Daniel Michaud-Soucy

Mr. Michaud-Soucy has over 5 years of experience in the fields of Computer Engineering, Systems Engineering, and Computer Programming. Over the past few years, he has focused on conducting cybersecurity assessments specifically on SCADA and Industrial Control Systems. He has been the lead technical role in several field assessments, and is well versed in the proprietary SCADA and APT Assessment methodology used by Red Tiger Security for both on-site data collection and offsite data analysis.

ICS Team

Michael J. Assante

Michael Assante is currently the SANS lead for training on Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) security. Mr. Assante was most recently Chief Executive Officer of NBISE and Chair of NBISE's National Board. He previously held the position of Vice President and Chief Security Officer at the North American Electric Reliability Corporation and oversaw the implementation of cybersecurity standards across the North American electric power industry. Prior to joining NERC, Mr. Assante held notable positions at Idaho National Labs, was Vice President and Chief Security Officer for American Electric Power, and pioneered the security intelligence landscape in his role as Chief Operating Officer of LogiKeep. A former U.S. Navy intelligence officer with experience in information warfare and information security management, Mr. Assante recognized the need to bring intelligence-type analysis to the networks of the corporate world by identifying risks and threats specific to the hardware, software and systems used by individual organizations.

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, current 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.

Derek Harp

Derek Harp is currently the business operations lead for the Industrial Control System (ICS) programs at SANS. Mr. Harp has served as a founder, CEO, advisor, of early-stage companies for the last sixteen years with a focus on cybersecurity. Mr Harp 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

SANS ICS Homepage
http//www.sans.org/ics

Twitter
@sansics

DHS Cybersecurity Evaluation Tool
http://ics-cert.us-cert.gov/Assessments

DHS ICS-CERT
http://ics-cert.us-cert.gov

NERC ES-ISAC
http://www.esisac.com/SitePages/Home.aspx

ICS-ISAC
http://ics-isac.org

Cybersecurity Vulnerability NSTB Program
http://energy.gov/oe/downloads/common-cyber-security-vulnerabilities-observed-control-system-assessments-inl-nstb

Vulnerability Analysis of Energy Delivery Control Systems
http://energy.gov/oe/downloads/vulnerability-analysis-energy-delivery-control-systems-2011

NIST SP 800-82 Guide to ICS Security
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

ISA-99 Control System Security Committee
http://isa99.isa.org/ISA99%20Wiki/Home.aspx

NERC CIP Standards
http://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

SANS Webcasts

Building an ICS Security Program: Where to Begin
https://www.sans.org/webcasts/building-ics-security-program-96167

Results of the SANS SCADA Security Survey
https://www.sans.org/webcasts/results-scada-security-survey-95745

Building an ICS Security Program: Where to Begin
https://www.sans.org/webcasts/building-ics-security-program-96167

Traditional Attack Motives must be Tailored for the ICS World
https://www.sans.org/webcasts/traditional-attack-motives-tailored-ics-world-96707

Why Every CSO Needs to Know Industrial Control Systems (ICS)
https://www.sans.org/webcasts/cso-industrial-control-systems-ics-96867

Why Every CSO Needs to Know Industrial Control Systems (ICS) (Singapore)
https://www.sans.org/webcasts/cso-industrial-control-systems-ics-96942

ICS Component Security Testing - Field Devices
https://www.sans.org/webcasts/ics-component-security-testing-field-devices-96560

ICS Component Security Testing - Field Devices (Singapore)
https://www.sans.org/webcasts/ics-component-security-testing-field-devices-singapore-96915

More added monthly! For the latest, go to www.sans.org/industrial-control-systems/resources

SANS Industrial Control Systems

NORTH AMERICA

ICS SECURITY SUMMIT

Lake Buena Vista, FL
March 12-18, 2014

www.sans.org/event/north-american-ics-scada-summit-2014

www.sans.org/info/138037

To download a free QR reader
www.mobile-barcodes.com/qr-code-software

SANS
5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

PROMO CODE

Register using this Promo Code

Save $400 when you register and pay by January 22, 2014
www.sans.org/event/north-american-ics-scada-summit-2014