SANS

11TH ANNUAL

ICS SECURITY

SUMMIT & TRAINING

February 16-23, 2016 | Orlando, FL

Training from industry experts on attacker techniques, testing approaches in ICS, and defensive capability in ICS environments.

Because "Defense is Do-able"

sans.org/ICSSummit-2016

SCHEDULE

	TUE 2-16	WED 2-17	THU 2-18	FRI 2-19	SAT 2-20	SUN 2-21	MON 2-22	TUE 2-23
ICS456 Essentials for NERC Critical Infrastructure Protection **NEW!**		Page 1						
ICS410 ICS/SCADA Security Essentials		Page 2						
ICS515 ICS Active Defense and Incident Response **NEW!**		Page 4						
SEC562 CyberCity Hands-on Kinetic Cyber Range Exercise **NEW!**	Page 6							
SEC573 Python for Penetration Testers		Page 8						
HOSTED Assessing and Exploiting Control Systems	Page 9							
HOSTED Critical Infrastructure and Control System Cybersecurity		Page 10						
MGT433 Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program					Pg 10			
ICS Security Summit							Pg 12	
NetWars - CyberCity					Pg 7			

Evening Bonus Sessions

Take advantage of these extra evening presentations and add more value to your training. Learn more on page 11.

- *KIPS: Kaspersky Industrial Protection Simulation*
- *WOPR: Shall We Play a Game?*
- *ICS Wall*
- *NetWars CyberCity*
- *SANS ICS Challenge (SIC)*

Hear what your peers have said about the SANS ICS Summit

"As a newbie I was not sure what was meant by a 'Summit.' What I found is frank discussions covering diverse topics in ICS and the audience gets to ask hard questions and they get honest answers, not fluff."
-Marc Hayden NuScale Power, LLC

"It really helped to hear the alternative perspectives from others and to know that others are fighting the same battles that we are."
-Steve Weisner, Encana Corporation

"The ability to interact with other people who are interested in SCADA Systems was a great opportunity to learn about new ways of thinking."
-Roberto Blanco Galicia, Secretaria de Seguridad Publica

"It reduces the gap between IT and SCADA system people and gives you the flavor of IT and the flavor of SCADA systems together."
-Bilal Namankani, Saudi Aramco

Be sure to register and pay for any 4-6 day course by Jan 6th for a $400 tuition discount!

Register today for ICS Security Summit 2016!
sans.org/ICSSummit-2016

@SANSICS
Join the conversation:
#ICSSummit

ICS456
Essentials for NERC Critical Infrastructure Protection

Hands-On | Five Days | Wed, Feb 17 - Sun, Feb 21 | Laptop Required | 30 CPEs

NEW!

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.

Who Should Attend

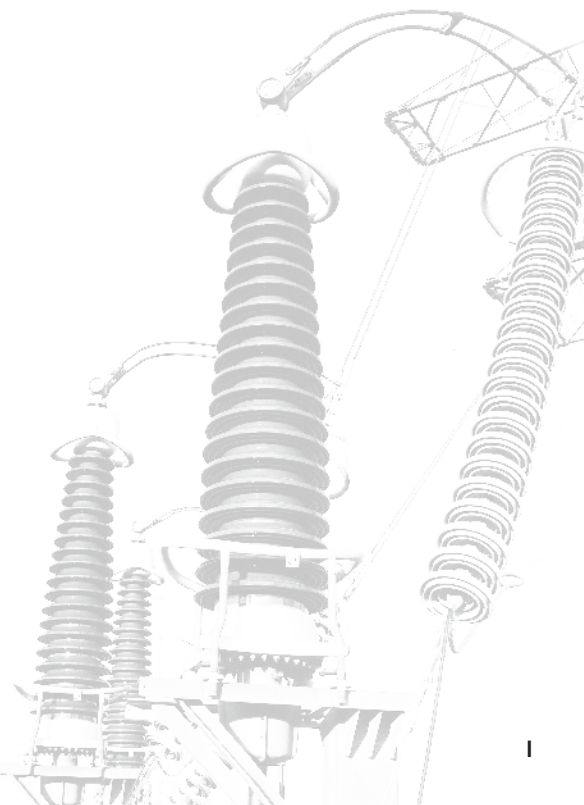
Individuals with CIP responsibilities in the following areas:

- IT and OT (ICS) cybersecurity
- Field support personnel
- Security operations
- Incident response
- Compliance staff
- Team leaders
- Governance
- Vendors/Integrators
- Auditors

INSTRUCTOR

Tim Conway

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



ICS410
ICS/SCADA Security Essentials

Hands-On | Five Days | Wed, Feb 17 - Sun, Feb 21 | Laptop Required | 30 CPEs

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. **ICS410: ICS/SCADA Security Essentials** provides an introductory set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals
- A license to Windows 10 and a hardware PLC for students to use in class and take home with them.

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

INSTRUCTOR

Justin Searle

Justin Searle is a Managing Partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. Justin 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. Justin 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). @meeas

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)

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

www.giac.org

ICS515
ICS Active Defense & Incident Response

Hands-On | Five Days | Wed, Feb 17 - Sun, Feb 21 | Laptop Required | 30 CPEs

NEW!

ICS515: ICS Active Defense and Incident Response will empower students to understand their networked industrial control system 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.

INSTRUCTOR

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. He is also the author of *SCADA and Me*. www.LittleBobbyComic.com @RobertMLee

Author Statement

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

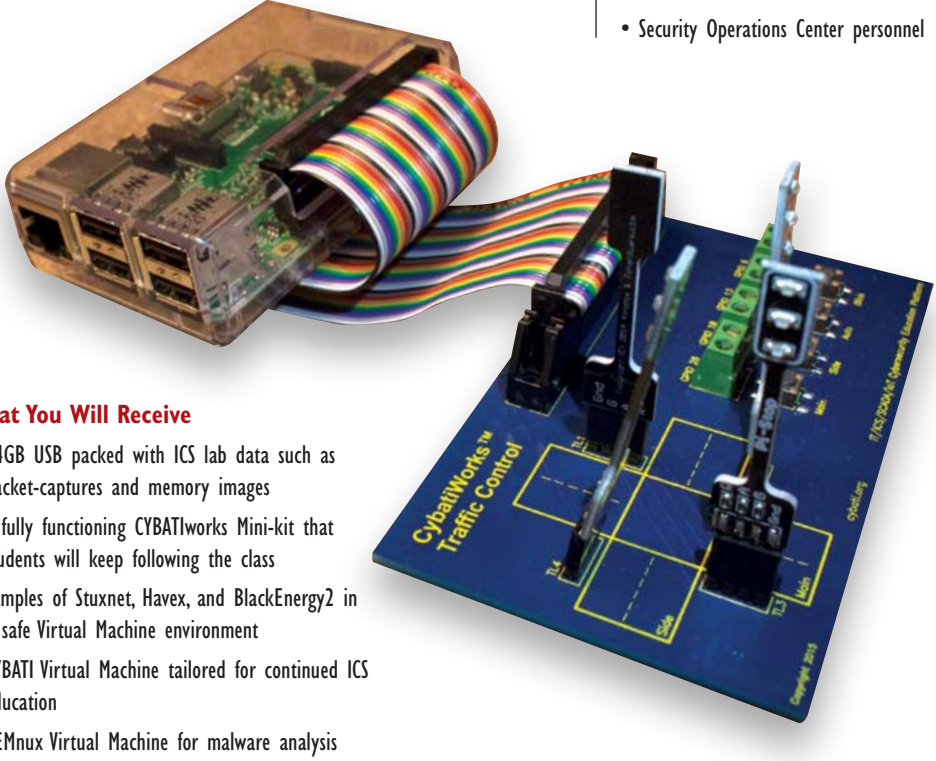
You Will Be Able To

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

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

Who Should Attend

- Information technology and operational technology (IT and OT) 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

SEC562
CyberCity Hands-on Kinetic Cyber Range Exercise

Hands-On | Six Days | Tue, Feb 16 - Sun, Feb 21 | Laptop Required | 36 CPEs

NEW!

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 this important infrastructure. 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 infrastructure, finding vulnerabilities that could result in a significant kinetic impact.

What Is NetWars CyberCity?

NetWars CyberCity is designed to teach warriors and InfoSec professionals that cyber action can have a 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 infrastructure. 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.

INSTRUCTOR

Tim Medin

Tim Medin is a senior technical analyst at Counter Hack, a company devoted to the development of information security challenges for education, evaluation, and competition. Through the course of his career, Tim has performed penetration tests on a wide range of organizations and technologies. Prior to Counter Hack, Tim was a Senior Security Consultant for FishNet Security, where the majority of his focus was on penetration testing. He gained information security experience in a variety of industries including control systems, higher education, financial services, and manufacturing. Tim regularly contributes to the SANS Penetration Testing Blog (pen-testing.sans.org/blog) and the Command Line Kung Fu Blog (blog.commandlinekungfu.com). He is also project lead for the Laudanum Project, a collection of injectable scripts designed to be used in penetration testing. Currently Tim is a certified instructor for the SANS Institute. @timmedin

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 in CyberCity exercises 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.

You Will Learn How To:

- Analyze cyber infrastructures that control and impact kinetic infrastructures.
- Manipulate a variety of key industrial protocols, including Modbus, CIP, DNP3, Profinet, and other SCADA-related protocols.
- Rapidly prototype computer attack tools against specific vulnerabilities
- Discover security flaws in a variety of SCADA and Industrial Control Systems and thwart attacks against them.
- Conduct penetration tests and assessments associated with kinetic infrastructures.

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.

SEC573
Python for Penetration Testers

Hands-On | Five Days | Wed, Feb 17 - Sun, Feb 21 | Laptop Required | 30 CPEs

Your target has been well hardened. So far, your every attempt to compromise their network has failed. You did find evidence of vulnerability, a break in their defensive posture. Unfortunately, all of your tools have failed to successfully exploit it. Your employers demand results. You want to model the actions of an advanced adversary and take advantage of that discovered flaw your tools can't seem to address. What do you do when off-the-shelf tools fall short? You write your own tool!

SEC573: Python for Penetration Testers will teach you the skills needed not only to tweak or customize tools, but to even develop your own tools from scratch. The course is designed to meet you at your current skill level and appeal to a wide variety of backgrounds. Whether you have absolutely no coding experience or are a skilled Python developer looking to apply your coding skills to penetration testing, this course has something for you.

You cannot become a world-class tool builder by merely listening to lectures, so this course is chock full of hands-on labs. Every day we will teach you the skills you need to develop serious Python programs and show you how to apply those skills in penetration testing engagements.

The course begins with an introduction to SANS pyWars, which is a four-day Capture-the-Flag competition that runs parallel to the course material. It will challenge your existing programming skills and help you develop new skills at your own pace. Experienced programmers can quickly progress to more advanced concepts while novice programmers spend time building a strong foundation.

Who Should Attend

- Security professionals who want to learn how to develop Python applications
- Penetration testers who want to move from being a consumer of security tools to being a creator and customizer of security tools
- Technologists who need custom tools to test their infrastructure and want to create those tools themselves

INSTRUCTOR

Mark Baggett

Mark Baggett is the owner of Indepth Defense, an independent consulting firm that offers incident response and penetration testing services. Mark has more than 28 years of commercial and government experience ranging from Software Developer to Chief Information Security Officer. Mark is a Senior Instructor for The SANS Institute and the author of the Python for Penetration testers course (SEC573). Mark has a Master's Degree in Information Security Engineering and many industry certifications including being 15th person in the world to receive the prestigious GIAC Security Expert certification (GSE). Mark is very active in the information security community. Mark is the founding president of The Greater Augusta ISSA (Information Systems Security Association) chapter which has been extremely successful in bringing networking and educational opportunities to Augusta Information Technology workers. Since January 2011, Mark has served as the Technical Advisor to the DoD for SANS where he assists various government organizations in the development of information security capabilities. @MarkBaggett

HOSTED

Assessing and Exploiting Control Systems

Hands-On | Six Days | Tue, Feb 16 - Sun, Feb 21 | Laptop Required | 36 CPEs

This is not your traditional SCADA security course! This course teaches hands-on penetration testing techniques used to test embedded electronic field devices, network protocols, RF communications, and controlling servers of ICS and Smart Grid systems like PLCs, RTUs, smart meters, Home Area Networks (HAN), smart appliances, SCADA, substation automation, and synchrophasors. The course is structured around the formal penetration testing methodology created by the National Energy Sector Cybersecurity Organization Resource (NESCOR), a U.S. Department of Energy project. Using this methodology and SamuraiSTFU (Security Testing Framework for Utilities), an open-source Linux distribution for pentesting energy sector systems and other critical infrastructure, we'll perform hands-on penetration testing tasks on embedded electronic field devices, their RF communications, and the myriad of user interfaces used throughout smart grid systems. We will 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.

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.

INSTRUCTOR

Don Weber

Don Weber is a Senior Security Analyst with InGuardians. He has devoted himself to the field of information security since 2002. His most recent experiences include providing penetration assessment, architecture review, detailed hardware security assessment, wireless and radio implementation analysis, and incident response management for a wide range of industries including those in the financial, retail, and energy markets. Don's Smart Grid experience includes end-to-end AMI assessments for several energy-related clients and he has provided guidance on several Smart Grid-related standards committees and during Smart Grid conferences.

HOSTED

Critical Infrastructure and Control System Cybersecurity

Hands-On | Five Days | Wed, Feb 17 - Sun, Feb 21 | Laptop Required | 30 CPEs

This course 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.

- Hands-on environment (PLC, HMI, Network Communications, Backtrack)
- Operational, Cyber and Physical Protective Solutions
- Kits provided and used by pods of two attendees (Laptop, Customized I/O Trainer, PLC, HMI, communications infrastructure, CYBATIFIED Backtrack)

INSTRUCTOR

Matthew Luallen

Matthew Luallen is a well-respected information professional, researcher, instructor, and author. He 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.

MGT433

Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program

Hands-On | Two Days | Sat, Feb 20 - Sun, Feb 21 | Laptop Required | 12 CPEs

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their employees and staff. As a result, people, not technology, have become their weakest link in cybersecurity. The most effective way to secure the human element is to establish a high-impact security awareness program that goes beyond just compliance and changes behaviors. This intense two-day course will teach you the key concepts and skills needed to build, maintain and measure just such a program. All course content is based on lessons learned from hundreds of security awareness programs from around the world. You will learn not only from your instructor, but from extensive interaction with your peers, as well. Please bring example materials from your security awareness program that you can show and share with other students during the course.

Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you can implement as soon as you return to your organization.

INSTRUCTOR

Lance Spitzner

Lance Spitzner is an internationally recognized leader in the field of cyber threat research and security training and awareness. He has helped develop and implement numerous multi-cultural security awareness programs around the world for organizations as small as 50 employees and as large as 100,000. He invented and developed the concept of honeynets, is the author of several books, and has published over 30 security whitepapers. @lspitzner

BONUS SESSIONS – EVENING TALKS

Don't miss out on the team-based game simulators for both business and risk decision-makers, as well as other simulation-based environments for technical hands-on interaction. These evening events will educate community members on ICS security while providing plenty of opportunities to connect with your peers.

KIPS: Kaspersky Industrial Protection Simulation

The Kaspersky Industrial Protection Simulation (KIPS) is a "Security Monopoly" game for maximizing enterprise revenue while building an ICS security capability. It features a simulated water utility trying to accomplish its mission to produce and sell water to the community, while dealing with and resolving unexpected cyber events. Participants will form teams that will run the same water utility trying to outperform others. Every response a team makes will have a knock-on effect on the running of its plant, so participants need to analyze data and make decisions despite uncertain information and limited resources. Sounds like real life? That's the point.

KASPERSKY lab

WOPR: Shall We Play a Game?

This year we are offering a speed dating meets charades style challenge. The SANS ICS team working with Cybati will provide timed sessions allowing participants a 15 minute session to connect to an unknown device contained in a protective case and interact with it through multiple communication channels for 15 minutes. After 15 minutes of investigating the device the participant will be allowed to enter a guess identifying what device is contained in the box. Participants will have five different device opportunities to interact with if they want to attempt every device and ICS challenge points will be granted based on correct answers.

CYBATI

ICS Wall

The ICS Wall is an interactive display that allows people to interact with real control system devices in a closed environment. Individuals are encouraged to bring their own computer, connect to the networks, and explore firsthand how these systems operate. The wall has hardware from various major manufactures such as Phoenix Contact, Siemens, Allen Bradley and Tofino. Once connected, direct interaction with industrial protocols such as ProfiNet, Modbus, Ethernet IP, DNP3 and OPC is possible.

NetWars CyberCity

SANS NetWars CyberCity is designed to teach warriors and InfoSec pros that cyber action can have a 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 have an increasing need for skilled defenders of critical infrastructure. We engineered and built CyberCity to help organizations grow these capabilities in their teams. In this evening session, registered participants will have an opportunity to face a challenge exercise in CyberCity and compete to be the winning team on the CyberCity score board.

NETWARS CYBERCITY

SANS ICS Challenge (SIC)

Announcing the first ever SIC! This year we will host a contest that aims to educate community members on ICS and its security – all while competing for exciting prizes. The contest will kick off a few months prior to the ICS Summit and will be open and free for everyone. Register an account on the SIC website and download the challenge files. This presents contestants with an exciting opportunity to access ICS-related data and sharpen their skills. The contestants will compete for prizes including free summit passes, challenge coins, and a free on-demand ICS class.

SANS ICS SUMMIT CYBER SECURITY CHALLENGE

Monday, February 22	
8:45-9:00am	**Welcome & Opening Remarks**
9:00-9:45am	***Keynote*** ***Philip Quade**, Director, Cyber Task Force; Special Assistant to the Director NSA for Cyber, National Security Agency*
9:45-10:30am	***Industry 4.0*** Some are suggesting we are on the verge of the fourth industrial revolution as digital devices, big data, and connectedness transform manufacturing and industry. The yellow brick road takes us to a fully-integrated value chain, but there might be a few flying monkeys with teeth along the way. Whether you prefer Industrial Internet of Things, Industry 4.0, or M2M and the Internet of Everything, come hear about what is coming and where the potholes are making for a bumpy ride. Find out how to think about the next wave of automation, analytics, and optimization and what type of security approaches best fit these new business-changing models. How can we begin to build bridges into the future when our legacy ICS is still struggling to catch up? Ask our panel experts representing the views of suppliers, end-users, and industry experts. You don't need to bring your rose colored glasses; probably better to reach for your safety belt for this fast-paced, pull-no-punches look at the new revolution affecting all of us. MODERATOR: ***Mike Assante**, SANS Institute* PANELISTS: ***David Foose**, Ovation Product Security Manager, Emerson* ***Additional Panelists to be Announced***
10:30-11:00am	**Networking Break and Vendor Expo**
11:00-11:45am	**Vendor-Sponsored Solution Sessions**
11:45am-12:15pm	***What's the DFIRence for ICS?*** Digital Forensics and Incident Response for IT systems has been around quite a while, but what about ICS? This talk will explore the basics of DFIR for embedded devices such as PLCs, RTUs, and controllers. If these are compromised or even have a misoperation, what files, firmware, memory dumps, physical conditions, and other data can be analyzed in compromised embedded systems to determine the root cause. This talk will not cover Windows or *nix based devices such as HMIs or gateways. ***Chris Sistrunk**, Senior ICS Security Consultant, Mandiant*

12:15-1:30pm	**Lunch & Learn**
1:30-2:15pm	***ICS Sec for n00bz: An Introduction to ICS Defense by Defending the Death Star*** In a humorous and nerdy take on ICS security, Kara Turner shares basic ways to defend the Galactic Empire from Rebel attacks on the Empire's latest Death Star. Learn the common vulnerabilities in the Empire's defenses such as storm troopers leaving ports open so they can watch the latest pod races, belief that the Death Star is impenetrable because no one understands how it works, being terrified to tell the Emperor you need to shut things down and do an upgrade, and Darth Vader using his pet's name as a password. Learn best practices and policies to address these issues and more in a memorable way that easily translates to your own ICS environment. Rebel scum are attacking the systems that control AT-AT walker manufactories, droid foundries, and trying to destroy the Death Star. Learn how to protect the Empire's infrastructure. The Empire needs you! ***Kara Turner**, Critical Infrastructure Threat Analyst, iSIGHT Partners*
2:15-3:00pm	***Logging and Monitoring for Distributed Control Systems*** It has long been accepted that security monitoring associated with Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) networks is operationally and administratively different from traditional information technology (IT) business environments. The proliferation of smart devices, extended networks, geographically dispersed assets, and enforceable regulatory standards increases the complexity of logging and monitoring for these systems. This session will provide a perspective on the adoption of automation tools and maturity of technology for logging and monitoring. The key takeaways will include best practices from advocating a leading utility on the design, configuration and implementation of this capability. ***Josh Axelrod**, Cybersecurity Leader – Power & Utilities, EY* ***Jodirah Green**, Manager of Generation, NERC CIP Compliance, Duke Energy*
3:00-3:30pm	**Networking Break and Vendor Expo**
3:30-4:30pm	***Cyber-Physical ICS Lessons from Nuclear*** This session features live demonstrations using man-in-the-middle cyber penetrations to spoof operators through playback attacks, while at the same time manipulating both systems to gain access and damage equipment. We'll demonstrate the very real potential of cyber attackers to manipulate and compromise ICS and physical systems and drive them to failure. Demo 1 will show the exploitation of two systems. The first will be a PPS system that consists of an entry controlled card reader, door alarms, and a CCTV monitoring system. The threat actors will gain access to the system, spoofing the door alarms and the CCTV in order to remain undetected; then they'll manipulate the card reader to penetrate the facility. Once on the inside, the physical perpetrators will plant malware and a secondary communication device connected to a CDA within the I&C system to allow access to external threat actors to execute an exploitation of a secondary coolant loop within the nuclear reactor process. Demo 2 includes a closed loop cooling process consisting of a controller, pumps, values, sensors, clear tubing (visualization), and an operator HMI for monitoring the I&C nuclear reactors cooling process. Through malware and a secondary communication device installed in Demo 1, the threat actors will gain access to the I&C system, monitor and analyze the traffic, and develop exploits. When the exploits are ready, the attackers will spoof the operator console to reflect normal operations, while at the same time manipulate the values and pumps. This is a wear attack, with the potential to cause a water hammer that would trigger a full safety shutdown. ***Andy Bochman**, Senior Cyber and Energy Security Strategist, Idaho National Lab's National and Homeland Security Directorate* ***Trent Nelson**, Cyber Security Assessment Lead, Idaho National Lab* ***Joseph Price**, Cyber Security Research & Development, Idaho National Lab*

4:30-5:15pm	***Mobile Apps, IoT, and Terrifying Grown Adults*** Somewhere along the line, product developers thought it would be a good idea to connect things like pet food dispensers and automated plant-watering devices to the Internet and smartphone apps. What could go wrong? Recently, Tim purchased some IoT devices that are controlled by mobile apps. The goal was to make the devices do things that the app doesn't normally allow you to do, or change the way the device works. In this talk, Tim will demonstrate some mobile application analysis and hacking techniques that he employed to hack the devices – the same practical techniques used in many mobile application assessments. Caution: the results may terrify small children and Summit audiences alike. ***Tim Medin**, Senior Technical Analyst, CounterHack*

Tuesday, February 23

8:45-9:00am	**Opening Remarks – *Ernie Rakaczky ICS Security Lifetime Achievement Award & Scholarship Program*** Ernie Rakaczky, Jr. was best known by his peers as an advocate with a passion for progress, innovation, and investment in the ICS field. He became a strong supporter of U.S. and Canadian efforts to enhance the security of ICS on an international scale, and an activist to bridge the gap of IT and OT through education and awareness of proper automation systems for security professionals. Ernie served on the GICSP steering committee, where his expertise and insight directed the formulation of the certification. Those who worked alongside Ernie will remember him for his dedication and contributions in shaping the ICS security field and his optimistic outlook on the potential to make a difference. Learn how the legacy of this leader will be honored through the Ernie Rakaczky ICS Security Lifetime Achievement Award & Scholarship Program. ***Mike Assante**, SANS Institute*
9:00-9:45am	***Keynote – TBD***
9:45-10:30am	***Snap, Crackle, and Pop – What Does it Take to Cause Damage?*** MODERATOR: ***Mike Assante**, SANS Institute* PANELISTS: ***Joseph Price,** Cyber Security Research & Development, Idaho National Lab* ***Robert M. Lee**, SANS Institute* ***Additional Panelists to be Named***
10:30-11:00am	**Networking Break and Vendor Expo**
11:00-11:45am	***Car Wars Episode I: Hacker Menace*** It is a time of relative peace in the Republic. Auto manufacturers have provided reliable automobiles to a large portion of the population, governments, and militaries throughout the known world. Convenience and safety have become a common expectation in life. Little does the Auto Alliance know that opportunistic evil awaits. While preparing for the ultimate auto-driving experience, dark plans have been laid to leverage this new power for death and destruction, and the changing of the universe forever. ***Matt Carpenter**, Principal Security Researcher, Grimm*
11:45am-12:15pm	***Connectivity Surprise Factor: What's in Your ICS?*** Every day, Industrial Control Systems perform tirelessly —safely and efficiently producing and delivering power, clean water, moving people and producing most all of the varied products and services on which the world depends. While communications is at the heart of these critical systems, operational challenges continue to be amplified. Technology convergence is often unknowingly blending industrial control, commercial and consumer products and technologies into common shared infrastructure leading to new risks and greater exposure to threats. In this session, learn about the "Connectivity-Surprise Factor" and the benefits that can be gained by performing comprehensive and real-time network asset-inventories, tracing data flows, base-lining normal and expected communication patterns and using passive industrial network anomaly detection technology to help improve and protect a control system's operational resiliency throughout its lifecycle. ***Doug Wylie**, CISSP, VP – Strategy, NexDefense, Inc.*

12:15-1:30pm	**Lunch & Learn**
1:30-2:15pm	***No Stone Unturned*** In the world of industrial safety we're pretty darn good at finding root cause and taking action to avoid similar incidents. The Chemical Safety Board and Transportation Safety Board are just two examples. Companies in the aftermath of a cyber incident often leave no stone unturned in seeking to understand their real exposure and what to do about it. In this presentation three incident investigations are distilled in the context of the industrial software support provider. ***Bryan Owen**, Cyber Security Manager, OSIsoft*
2:15-3:00pm	***The ICS Cyber Kill Chain: Active Defense Edition*** The ICS Cyber Kill Chain details the attack steps an adversary has to take to complete a high confidence process or equipment attack. Understanding the kill chain allows defenders to analyze and learn from advanced threats. It also highlights defender strengths. In this presentation, the ICS Cyber Kill Chain will be used to analyze a number of high-profile threats and showcase how defenders can take an active defense approach to protecting their ICS from them. Defense is doable – learn how in this presentation. ***Robert M. Lee**, SANS Institute*
3:00-3:30pm	***Building Skills with Challenges and Training*** The ICS Cyber Security Challenge is more than just an excuse to break stuff and compete for bragging rights. Challenges are a fun but effective way to build the skills you need to defend your systems and advance your career. Hear about the lessons learned so far from the ICS Cyber Security Challenge, and get a sneak peek at the next step in the SANS ICS curriculum, ICS456. ***Tim Conway**, SANS Institute* ***Robert M. Lee**, SANS Institute*
3:30-3:50pm	**Networking Break and Vendor Expo**
3:50-4:30pm	***Why 90%+ of the ICS Vulnerabilities Don't Increase Risk – And How to Identify the Important Ones That Do*** The most frequent and hyped ICS security news items involve newly discovered vulnerabilities in ICS software and hardware. However over 90% of these vulnerabilities, whether patched or left unpatched, have only a minor impact on risk to the ICS. In this session Dale will use the ICS-CERT reported vulnerabilities and provide a risk taxonomy of ICS vulnerabilities with 2015 statistics and specific examples for each category. Attendees will learn how to identify and avoid spending time and money inefficiently to address vulnerabilities that do not affect ICS risk. The second part of the session will provide a simple method to identify the small percentage of vulnerabilities that do affect ICS risks. This is where owner/operators should place their security patching efforts. ***Dale Peterson**, CEO of Digital Bond, Inc.*
4:30-5:15pm	***Lessons Learned Integrating Security Products into ICS*** This presentation will provide lessons learned dealing with traditional IT Security firms and products in the long lifespan ICS environment. It will cover various red flags and challenges that may not be apparent when first approaching the selection, deployment and ongoing upkeep of software and hardware solutions. It will also offer some suggestions on relaying security wants or requirements to the DCS vendor so that they can properly answer or scope the security solutions you require. ***David Foose**, Ovation Product Security Manager, Emerson*
5:15pm	**Closing Remarks** ***Mike Assante**, SANS Institute*

OTHER SANS TRAINING EVENTS

SANS Las Vegas 2016
Las Vegas, NV | January 9-14

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

SANS Cyber Threat Intelligence SUMMIT & TRAINING
Alexandria, VA | February 3-10

SANS Scottsdale 2016
Scottsdale, AZ | February 8-13

SANS McLean 2016
McLean, VA | February 15-20

SANS Anaheim 2016
Anaheim, CA | February 22-27

SANS Philadelphia 2016
Philadelphia, PA | February 29 - March 5

SANS 2016
Orlando, FL | March 12-21

SANS Reston 2016
Reston, VA | April 4-9

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events sans.org/security-training/by-location/all
Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers

Community SANS sans.org/community
Live Training in Your Local Region with Smaller Class Sizes

Private Training sans.org/private-training
Live Onsite Training at Your Office Location. Both In-Person and Online Options Available

Mentor sans.org/mentor
Live Multi-Week Training with a Mentor

Summit sans.org/summit
Live IT Security Summits and Training

ONLINE TRAINING

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

vLive sans.org/vlive
Online, Evening Courses with SANS' Top Instructors

Simulcast sans.org/simulcast
Attend a SANS Training Event without Leaving Home

OnDemand Bundles sans.org/ondemand/bundles
Extend Your Training with an OnDemand Bundle Including Four Months of E-learning

ICS SECURITY SUMMIT

Hotel Information

Training Campus

DoubleTree by Hilton

5780 Major Boulevard
Orlando, FL 32819
407.351.1000

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

At the DoubleTree by Hilton at the Entrance to Universal Orlando, the magic begins the moment you step through the doors. Smiles grow wider and business gets smarter. With its captivating Orlando, Florida location, our 100% non-smoking hotel and convention center charms business travelers and vacationing families with a unique combination of high-speed hospitality and exceptional home-style service.

Special Hotel Rates Available

A special discounted rate of $129.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate [1-800-222-TREE (8733)]. These rates include high-speed Internet in your room and are only available through Jan. 22, 2016.

Top 3 reasons to stay at the DoubleTree by Hilton at the Entrance to Universal Orlando

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
2. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
3. You gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the conference

ICS SECURITY SUMMIT

Registration Information

We recommend you register early to ensure you get your first choice of courses.

Register online at sans.org/event/ics-security-summit-2016/courses

Select your course or courses and indicate whether you plan to test for GIAC certification.

If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Use code **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**1-6-16**	**$400.00**	**1-13-16**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)

10% discount if 10 or more people from the same organization register at the same time

5% discount if 5-9 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by January 27, 2016 – processing fees may apply.

SANS Voucher Credit Program

Expand your training budget! Extend your fiscal year. The SANS Voucher Discount Program pays you credits and delivers flexibility.
sans.org/vouchers

The ICS Security Summit is the premier event for ICS cybersecurity practitioners and managers. You will:

- Understand how ICS systems are being targeted
- Learn how to safeguard ICS against the new threat matrix
- Network with fellow practitioners to share skills and acquire new ones
- Explore how to combine cyber-informed engineering with cybersecurity for ICS success
- Discover the best practices for teaching operators cybersecurity awareness
- Test and expand ICS security knowledge through hands-on challenges

Follow us at @SANSICS and join the conversation #ICSSummit to hear the latest news.