SANS

8TH ANNUAL ICS & SCADA SECURITY SUMMIT

Program Guide

Lake Buena Vista, FL | February 12-13

Summit Agenda

All Summit Sessions will be held in the Grand Harbor Ballroom North (unless noted).

All approved presentations will be available online following the Summit at https://files.sans.org/summits/nascada13.
An e-mail will be sent out within 5 business days once the presentations are posted.

Tuesday, February 12

7:00 a.m. - 5:00 p.m.

Registration

Location: Cape Cod Registration Desk

8:00-9:00 a.m.

Reality Check 2013: SCADA Now and Next

Moderator: Michael J. Assante, ICS & SCADA Chair, SANS Institute

Panelists:

- *Ed Goff, CISSP, Enterprise Architect - IT Architecture & Security, Duke Energy*
- *Seán Paul McGurk, Managing Principal, Industrial Control Systems Cybersecurity, RISK Team, Verizon*
- *Patrick Miller, Principal Investigator, National Electric Sector Cybersecurity Organization; President & CEO, EnergySec*
- *Tim Roxey, Chief Cyber Security Officer; Director – ES-ISAC North American Electric Reliability Corporation*
- *Christopher Tarnovsky, VP of Semiconductor Security Services, IOActive, Inc.*

We've made some advances in SCADA security, but impactful attacks against enterprise systems still regularly make headline news, and ICS/SCADA is sorely at risk. As 2013 gets underway, we'll look at some of 2012's SCADA success and horror stories, and lay out a roadmap for what we should be prioritizing now and over the next several years. This panel of SCADA all-stars is pulling no punches in a hard-hitting review of the current state of SCADA security and what is needed to make real progress.

9:00-9:45 a.m.

Leveraging Corporate Risk Porfolios to Quantify the Need for Security Team Expansion

Robert McComber, Sr. Program Manager (Security), Telvent

Today's security leaders face an increasingly complex challenge with regard to expanding their teams to meet what they believe to be an apparent threat. As executives try to balance increasing shareholder pressure for fiscal restraint with a desire to keep the enterprise safe through security investment, new approaches are required not only to 'sell' security upstream to corporate leadership, but also to determine internally where to invest more limited budgets. This talk will focus on the application of corporate risk analysis tools and models to security challenges in a manner that not only provides strong justification, but also reduces overlap with other groups and focuses on core threats, rather than expending resources on outlier risks.

9:45 - 10:15 a.m.

Networking Break & Vendor Expo

Location: Cape Cod B&C

10:15-11:00 a.m.

SCADA 2017: The Future of SCADA Security

Jonathan Pollet, CAP, CISSP, PCIP, Founder/Principal Consultant, Red Tiger Security

New threats to cyber security are constantly emerging and rapidly evolving. One of the best ways to prepare for threats you can't predict is to build an agile organization with flexible response strategies. This session will delve into the current threat landscape, scan the horizon for emerging threats that are likely to emerge in the next few years, and look at how your team can be ready to respond to the threats no one can yet predict.

11:00-11:45 a.m.

What Operations Technology Teams Can Learn from Operations

Tim Conway, Director, NERC Compliance and Operations Technology, NiSource

For a decade and a half, Conway has supported control center operations and has learned much about the capabilities and strengths of Bulk Electric System operations processes and procedures. Many of these processes and methodologies can – and, he asserts, should – be leveraged to improve Operations Technology approaches for similar real-time system challenges in the SCADA sector. Compliance culture, systems management, and training will be addressed.

Summit Agenda

11:45 a.m. -1:00 p.m.

Corporate Risk®
>>>>>>>SOLUTIONS

Lunch & Learn

Securing Remote Access to Critical Infrastructure Field Components

Boyd Nation, MS, MBA, Senior Security Consultant
Todd Ponto, CISSP, BSCIS, MSIS, CCSA, CCENT, Security +, Network +, A+, Senior Security Consultant

CRSI will present on securing remote access to critical infrastructure field components. The focus of the discussion will be on substation automation and complying with the NERC CIP Reliability Standards in non-IT environments (primarily substations and generation plants) but the principles being discussed during this presentation will also be able to be applied to the oil and gas industry and other critical infrastructure sectors.

Note: This lunch & learn will be limited to the first 50 attendees.

Palantir

Lunch & Learn

Kasparov and the Glass Cockpit: From Disparate Data to Enterprise-wide Understanding

Dennis Lu, Forward Deployed Engineer

The success of your enterprise is dependent on securing your information network. Unfortunately, the traditional patchwork of automated defenses such as firewalls, anti-virus software, and intrusion detection systems fails against an intelligent and innovative adversary. Effective network defense requires a command-level view that integrates signals from all parts of your enterprise and enables expedient analysis. Palantir provides a platform that allows you to integrate all your disparate data sets to search, analyze, manage, and share your data like never before. Come learn how we are changing the game in cyber security by applying lessons from our work in intelligence, health, finance, and other industries.

1:00-1:45 p.m.

13 Ways Through a Firewall

Andrew Ginter, M.Sc., ISP, CISSP, Director of Industrial Security, Waterfall Security Solutions

Firewalls are a given - everyone assumes that every security posture includes a firewall. But are they really secure? Join us to see 13 ways to break through a firewall. Attacks include: walking a USB stick past the firewall, phishing attacks, steal a password, use essential connections to compromise servers, piggy-back on VPN, split tunneling, firewall vulnerabilities, firewall configuration errors and omissions, forge an IP address, use default password, stand up a wireless access point inside the protected network, and using vendor back-doors. Note: One or two interesting scenarios will be a live presentation, others will be screen shots taken from live demos, and still other scenarios will be discussion only. For each scenario, compensating measures are discussed and compared.

1:45-2:45 p.m.

Supply Side: Perspective on Progress and Challenges

Moderator: Michael J. Assante, ICS & SCADA Chair, SANS Institute
Panelists:

- *Markus Braendle, Group Head of Cyber Security, ABB Inc.*
- *Paul Forney, CSSLP , Chief Technologist, Invensys Operations Management*
- *Ed Goff, CISSP, Enterprise Architect - IT Architecture & Security, Duke Energy*
- *Walt Sikora, Vice President – Security Solutions, Industrial Defender*

In this session, representatives from the leading control systems suppliers will share their perspective on the progress that has been made and the challenges still to be tackled. Learn what's new and what's next in testing, security baseline, life-cycle support, vulnerability management, patch validation, and more.

2:45-3:15 p.m.

Networking Break & Vendor Expo

Location: Cape Cod B&C

Summit Agenda

3:15-4:00 p.m.

ICS Security from the Trenches

Billy Rios, Technical Director, Cylance, Inc.

Over the last two years, researcher Billy Rios has discovered thousands of vulnerabilities in Industrial Control Systems (ICS) software and hardware. Join him as he describes some of the most interesting vulnerabilities he has discovered and listen as he chronicles his interaction with the various ICS vendors. This talk will also cover the methodologies used to discover various vulnerabilities, the poor security architecture of common ICS components, and various trends seen in ICS security.

4:00-5:00 p.m.

New Challenges, New Solutions: Securing the Utility & CyberCity

• Chris Humphreys, Director, The Anfield Group

• Ed Skoudis, Fellow, SANS Institute

The cyber threat to North America's most critical infrastructures continues to be the top priority for both public and private sector asset owners. Electric utilities are constantly trying to balance the security, reliability, and regulatory responsibilities around cybersecurity to ensure the integrity of the North American Bulk Electric System. Leveraging the NERC Critical Infrastructure Protection (CIP) regulatory framework as a baseline, the SANS Securing the Utility (STU) course provides in-depth training and awareness to understand the foundations of implementing a sustainable and effective security and compliance program. The STU course modules comprehensively cover CIP requirements while providing proven information that close the most exploitable human vulnerabilities. This discussion will provide the audience with a mapping of what your security awareness programs should contain and you will leave with a list of the top human vulnerabilities to be addressed. The security principles and best practices for utilities contained in the STU course will give participants everything they need to be secure while managing the constantly evolving regulatory climate around cyber and CIP.

Attendees will also hear from Ed Skoudis, creator of the dynamic CyberCity virtual training, which allows government hackers to prepare for and learn to defend against attacks in a virtual reality setting. Ed will give an overview of CyberCity's capabilities, and will be available to answer attendee questions following the session.

Please complete all summit evaluations so we may improve future summits. You may leave the surveys at your seat or turn them into the SANS registration desk.

5:00-6:00 p.m.

Networking Reception for International Delegates

Location: Asbury C

SCADA professionals around the world face the same challenges, but don't often get the chance to network face-to-face with peers from other nations. The SCADA Summit brings together attendees from across the globe. Join your fellow international attendees for refreshments, networking, and the exchange of ideas. Share best practices and learn what's being done to advance the state of SCADA security around the world.

6:00-8:00 p.m.

Welcome Reception for All Attendees

Location: Yacht Club Marina

Sponsored by

CODENOMICON

Summit Agenda

All Summit Sessions will be held in the Grand Harbor Ballroom North (unless noted).

All approved presentations will be available online following the Summit at https://files.sans.org/summits/nascada13.
An e-mail will be sent out within 5 business days once the presentations are posted.

Wednesday, February 13

7:30-8:00 a.m.

Registration

Location: Cape Cod Registration Desk

8:00-8:45 a.m.

Getting Defensive: Better Defenses and Advanced Incident Response

Eric Cornelius , Director, Critical Infrastructure/ICS, Cylance, Inc.

Eric Cornelius will update last year's wildly popular talk on incident response handling and strategies, but will also move your thinking forward. New defensive techniques and technologies can be wielded proactively – minimizing your exposure to risk and the likelihood of having an incident in the first place.

8:45-9:30 a.m.

Putting SCADA Security to the Test: Why You Need a Lab and How to Get One

Chris Sistrunk, PE, Senior Engineer - T&D Technical Services, Entergy Services, Inc.

IT folks have been doing it for years - building labs to test new products before rolling them out – but the concept is still rather revolutionary to most practitioners of SCADA security. Yet the benefits of a lab are many, including training staff and solving real-world problems by replicating and attacking them in the relatively low-risk lab environment. But how do you pitch this (not inexpensive) idea in a way that gets organizational buy-in? And if your organization is just too small, what are the factors to considering when using a third-party lab? Hear ideas and ask questions of someone who evolved his organization's capabilities from one small lab to five complete labs.

9:30-10:00 a.m.

Networking Break & Vendor Expo

Location: Cape Cod B&C

10:00-11:00 a.m.

Threats, Defined: Updates from INL

Bri Rolston & Rita Wells, Idaho National Laboratory

The U.S. government understands risk as threats, vulnerabilities and consequences. Industry understands the risk as impacts and probabilities. Understanding the differences in these risk equations and creating the tie to the asset owner's configurations will promote better partnerships between USG and critical infrastructure asset owners. The DOE Office of Electricity Delivery and Energy Reliability has funded two projects for the Idaho National Laboratory which delve deeper into certain aspects of the asset owner risk equation. The first project is the Root Cause Security Analysis Matrix, which will solve the complex story problem by analyzing a historical incident. Why did the exploit worked? - What mitigations would have prevented the exploit? - What was the cost to defend/respond? These are the questions to be solved. The second project is the Advanced Cyber Threat Analysis which involves an operational threat assessment to create a predictive attack path and adversary fingerprint. This analysis will understand how a specific threat impacts risk.

Summit Agenda

11:00-11:45 a.m.

You Have No Integrity!

Dale Peterson, CEO, Digital Bond, Inc.

The mantra in the ICS world is that availability is the #1 concern and trumps all, but today almost all SCADA and DCS have no integrity. An asset owner really has no idea of the state of their deployed system because rogue firmware and ladder logic can be loaded onto their systems. The systems could be compromised today, and they would never know. In this session Dale will provide vivid examples of the impact of integrity failures on real SCADA and DCS equipment and why the reliance on keeping the bad guys out is more foolish by the day.

Dale will also address the lack of integrity in the ICS community shown by inaction, mistakes and false information by vendors, asset owners, government and consultants. Why does the community want to focus on side issues like information sharing, responsible disclosure, cyber legislation when we won't even face the basic truth that critical infrastructure ICS has no integrity and we, as a community, are doing nothing about it.

11:45 a.m. - 1:00 p.m.

INDUSTRIAL DEFENDER®

Lunch & Learn

SANS Survey on the Security Practices of SCADA System Operators

Justin Searle, Managing Partner, UtiliSec

A survey is underway examining the level of awareness system operators have around cyber risk, their attempts to manage that risk, and how their efforts are working out so far. Be among the first to hear the results of this research, and see how you stack up to your peers.

1:00-1:45 p.m.

Wastewater Plant Process Protection

Thomas J. McGovern, Broward County North Regional Wastewater Treatment Facility

In a utility treatment plant controlled by a Supervisory and Data Acquisition (SCADA) system, what is it that needs protection? Isn't it the actual treatment processes? If that is the case, those processes must then be self-protecting. Mechanisms must be built into the treatment processes that make them failsafe from any directives from SCADA that might drive a process into an undesirable condition. If implemented correctly, the failsafe protection renders SCADA misdirects harmless. The presentation explores how to analyze the individual processes and how to best implement failsafe controls from an engineering perspective.

1:45-2:45 p.m.

Analysis First! A Model for Actionable Critical Infrastructure Cyber Intelligence

Sean McBride, Co-Founder & Director of Analysis, Critical Intelligence

Information sharing is the fall back approach for what critical infrastructure industrial control system asset owners say they want from their governments. Ironically, it is also what governments say they want to provide to the private sector. Such happy chatter overlooks the need for all stakeholders to develop the analytical capabilities that result in improved security posture. This presentation uses real-world examples of intelligence gathering and analysis to overcome the fallacy/excuse/petition of "give us more information."

2:45-3:15 p.m.

Networking Break & Vendor Expo

Location: Cape Cod B&C

Summit Agenda

3:15-4:00 p.m.

Storming the Castle: Pitfalls of Defense-in-Depth Strategies

Major Jonathan Butts, Assistant Professor of Computer Science, Air Force Institute of Technology and Chair,
IFIP Working Group 11.10 on Critical Infrastructure Protection

Current defense-in-depth mitigation strategies protect against traditional malware but are not sufficient at safeguarding against threats in the SCADA environment. To adequately protect against advanced threats and account for the unique operating requirements, a shift in mindset is needed. This talk presents a vulnerability assessment strategy developed for Dept of Defense weapon systems. The concept relies on input/output validation and evaluation from the inside-out, as opposed to traditional outside-in strategies. Case studies are provided to highlight the pitfalls associated with a purely defense-in-depth strategy and to demonstrate an alternative approach to securing SCADA systems.

4:00-5:00 p.m.

SCADA Goes Global: Lessons Learned from Around the World

Moderator: Art Conklin, Ph.D, Center for Information Security Research and Education at The University of Houston

Panelists:
- *Adam Bosnian, EVP Americas, Cyber-Ark*
- *Paul Forney, CSSLP, Chief Technologist, Invensys Operation Management*
- *Manuel Humberto Santander Peláez, IT Security Architect, EPM (Colombia)*
- *Tyler Williams, Industrial Cyber Security Solutions Manager, Global Oil and Gas Company*

Any control systems supplier can tell you that a power plant in South Carolina is using the same systems and the same OS as a power plant in Barcelona; there are no great differences in systems or technologies from one area of the globe to another. Yet international information sharing and collaboration lag behind advances in SCADA security, and opportunities for learning may be missed. This panel takes a proactive approach to a global dialog.

Please complete all summit evaluations so we may improve future summits. You may leave the surveys at your seat or turn them into the SANS registration desk.

Thank you for attending the
North American ICS & SCADA Security Summit!

Exhibitors

AlertEnterprise!

AlertEnterprise Delivers IT-OT Convergence to protect Critical Infrastructure from Cyber and Operational security threats. Correlating threats across IT systems, Physical Security and SCADA/DCS Systems enables true prevention of theft, sabotage, insider threat and acts of terrorism. AlertEnterprise solutions deliver Identity and Access Management, Situational Intelligence and Incident Management and Response.

Asguard Networks

Asguard Networks provides network security appliances that help companies connect their industrial assets in a way that is highly secure, cost-effective and easy-to-use. Our standards-based SimpleConnect™ product allows companies to leverage their existing network infrastructure in order to realize the benefits of pervasive connectivity while strengthening security.

Bayshore Networks

Bayshore SCADA Firewall™ from Bayshore Networks is the only application-aware firewall used to protect SCADA systems in energy, building automation and other critical infrastructure sectors. We support various industrial control protocols including Modbus, DNP3, IEC 61850, and other popular protocols, delivering unmatched defense against targeted attacks on SCADA infrastructure.

Codenomicon

Codenomicon finds zero-day vulnerabilities others can't find. Codenomicon's Defensics Traffic Capture Fuzzer finds security bugs in industrial communications protocol-implementations, including proprietary protocols. New for SANS North American ICS & SCADA Security Summit 2013, Codenomicon introduces its Defensics MODBUS Slave protocol testing tool. For more information, go to **www.codenomicon.com**.

Corporate Risk Solutions

Corporate Risk Solutions, Inc. (CRSI) is a wholly owned subsidiary security consulting firm of Corporate Enterprise Security, Inc. that specializes in providing security consulting services for Energy (Electric, Oil and Gas), Government, and other Critical Infrastructure Industries. CRSI provides consulting services in regulatory compliance, IT / Cyber Security, and Physical / Corporate Security.

DEXA Systems

Dexa Systems is a global, privately held company that provides cyber and physical security solutions for Critical Infrastructure (CI) industries, including oil and gas, utilities, petro chemicals, pipeline, upstream, refineries, mining and storage. We provide cyber-security solutions through risk-based strategies, comprehensive products & services, and compliance options for both existing and upcoming regulations.

EnerNeX

EnerNeX is an electric power research, engineering, and consulting firm specializing in providing solutions for challenges in the electric power industry through research, engineering, and cyber security using advanced methodologies and technologies. EnerNeX Smart Grid Labs has a core infrastructure that supports end-to-end application testing from distribution feeder equipment to the substation to utility control centers and enterprise systems, to field area communication networks to meters and gateways to building automation networks and home area networks, to smart devices and appliances.

Exhibitors

Industrial Defender

Industrial Defender is the global leader in Automation Systems Management. Our solutions offer a single, unified view into security, compliance, and change management activities across heterogeneous environments. Thanks to an exclusive focus on automation environments, Industrial Defender is able to monitor activities, manage information, and protect vital assets from threats that might compromise availability, performance, health, and safety. For over a decade, Industrial Defender has been delivering solutions with a low operational impact, tight integration with systems, and protocols core to your business. Over 400 companies in 25 countries trust Industrial Defender technology to help secure their critical infrastructure.

IOActive

Established in 1998, IOActive positioned itself as a leader in the Northwest's computer security community, where it specializes in application security, infrastructure assessments, compliance, incident response, and smart grid services. The company has helped Fortune 500 organizations with enterprise risk management, and independent technical validations of security hardware and applications.

Mutualink

Mutualink is the industry's pioneer in creating scalable, dynamic peer based multimedia interoperability at an affordable price. Through Mutualink, mobile radios, telephones, PA systems, streaming video, images, and files can be shared in real time providing critical communications that enhance preparedness and effective emergency management, coordination and response.

National Electric Sector
Cybersecurity Organization

NESCO

The National Electric Sector Cybersecurity Organization (NESCO) is an independent public-private partnership operated by EnergySec with funding assistance from the Department of Energy. NESCO serves as a focal point bringing together utilities, federal agencies, regulators, researchers, and academics. NESCO supports efforts to enhance the cybersecurity of the electric infrastructure.

Palantir

Palantir is a Silicon Valley software company founded in 2004 by a group of PayPal and Stanford alumni. Originally developed for the Intelligence Community, Palantir's data fusion and analysis platform is currently deployed against the most critical problems at many of the world's most critical enterprises.

One Way to Connect

Waterfall

Waterfall® Security Solutions Ltd. is the leading provider of Unidirectional Security Gateways™, securely integrating industrial control systems with business networks, without incurring the safety and reliability risks which accompany firewalls. Unidirectional Gateways simplify regulatory and standards compliance, and reduce security program operating costs. For true security, demand Unidirectional Security Gateways.

2013 UPCOMING SUMMITS & TRAINING COURSES

What Works in Cyber Threat Intelligence Summit
Washington, DC | March 22

AppSec Summit & Training
Austin, TX | April 22-27

Critical Security Controls International Summit & Training
London, UK | April 22 - May 2

Mobile Device Security Summit & Training
Anaheim, CA | May 30 - June 6

Virtualization & Cloud Computing Summit & Training
Anaheim, CA | May 30 - June 6

Security Impact of IPv6 Summit & Training
Washington, DC | June 14-16

Digital Forensics and Incident Response Summit & Training
Austin, TX | July 9-16

Critical Security Controls Summit
Washington, DC | August 12-18

APAC ICS & SCADA Security Summit
Singapore | Fall 2013

Counter Hack Summit & Training
Washington, DC | November 7-14

For more information on speaking at an upcoming summit or sponsorship opportunities, e-mail SANS at **summit@sans.org**

Visit **www.sans.org/summit** for detailed summit agendas as they become available.