SANS ICS SECURITY

ORLANDO

SUMMIT & TRAINING

SUMMIT:
March 20-21

TRAINING:
March 22-27

www.sans.org/ICS-Summit

SANS ICS SECURITY

ORLANDO

SUMMIT & TRAINING

SUMMIT: **March 20-21**

TRAINING: **March 22-27**

The 12th Annual Industrial Control Systems Security Summit & Training is the event to attend in 2017 to better understand targeted ICS campaigns and how to protect your organization.

Top three reasons to attend the SANS ICS Security Summit & Training:

1. **Two days of in-depth Summit presentations, panel discussions, and live demonstrations** Learn the latest defense techniques and strategies from industry leaders and in-the-field practitioners.
2. **World-class information security training** Following the Summit, choose from seven courses taught by real-world security practitioners.
3. **Community** Connect with fellow attendees and industry leaders for the brand-new ICS NetWars Tournament, evening receptions, and other exclusive networking opportunities.

SAVE $200

when you register and pay for the Summit by Feb 1st – Use code **EarlyBird17**

"This summit was extremely beneficial because it gives insight into what challenges my peers are facing and how they are addressing them. It is a forum for sharing information and cultivating new ideas."

-Jeff Jones, Exelon Corporation

REGISTER TODAY AT **www.sans.org/ICS-Summit**

SANS ICS Security Summit & Training Courses

March 22-27, 2017

ICS410: **ICS/SCADA Security Essentials**
Instructor: Justin Searle | Certification: GICSP

ICS456: **Essentials for NERC Critical Infrastructure Protection**
Instructor: Tim Conway

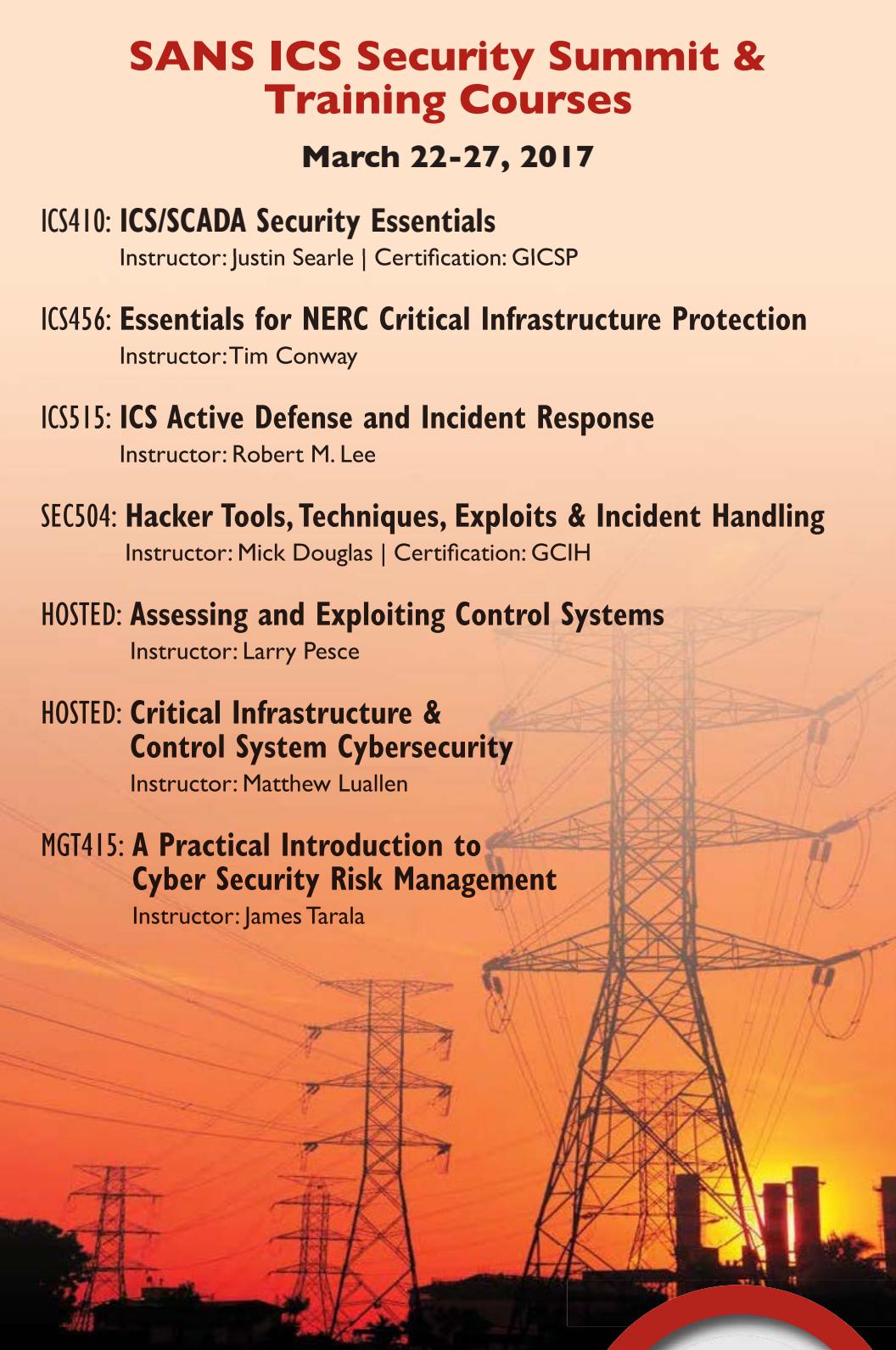
ICS515: **ICS Active Defense and Incident Response**
Instructor: Robert M. Lee

SEC504: **Hacker Tools, Techniques, Exploits & Incident Handling**
Instructor: Mick Douglas | Certification: GCIH

HOSTED: **Assessing and Exploiting Control Systems**
Instructor: Larry Pesce

HOSTED: **Critical Infrastructure & Control System Cybersecurity**
Instructor: Matthew Luallen

MGT415: **A Practical Introduction to Cyber Security Risk Management**
Instructor: James Tarala



@SANSICS
#ICSSummit

SAVE $400
when you register for the ICS Summit and a 5- or 6-day course!

REGISTER TODAY AT **www.sans.org/ICS-Summit**

ICS SECURITY SUMMIT PRESENTATIONS

KEYNOTE PRESENTATION

Exploring the Unknown ICS Threat Landscape

Robert M. Lee
CEO, Dragos; Certified Instructor, SANS Institute

ICS (in)security is hiding in plain sight. This presentation will be our first public discussion of unique research on industrial control system software, malware, and the consequences of poor operations security. Our premise for this project is the belief that there is a wealth of information surrounding Industrial Control Systems that is unrecognized by the traditional IT cybersecurity industry. We will walk through our methodology, show real-world findings and conclusions of what this means in our space.

Ben Miller
Director of Threat Operations, Dragos

FEATURED LIVE DEMONSTRATION

I Can See the Ukraine from Orlando!

Tim Conway
Technical Director – ICS & SCADA Programs, SANS Institute

Hot off a multi-city North American roadshow and rolling straight into Orlando, we will host a live demonstration of various attack concepts utilized to manipulate field control environments. This simulation will demonstrate technology misuse and trusted path manipulation techniques, as well as key issues for defenders to consider as they return to work and explore options for protecting their systems.

Andy Bochman
Idaho National Lab, Senior Cyber and Energy Security Strategist

FEATURED PANEL DISCUSSION

If We're Doing So Well, Why Are We Still Doing So Poorly?

Awareness campaigns, frameworks, community, public-private partnerships. We should be patting ourselves on the back for all the hard work we've been doing to advance the state of cybersecurity. Right? But...wait! Why is ransomware flourishing? Why are IoT devices the scourge of security? How come the Internet seems to be getting more dangerous?

MODERATOR
Mike Assante
Industrials & Infrastructure Practice, ICS/SCADA Lead, SANS Institute

PANELIST
Markus Braendle
Group Head of Cybersecurity, ABB

PANELIST
Marty Edwards
Director of the Industrial Control Systems Cyber Emergency Response Team, U.S. Dept. of Homeland Security

PANELIST
Tyler Williams
Global Technology Leader, Shell

Keeping Up with the Cyber-Joneses

David Foose
Manager of Ovation Security Products, Emerson

Over the last eight years, our team has worked with multiple groups throughout the world to achieve an acceptably secure state. This presentation will use anonymous anecdotal examples to show that all organizations face similar challenges and, while they often approach them in completely different ways, they eventually come to a similar conclusion. Let's talk about what these general areas of need are, how they have been approached (both good and bad), and where improvement can still be made to work towards a common goal of a stable and defensible system.

The 1990s Called; They Want Their Technology Back: How ICS Is Still Using Paging Technologies

Stephen Hilt
Sr. Threat Researcher, Trend Micro

Pagers are prevalent even to this day in many sectors around the world. The prevalence of software-defined radios with low price points give even the most novice attacker the ability to sniff and decode messages sent to pagers. We will cover the basics of pagers, the protocols that are used, the systems that are currently using them, and the analysis of some of the pagers that have been observed by researchers at Trend Micro during the project. This talk will focus only on the pager messages used within ICS fields and messages that have been observed that are relevant to the audience at SANS ICS.

I'll Let Myself In: How Threats Are Slipping in the Actual Back Door While You're Looking at Logs

Deviant Ollam
Security Auditor & Pen Test Consultant, The CORE Group

Many organizations are accustomed to being scared at the results of their network scans and digital penetration tests, but seldom do these tests yield outright "surprise" across an entire enterprise. Some servers are unpatched, some software is vulnerable, and networks are often not properly segmented. No huge shocks there. As head of a Physical Penetration Team, however, my deliverable day tends to be quite different. With faces agog, executives routinely watch me describe (or show video) of their doors and cabinets popping open in seconds. This presentation will highlight some of the most exciting and shocking methods by which my team and I routinely let ourselves in on physical jobs.

Disassembly and Hacking of Firmware Where You Least Expect It: In Your Tools

Monta Elkins
Hacker-in-Chief, FoxGuard Solution

This live hacking demonstration will investigate vulnerability and capability assessment of firmware attacks; physical ramifications of tool attacks; instances where "less security" is better; and security tips for firmware. You'll leave with a better understanding of the location and use of firmware in unexpected places and gain insight into the attack methodologies for and security of devices with firmware, so you can better protect yourself.

ICS SECURITY SUMMIT PRESENTATIONS

From Research to Reality: Real-World Applications of Threat and Vulnerability Data Analysis

Clint Bodungen
Senior Researcher, Critical Infrastructure Threat Analysis, Kaspersky Lab, North America

Vladimir Dashchenko
Senior Research Developer, Critical Infrastructure Threat Analysis, Kaspersky Lab, North America

In October 2016, Kaspersky Lab launched the first non-government run Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) – a non-commercial project focused on collecting and sharing the latest ICS threat vectors, incident investigation, vulnerability research, and analysis from Kaspersky researchers as well as external sources. This talk will highlight major research, case studies, findings, and analysis covering the following topics:

1) ICS Threat intelligence: attacks and threats
2) Vulnerability research: statistics and main vulnerability vectors
3) Threat analysis: what are the major threats in ICS field – how the threats changed
4) Modern attack vectors on ICS

IT and OT Convergence – It's a Thing for Attackers, Too!

Eric Cornelius
Director of Critical Infrastructure and ICS, Cylance; Certified Instructor, SANS Institute

This live demo will welcome the audience into the minds of a simulated adversary group tasked with creating a destructive critical infrastructure attack. Successful attacks targeting complex environments require diverse adversary teams capable of developing a sound concept of operations and executing that plan across diverse IT- and OT-supported environments. This talk will feature an on-stage demo of open-source facility recon and targeting, leveraging ICS field device attack vectors, process control manipulation, zero-day fun time, and firmware manipulation.

USACE Control System Cybersecurity Program: Processes and Lessons from the Corps

Phillip Copeland
Director, Critical Infrastructure Cyber Security, U.S. Army Corps of Engineers

Gregory Garcia
Chief Information Officer/G-6, U.S. Army Corps of Engineers

The global climate of cyber threats continually increases in intensity. The U.S. Army Corps of Engineers (USACE) has responded by launching an aggressive cybersecurity program for control systems spanning the entire system lifecycle. Starting with enterprise-wide inventory implementation and moving through system hardening to Authority To Operate issuance and continuous monitoring, USACE has developed a comprehensive control system cybersecurity methodology based on real cyber risk that is being incorporated in other cybersecurity programs across the Department of Defense and other branches of the military.

Top-Down, Purpose-Based Cybersecurity

David E. Stone
Colonel, U.S. Air Force, Air Force Cyber College

Cyber attacks that cause physical damage or affect physical processes are no longer limited to theory or speculation. Innovations within the Departments of Defense and Energy reveal a commonality in a top-down, purpose-based approach to preventing unacceptable losses and significant consequences resulting from malicious cyber activity. Such an approach allows an organization to apply limited resources to critical, key elements of its operation without having the need to cover the entire waterfront.

Controls, Captains, and Careers

Mike Assante
Industrials & Infrastructure Practice, ICS/SCADA Lead, SANS Institute

The gloves are coming off, as we put tough questions to this panel of ICS pros. How are we really doing? How can we build teams with the right skills to make an impact on security? What controls are successful IS practitioners embracing, and what's a waste of time?

Incentivizing ICS Security: The Case for Cyber Insurance

Jason Christopher
CTO, Axio

Over the past couple of decades, the cybersecurity field has had difficulty speaking to executives and boards about risk. Our community often qualifies cyber risk as "high, medium, and low" or "red, yellow, and green." When compared to more mature areas of traditional risk management, which feature quantifiable metrics and graphs as complex as the Dow Jones Industrial Average, our security professionals may look like they're carrying crayons to a math test. Fortunately, in the past few years, we've seen a jump in maturity when discussing cyber risk management. By applying leading and lagging metrics, quantifying the impacts due to cyber risk beyond "criticality," and branching into data analytics, many information security professionals have found new ways to communicate cyber risk in meaningful ways for executives and boards. This presentation will highlight the new metrics and methodologies used for quantifying cyber risk and cyber program improvements in critical infrastructure. Recognizing the many different drivers for maturing a cyber risk management program, we'll also discuss the internal and external partners for these sorts of program improvements, and why security professionals should become very good friends with the insurance industry.

How the Midcontinent Independent System Operator (MISO) moved to Active Defense and Advanced in the Hunting Maturity Model (HMM)

Jamie Buening
Information Security Analyst, Midcontinent Independent System Operator

Industry is shifting away from traditional cybersecurity approaches. We commonly hear that preventative security solutions are lagging and that we should assume we are already breached. MISO considered the available information and agreed that a different approach to security was needed. Steps were taken in late 2014 to prepare for new cybersecurity capabilities. Those activities have enabled MISO to move towards Active Defense, including the ability to hunt for anomalies and indicators of compromise across its infrastructure. This presentation will cover how MISO was able to implement and use these new proactive capabilities. Examples will show hunting activities that MISO is performing. The activities will also be mapped to where they fit within the Hunting Maturity Model (HMM). The presentation will also demonstrate what Cyber Hunting means at a practical level. Much of what has been written about Cyber Hunting leaves an abstract and cloudy perception about the topic. Three specific examples will be used to show activities at HMM levels 0, 1, and 2. Outcomes of the examples will include the lessons learned and the value that the activities brought to MISO.

"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

ICS410:
ICS/SCADA Security Essentials

SANS

Five-Day Program
Wed, Mar 22 - Sun, Mar 26
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Justin Searle

www.giac.org/gicsp

SANS Technology Institute
www.sans.edu

Bundle OnDemand
with this course
www.sans.org/ondemand

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

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

The course will provide you with:

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

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

"This course was a great introduction into the ICS landscape and associated security concerns. The ICS material presented will provide immediate value relative to helping secure my company." -Mike Poulos, Coca-Cola Enterprises

Given 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.

Justin Searle *SANS Principal Instructor*

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). Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences. In addition to electric power industry conferences, Justin frequently presents at top international security conferences such as Black Hat, DEFCON, OWASP, Nullcon, and AusCERT. He 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. Justin 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

ICS456:

Essentials for NERC Critical Infrastructure Protection

NEW

SANS

Five-Day Program
Wed, Mar 22 - Sun, Mar 26
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Tim Conway

ICS456: Essentials for NERC Critical Infrastructure Protection is a five-day course that empowers students with knowledge of the "what" and the "how" of the Version 5/6 standards. The course addresses the role of the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), and the regional entities. It provides multiple approaches to identifying and categorizing BES Cyber Systems and helps asset owners determine the specific implementations applicable to the requirements. Additionally, the course covers implementation strategies for the Version 5/6 standards with a balanced practitioner approach to both cybersecurity benefits and regulatory compliance.

This course also contains 24 hands-on labs ranging from securing workstations to digital forensics and lock picking.

Who Should Attend

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

"This is best-in-class NERC CIP training. The courseware provides valuable compliance approaches and software tools for peer collaboration to build consent on implementation."

-Jeff Mantong, WAPA

Author Statement

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

"Best CIP training I've ever had in all my years of the CIP program."

-Michael Veillon, Cleco

Tim Conway *SANS Instructor*

Tim 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 previously served as the Director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO), where he was responsible for Operations Technology, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric. Tim was also an EMS Computer Systems Engineer at NIPSCO for eight years, with responsibility over the control system servers and the supporting network infrastructure. He was the chair of the RFC CIPC, and is the current chair of the NERC CIP Interpretation Drafting Team, member of the NESCO advisory board, chair of the NERC CIPC GridEx Working Group, and chair of the NBISE Smart Grid Cyber Security panel.

ICS515:
ICS Active Defense and Incident Response

SANS

Five-Day Program
Wed, Mar 22 - Sun, Mar 26
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Robert M. Lee

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

"This course provides contemporary ICS security perspective on active defense and response, and a high value student interaction and best practice sharing. This was an enriching learning experience."
-FRED H., U.S. NAVY

"Robert did a great job, very personable, and easy to talk with in class and after class. The labs were awesome, and I learned more by encountering the problem and working through it."
-ROB CANTU, DOE

ICS515: ICS Active Defense and Incident Response will help you deconstruct cyber attacks on industrial control systems (ICS), leverage an active defense to identify and counter threats in your ICS, and use incident response procedures to maintain the safety and reliability of operations. This course will empower students to understand their networked 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 internal to the network is known as active defense. An active defense is the approach needed to 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 with the ability to deconstruct targeted ICS attacks and fight these adversaries and others. The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of leveraging active defense concepts such as using threat intelligence, performing network security monitoring, and utilizing malware analysis and incident response to ensure the safety and reliability of operations. The strategy and technical skills presented in this course serve as a basis for ICS organizations looking to show that defense is do-able.

Who Should Attend

- ICS incident response team leads and members
- ICS and operations technology security personnel
- IT security professionals
- Security Operations Center (SOC) team leads and analysts
- ICS red team and penetration testers
- Active defenders

You Will Be Able To

- Examine ICS networks and identify the assets and their data flows in order to understand the network baseline information needed to identify advanced threats
- Use active defense concepts such as threat intelligence analysis, network security monitoring, malware analysis, and incident response to safeguard the ICS
- Build your own Programmable Logic Controller using a CYBATIworks Kit and keep it after the class ends
- Gain hands-on experience with samples of Havex, BlackEnergy2, and Stuxnet through engaging labs while de-constructing these threats and others
- Leverage technical tools such as Shodan, Security Onion, TCPDump, NetworkMiner, Foremost, Wireshark, Snort, Bro, SGUIL, ELSA, Volatility, Redline, FTK Imager, PDF analyzers, malware sandboxes, and more
- Create indicators of compromise (IOCs) in OpenIOC and YARA while understanding sharing standards such as STIX and TAXII
- Take advantage of models such as the Sliding Scale of Cybersecurity, the Active Cyber Defense Cycle, and the ICS Cyber Kill Chain to extract information from threats and use it to encourage the long-term success of ICS network security

Robert M. Lee *SANS Certified Instructor*

Robert M. Lee is the CEO and founder of 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. Robert is also a non-resident National Cyber Security Fellow at New America focusing on policy issues relating to the cybersecurity of critical infrastructure and a PhD candidate at Kings College London. For his research and focus areas, he was named one of Passcode's Influencers and awarded EnergySec's 2015 Cyber Security Professional of the Year. Robert obtained his start in cybersecurity in the U.S. Air Force, where he served as a Cyber Warfare Operations Officer. He has performed defense, intelligence, and attack missions in various government organizations, including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles in publications such as *Control Engineering* and the *Christian Science Monitor's Passcode* and speaks at conferences around the world. He is also the author of *SCADA and Me* and the weekly web-comic (www.LittleBobbyComic.com) @RobertMLee

SEC504:

Hacker Tools, Techniques, Exploits, and Incident Handling

SANS

Six-Day Program
Wed, Mar 22 - Mon, Mar 27
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
Instructor: Mick Douglas

www.giac.org/gcih

www.sans.edu

www.sans.org/cyber-guardian

www.sans.org/8140

BUNDLE ONDEMAND
WITH THIS COURSE
www.sans.org/ondemand

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization has an Internet connection or one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. **As defenders, it is essential we understand these hacking tools and techniques.**

Who Should Attend

- Incident handlers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

"Great instruction! SEC504 covered topics very thoroughly and gave great examples."
-Kevin H., U.S. Department of Homeland Security

This course enables you to turn the tables on computer attackers by helping you to understand their tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare for, detect, and respond to attacks. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a **hands-on** workshop that focuses on scanning, exploiting, and defending systems. This will enable you to discover the holes in your system before the bad guys do!

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. **General security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.**

"This was a valuable course and will benefit me in the aspect of explaining the pieces attackers follow to gain access to system networks and the practices to mitigate these attacks." - Derek S., U.S. Air Force

Mick Douglas *SANS Instructor*

Even when his job title indicated otherwise, Mick Douglas has been doing information security work for over ten years. He received a bachelor's degree in Communications from the Ohio State University and holds the CISSP, GCIH, GPEN, GCUX, GWEB, and GSNA certifications. He currently works at Binary Defense Systems as the DFIR Practice Lead. He is always excited for the opportunity to share with others so they do not have to learn the hard way! Please join in; security professionals of all abilities will gain useful tools and skills that should make their jobs easier. When he's not "geeking out" you'll likely find him indulging in one of his numerous hobbies; photography, scuba diving, or hanging around in the great outdoors.

HOSTED:

Assessing and Exploiting Control Systems

NEW

SANS

Six-Day Program
Wed, Mar 22 - Mon, Mar 27
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Larry Pesce

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 additional inter-system communication, modern control systems bring a greater risk of compromise that vendors, asset owners/operators, and society in general must accept in order 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.

Topics:

- Introduction to the NESCOR methodology for penetration testing
- Architecture reviews of major ICS and smart grid systems and protocols
- Introduction to SamuraiSTFU (Security Testing Framework for Utilities)
- Performing traditional network pentests on control systems
- Types of ICS-user interfaces
- User interface mapping
- Vulnerability discovery
- Application exploitation
- Different levels of network communication penetration testing
- Serial communications
- Pentesting RF communications between master servers and field devices
- Pentesting TCP/IP-based ICS protocols
- Pentesting technician interfaces on ICS field and floor devices
- Analyzing field and floor device firmware
- Overview of pentesting field and floor-device-embedded circuits
- Analysis of embedded electronics in ICS field and floor devices
- Dumping data at rest on embedded circuits
- Bus Snooping on embedded circuits
- Analyzing data obtained from data dumping and bus snooping
- End-to-end analysis and reporting

Larry Pesce *SANS Certified Instructor*

Larry is a Senior Security Analyst with InGuardians after a long stint in security and disaster recovery in healthcare, performing penetration testing, wireless assessments, and hardware hacking. He also diverts a significant portion of his attention to co-hosting the PaulDotCom Security Weekly podcast and likes to tinker with all things electronic and wireless, much to the disappointment of his family, friends, warranties, and his second Leatherman Multi-tool. Larry co-authored Linksys WRT54G Ultimate Hacking and Using Wireshark and Ethereal from Syngress. Larry is an Extra Class Amateur Radio operator (KB1TNF) and enjoys developing hardware and real-world challenges for the Mid-Atlantic Collegiate Cyber Defense Challenge.
@haxorthematrix

HOSTED:

Critical Infrastructure and Control System Cybersecurity

SANS

Five-Day Program
Wed, Mar 22 - Sun, Mar 26
9:00am - 5:00pm
30 CPEs
Laptop Provided
Instructor: Matthew Luallen

This course is an intermediate to advanced course covering control system cybersecurity vulnerabilities, threats and mitigating controls. This 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.

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, as well as 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 active threats against our critical infrastructure control systems.

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.

Matthew Luallen *SANS Certified Instructor*

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 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.

MGT415:

A Practical Introduction to Cyber Security Risk Management

SANS

Two-Day Course
Wed, Mar 22 - Thu, Mar 23
9:00am - 5:00pm
12 CPEs
Laptop Required
Instructor: James Tarala

Hands-On Training

- Performing a Simple Risk Assessment
- Risk Assessment Case Study
- Formal Risk Assessment Tools
- Formal Risk Management Tools
- Log Parsing to Identify Risks
- Using a LiteGRC Risk Management Tool

"You come away with a framework for action that you can take back to help your organization deal with risk."

-James Voorhees, Sage Management

In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform risk management is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities that could exist, and simply not enough resources to create an impregnable security infrastructure. Therefore every organization, whether they do so in an organized manner or not, will make priority decisions on how best to defend their valuable data assets. Risk management should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

Who Should Attend

- Security engineers, compliance directors, managers, and auditors
- Auditors
- Directors of security compliance
- Information assurance managers
- System administrators

You Will Learn

- How to perform a risk management assessment step by step.
- How to map an organization's business requirements to implemented security controls.
- The elements of risk assessment and the data necessary for performing an effective risk assessment.
- What in-depth risk management models exist for implementing a deeper risk management program in their organization.

Course Author Statement

"Most every time we talk with an organization, whether that be a private company or a government agency, we meet people who want to use risk assessment as a tool, but are not actually using it as they could. No organization has enough resources to do everything they would like to defend themselves. At some point a priority decision has to be made. We either make those decisions individually based on whatever need seems to be the most pressing in from of us today, or we take a methodical approach, getting as much input from the business as possible. Risk management is the tool we have available for taking the methodical path.

This course has been written with practicality and usability in mind. Risk models and learning ALE to pass a certification test is fine. But to defend our systems, we need practical skills in risk assessment. This course will teach students the hands-on skills necessary to immediately start using risk assessment as a tool to defend their organization."

-James & Kelli Tarala

James Tarala *SANS Senior Instructor*

James Tarala is a principal consultant with Enclave Security and is based in Venice, Florida. He is a regular speaker with the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years developing large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them in their security management, operational practices, and regulatory compliance issues, and he often performs independent security audits and assists internal audit groups in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications. @isaudit

ICS NETWARS EXPERIENCE

NEW!

Test your knowledge and skills at

The Debut of ICS NetWars at ICS Security Summit 2017!

MONDAY, MARCH 20 | 6:30-9:30 PM

Join us for this exciting event to test your skills in a challenging and fun learning environment. Registration for ICS NetWars is **FREE OF CHARGE TO ALL STUDENTS AT SANS ICS SECURITY SUMMIT 2017**. External participants are welcome to join for an entry fee of $1,520.

Participants will work through various ICS security challenges and questions designed to test their experience and skills in a safe, controlled environment. ICS NetWars Experience provides an excellent forum for building your ICS security skills while having a little fun with fellow practitioners.

www.sans.org/ICS-Summit

EVENING BONUS SESSIONS

Enrich your SANS training experience!

Evening talks by our instructors and selected subject-matter experts help you broaden your knowledge, hear from the voices that matter in computer security, and get the most for your training dollar.

Summit Vendor Reception

Prior to ICS NetWars and the KIPS simulation, join us for a casual reception in the vendor expo area where you can enjoy drinks and appetizers while networking with leading security solution providers and your fellow Summit attendees and speakers. Take advantage of this opportunity not only to familiarize yourself with leading security solutions/products, but also to build your relationships within the ICS cybersecurity space.

ICS NetWars Experience

The brand-new SANS ICS NetWars Experience will debut at the 2017 SANS ICS Security Summit & Training! Participants will work through various ICS security challenges and questions designed to test their experience and skills in a safe, controlled environment. ICS NetWars Experience provides an excellent forum for building your ICS security skills while having a little fun with fellow practitioners.

KIPS: Kaspersky Industrial Protection Simulation

The SANS ICS team will be offering the Kaspersky Industrial Protection Simulation (KIPS) scenario on the evening of March 20th. This year's simulation will feature a challenging scenario that players will have to work through in teams. KIPS is essentially 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 addressing and resolving unexpected cyber events. Players will form teams that will run the same water utility trying to outperform the other teams. Every response a team makes will have an effect on the running of its plant, so participants need to analyze data and make decisions despite uncertain information and limited resources. Sound like real life? That's the point.

"A fun event – great opportunity to get new ideas, meet old friends, and make new ones!"

-Ernie Hayden, Securicon

Enhance Your Training Experience

Add an

OnDemand Bundle & GIAC Certification Attempt*

to your course within seven days of this event for just $689 each.

SPECIAL PRICING

Extend Your Training Experience with an OnDemand Bundle

- Four months of supplemental online review
- 24/7 online access to your course lectures, materials, quizzes, and labs
- Subject-matter-expert support to help you increase your retention of course material

"The course content and OnDemand delivery method have both exceeded my expectations."

-Robert Jones, Team Jones, Inc.

Get Certified with GIAC Certifications

- Distinguish yourself as an information security leader
- 30+ GIAC cybersecurity certifications available
- Two practice exams included
- Four months of access to complete the attempt

"GIAC is the only certification that proves you have hands-on technical skills."

-Christina Ford, Department of Commerce

MORE INFORMATION

www.sans.org/ondemand/bundles www.giac.org

*GIAC and OnDemand Bundles are only available for certain courses.

SANS

SAVE THE **DATE**

Automotive Cybersecurity Summit & Training

Detroit, MI | May 1 - May 8, 2017

www.sans.org/AutoSummit

Save the Date!

SANS ICS & ENERGY HOUSTON SUMMIT & TRAINING

July 10-16, 2017

www.sans.org/ICS-Houston

Hotel Information

Training Campus

Wyndham Garden Lake Buena Vista Disney Springs Resort

1850B Hotel Plaza Boulevard | Orlando, FL 32830
407-842-6644
www.sans.org/event/ics-security-summit-2017/location

Extending your stay or bringing your family?

Get pre-arrival savings of 10% on multi-day tickets and receive one complimentary admission to an additional Disney Experience. For more details, visit:

www.mydisneygroup.com/ics17

Special Hotel Rates Available

A special discounted rate of $154.00 S/D will be honored based on space availability.

These rates include high-speed Internet in your room and are only available for a limited time. When calling the hotel, you must mention that you are attending the SANS event to get the discounted rate. Please note that the group rate is based on availability.

Registration Information

Register online at www.sans.org/ICS-Summit

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

Save $400 when you register for the summit and a course!

Pay Early and Save

FOR THE SUMMIT ONLY	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**2-1-17**	**$200.00**	**2-22-17**	**$100.00**
FOR A COURSE ONLY	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**2-1-17**	**$400.00**	**2-22-17**	**$200.00**

Some restrictions apply. Discount offers cannot be combined.

Use code **EarlyBird17** when registering early

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 March 1, 2017 – processing fees may apply.

SANS ICS SECURITY
ORLANDO
SUMMIT & TRAINING

SUMMIT:
March 20-21

TRAINING:
March 22-27

ICS410: **ICS/SCADA Security Essentials**
Instructor: Justin Searle | Certification: GICSP

ICS456: **Essentials for NERC Critical Infrastructure Protection**
Instructor: Tim Conway

ICS515: **ICS Active Defense and Incident Response**
Instructor: Robert M. Lee

SEC504: **Hacker Tools, Techniques, Exploits, and Incident Handling**
Instructor: Mick Douglas | Certification: GCIH

HOSTED: **Assessing and Exploiting Control Systems**
Instructor: Larry Pesce

HOSTED: **Critical Infrastructure & Control System Cybersecurity**
Instructor: Matthew Luallen

MGT415: **A Practical Introduction to Cyber Security Risk Management**
Instructor: James Tarala

www.sans.org/ICS-Summit