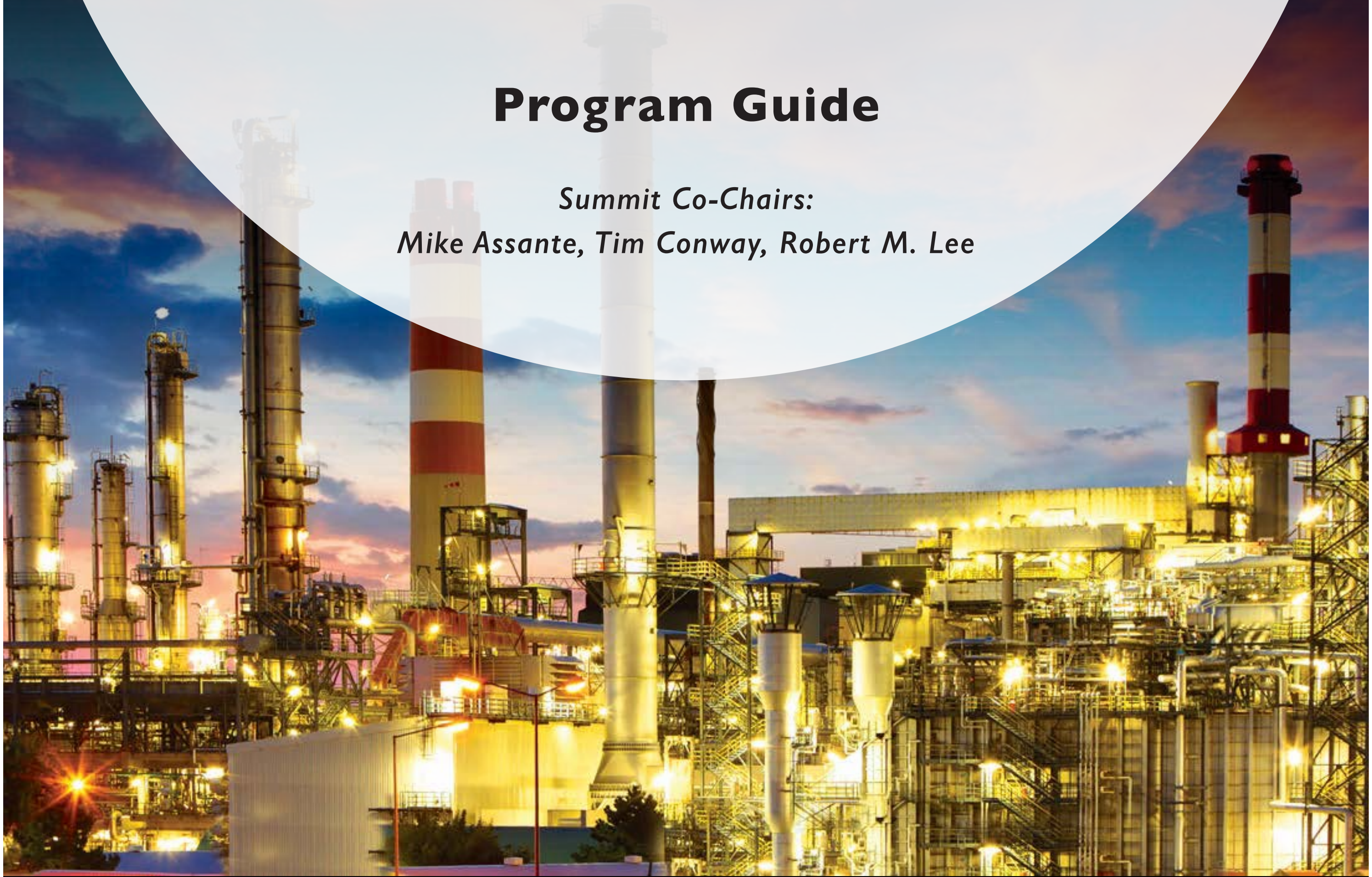
SANS

11TH ANNUAL ICS SECURITY SUMMIT

February 22-23, 2016 | Orlando, FL

Program Guide

Summit Co-Chairs:
Mike Assante, Tim Conway, Robert M. Lee



@SANSICS #ICSSummit

Agenda

All Summit Sessions will be held in the Orange/Lake/Osceola rooms (unless noted).

All approved presentations will be available online following the Summit at
https://ics.sans.org/ics-library/summit-archives
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Monday, February 22

7:30-8:30 am

Registration & Coffee (LOCATION: SUMMIT FOYER)

8:30-8:45 am

Building Skills with Challenges and Trainings

The ICS Cybersecurity 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 to advance your career. Hear about the lessons learned so far from the ICS Cybersecurity Challenge and how you can play to win.

Mike Assante*, Director – ICS/SCADA, SANS Institute*
Tim Conway*, Technical Director – ICS, Author, Instructor, SANS Institute*
Robert M. Lee*, Author & Instructor, SANS Institute*

8:45-9:30 am

KEYNOTE: ***What's Changed, What Hasn't, and What We Should Do About Both***

With the increased adversary attention to critical infrastructures and key resources in the U.S. and abroad, there has never been a more critical time for public and private interests to collaborate to mitigate risks to ICS assets that contribute to the nation's critical infrastructures. Mr. Quade will provide an overview of the current threat environment and will seek to stimulate a dialogue on a number of technical and operational strategies to mitigate the risks that cyber attackers see fit to exploit, leveraging our collective strengths, and the adversaries' weaknesses.

Philip Quade*, Director, Cyber Task Force; Special Assistant to the Director NSA for Cyber, National Security Agency*

9:30-9:45 am

The View from the ICS Wall

Possibly the best way to learn how to defend your systems from attack is to learn more about how the attacks actually happen. In other words, if you want to prevent attackers from breaking your stuff, you need to know what it really takes to break it. Now's your chance to come face-to-face with a life-sized wall of control systems just waiting for you to mess with them. Learn more about how to put your skills to the test, and get ready to do some damage.

Tom Van Norman*, Sr. Technical Staff, Counter Hack Challenges*

Monday, February 22

9:45-10:30 am

Industry 4.0

Some are suggesting we are on the verge of the fourth industrial revolution as digital devices, big data, and connectedness transforms 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 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 view from a supplier, end user, and two industry security experts. You don't need to bring your rose-colored glasses; but probably is 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****, Director – ICS/SCADA, SANS Institute*

PANELISTS: ***David Foose****, Ovation Product Security Manager, Emerson*
Ernie Hayden*, Securicon*
Bryan Owen*, Cyberecurity Manager, OSIsoft*

10:30-11:00 am **Networking Break and Vendor Expo** (LOCATION: UNIVERSAL A/B)

11:00-11:45 am **Solutions Sessions**

Presented by

paloalto networks

Advanced Threat Prevention in ICS Using Network, Endpoint and Cloud

During this session, we will discuss how to use a Next-generation security platform comprised of a Next-generation Firewall, Advanced Endpoint Protection and Threat Intelligence Cloud to:

- Quickly reveal zero-day malware that may be trying to penetrate and move laterally across your network
- Leverage a community-based approach to make sure your IR teams are mobilized on the real, highest-priority threats
- Prevent your HMIs, Workstations and Automation Servers from being commandeered by attacks utilizing zero-day exploits and malware
- Ensure an automated and complete lifecycle approach to stopping APTs such as Black Energy

Yves-Laurent Sivuilu, Systems Engineer, Palo Alto Networks

Presented by

SECURITY MATTERS

Expecting the Unexpected: Finding Where the Wild Things Are through ICS Network Monitoring

Control system networks are threatened from both internal and external sources. This presents a broad spectrum of threats to your network, from external actors with malicious intent to internal employees unintentionally harming reliability. Regardless of the source, unwanted activity can be identified through passive network monitoring using a mixture of whitelisting, blacklisting, and deep-packet inspection. In this talk, we will reveal some of the unexpected results from monitoring ICS networks and how you can capture and analyze this traffic to reduce and eventually remove unwanted behaviors and activities in your control system network.

Dennis Murphy, Senior ICS Security Engineer, SecurityMatters, LLC

Presented by

WATERFALL®
Stronger Than Firewalls

Cybersecurity: How Much is Enough?

Advice on costs and benefits of a cybersecurity program is often confusing and contradictory. For example, experts on a recent panel were heard to observe all of: "Security is pure cost," "there has to be an ROI for every one of our security investments, so we use a risk-based approach, but none of the risk calculations are quantitative," and "it all depends on the risk appetite of your board and executive." Even more confusing to business leaders: it is always possible to be more secure, or less secure. We know that all for every security defense, there is an offense that will succeed. How then, to evaluate cyber security funding requests? How can anyone ever know how much is enough? We explore the question "how much is enough" and draw some simple conclusions. We discuss how classic "natural disaster" risk models and other IT-centric security risk models that attempt to quantify the likelihood of attacks are poor fits to physical or cyber security problems. A good understanding of the characteristics of control system networks, industrial processes, safety systems, protection systems, security systems and attack capabilities are all prerequisites to an effective risk assessment. Assembling all this knowledge and these costs into a simple matrix for business leaders to understand and evaluate is very much possible. Join us to review approaches to risks, calculations, costs, and understand how to communicate these to business decision-makers.

Michael Firstenberg, GICSP, CISSP, GCIH, Director of Industrial Security Waterfall Security Solutions

Monday, February 22

11:45 am - 12:15 pm

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*

12:15-1:30 pm

Lunch & Learn Presentations

Presented by

LOCKHEED MARTIN

Why does the Ukrainian power outage news still get so much attention?

LOCATION: HILLSBOROUGH/PINELLAS

There are two types of organizations, those that have been compromised by an adversary and know it and those who have been compromised and do not know it. Which are you? When reports of an incident like the Ukrainian power outage are reported, our first thought is "hackers" must have done it. Sure, for the past decade we have been warned that hackers would find a way to shut down our critical infrastructure. It should be no surprise given the fragile and vulnerable operational technology control systems in production today. So, why does the Ukrainian power outage news get so much attention?

In this talk we will discuss why everyone wants to read about companies being hacked. The talk will also offer recommendations on how to mitigate your organization from being in the headlines. The presentation will not offer any "silver bullets". However, lunch will be provided and you might walk away with some ideas on how to improve security maturity.

Walt Sikora, VP Security Solutions, Lockheed Martin

Presented by

Recorded Future

BlackEnergy: The Before, The Attack, The Now

LOCATION: SEMINOLE B

What was being discussed/reported on BlackEnergy in the months before the Ukrainian attack, the attack itself, and the aftermath from the time of the attack leading up to the lunch and learn.

Zach Flom, Threat Intelligence Analyst, Recorded Future

Presented by

paloalto networks

How to Architect "Zero Trust" Network Segmentation in Industrial Control Systems

LOCATION: SEMINOLE A

ICS environments are typically "flat", designed with a rudimentary security posture, never intended to be connected to the corporate network nor the Internet. The trend towards connectedness along with the rising ICS threat landscape has made ICS a prime target for cyber attacks. Stronger access controls are critical for managing the different attack surfaces.

Join Palo Alto Networks where we will have a practitioner with 20 + years hands-on experience in the IT/OT space specializing in ICS/SCADA systems. He will share with you how he was able to apply zero trust principles to achieve connectedness securely and easily utilizing the pre-existing infrastructure. You will learn:

- How to architect for prevention, and plan for detection with Zero Trust and the Palo Alto Networks Security Platform.
- How to bolster your network visibility and segmentation without having to completely re-engineer the infrastructure
- How the Palo Alto Networks platform can help you realize these concepts in a systematic, organized, and minimally disruptive way

Lionel Jacobs, Palo Alto Networks

Monday, February 22

1:30-2:30 pm

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. They will then 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 the 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**, Cybersecurity Assessment Lead, Idaho National Lab*
***Joseph Price**, Cybersecurity Research & Development, Idaho National Lab*

2:30-3:15 pm

Logging and Monitoring for Distributed Control Systems

It has long been accepted that security monitoring associated with Distributed Control Systems and Supervisory Control and Data Acquisition networks is operationally and administratively different from traditional information technology business environments. The proliferation of smart devices, extended networks, geographically dispersed assets, and enforceable regulatory standards increase 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*

3:15-3:45 pm **Networking Break and Vendor Expo** (LOCATION: UNIVERSAL A/B)

Monday, February 22

3:45-4:30 pm	***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*
4:30-5:00 pm	***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*
5:00-6:00 pm	**Vendor Networking Reception** (LOCATION: UNIVERSAL A/B)

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.

You may leave completed surveys at your seat or turn them in to the SANS registration desk.

6:30-9:30 pm	**ICS Game Night**

KIPS, Kaspersky Industrial Protection Simulation	**WOPR: Shall We Play a Game?**	**NetWars CyberCity Tournament**
LOCATION: UNIVERSAL E	LOCATION: UNIVERSAL D	LOCATION: ORANGE/LAKE/OSCEOLA

Be Sure to Visit the ICS Wall

The ICS Wall is an interactive display that allows students to interact with real control system devices in a closed environment. Individuals are encouraged to bring their own computers, 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.

Tuesday, February 23

7:30-8:30 am

Registration & Coffee (LOCATION: SUMMIT FOYER)

8:30-8:45 am

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 to 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**, Director – ICS/SCADA, SANS Institute*

8:45-9:15 am

So You Have Just Been Asked To Brief the Board of Directors on Cybersecurity

Situation: Your boss emails you to say that the Board of Directors is meeting next week and cybersecurity is on the agenda. The CEO wants you to brief the board.

A big opportunity? Perhaps. A high-risk moment? Most certainly.

In this very practical briefing, Alan will share the results of five months of research on the most interesting and appropriate-for-the-audience techniques IT security managers have used in high-level gatherings and the most damaging errors that they continue to make. The problem is especially acute in the ICS realm where one has to cross the streams of well-understood engineering with tech talk.

***Alan Paller**, Director of Research, SANS Institute*

9:15-9:35 am

Breaking Down the Ukraine Power Hack: What We Need to Know and Why

Join the SANS ICS team to explore this developing story and discover the likely ramifications, now and in the long term.

***Mike Assante**, Director – ICS/SCADA, SANS Institute*
***Tim Conway**, Technical Director – ICS, Author, Instructor, SANS Institute*
***Robert M. Lee**, Author & Instructor, SANS Institute*

9:35-10:15 am

Snap, Crackle, and Pop – What Does it Take to Cause Damage?

We have all heard about a furnace that was damaged, but are we going to see more incidents like that? ICS is where cyber meets the physical world but it takes specific knowledge and understanding to predictably cause havoc. What does it take for intruders to develop and test a capability that can meaningfully attack the ICS? Can intruders accidentally disrupt the process, release substances, or damage equipment? How can things go wrong? We know of many ICS environments that have already been intruded upon; what happens next?

MODERATOR: ***Mike Assante**, Director – ICS/SCADA, SANS Institute*

PANELISTS: ***Robert M. Lee**, Author & Instructor, SANS Institute*
***Jeff Melrose**, Principal Technology Strategist for Cybersecurity, Yokogawa U.S.*
***Joseph Price**, Cybersecurity Research & Development, Idaho National Lab*

10:15-10:45 am

Networking Break and Vendor Expo (LOCATION: UNIVERSAL A/B)

Tuesday, February 23

10:45-11:15 am

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 expectations 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*

11:15 am - Noon

Connectivity Surprise Factor: What's in Your ICS?

Everyday, 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 onto common shared infrastructures leading to new risks and greater exposure to threats. In this session, learn about the "Connectivity-Surprise Factor" and benefits that can be gained by performing comprehensive and real-time network asset-inventories, by 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.*

Noon-1:15 pm

Lunch & Learn Presentations

Presented by

SYNOPSYS®

Defining A Cybersecurity Signoff Process

LOCATION: SEMINOLE B

In recent years efforts have been undertaken to develop best practices for building security into products used in industrial control systems. While these best practices go a long way towards creating products where security can be managed more adequately, what has been absent is adequate cybersecurity testing practices and standards that allow organizations to validate and verify that the best practices meet a requisite level of cyber assurance. Software must ship, so it is important for organizations to know when cyber assurance is adequate. Join this session for an overview on how organizations can apply testing practices that lead to a cybersecurity signoff process.

Mike Ahmadi, Global Director,
Critical Systems Security, Synopsis

Presented by

PAS®

Little Green Men, Industrial Cybersecurity, and Life As We Know It

LOCATION: HILLSBOROUGH/PINELLAS

Do aliens exist? If so, why have we not had a confirmed visit? Maybe the answer is that it's hard for civilizations and their technology to advance far enough to travel to other worlds. As our civilization and technology progress, are there threats lurking out there for us as well? We find one such threat from groups determined to infiltrate and commandeer the systems that control our power stations, refineries, water treatment facilities, and petrochemical plants. Science fiction? APTs such as Black Energy and their success getting into process control networks clearly indicate no. How do we keep critical infrastructure - and people that rely on it – safe and secure? In this session, we'll discuss what is missing from most industrial control system cybersecurity approaches today and best practices for mitigating ever-present cyber risk, whether from malicious attack or inadvertent engineering mistakes.

David Zahn, Chief Marketing Officer/General Manager - Cybersecurity BU, PAS

Presented by

LogRhythm®
The Security Intelligence Company

The Modern Cyber Threat Pandemic

LOCATION: SEMINOLE A

According to the 2015 Cyber Defense Report, 71% of organizations were compromised by a successful cyber-attack. The threat is real! It's no longer a matter of IF, but WHEN. In this session, Brian Emond will discuss the Security Intelligence Maturity Model (SIMM). Organizations can leverage the SIMM to drive security budgets by measuring the effectiveness of an organization's security capabilities around Mean-Time-to-Detect™ (MTTD™) and Mean-Time-to-Respond™ (MTTR™). Deliver the right information, at the right time, with the appropriate context, to significantly decrease the amount of time it takes to detect, respond to and neutralize damaging cyber threats.

Brian Emond, Sales Engineer, LogRhythm

Tuesday, February 23

1:15-2:00 pm

Critical Infrastructure ICS Attack Targeting

In the wake of ICS cyber intrusion escalation around the world, organizations are beginning to develop a robust security posture for their critical operations. To truly understand how to build early detection of persistent adversaries, we must realize the process they might take in identification and selection of a target using publicly available information. Included in this treasure trove are details about unique physical relationships between industries, for example shared corridors in the case of pipelines and high voltage AC power lines.

Recent ICS attacks and Stage 1 of the ICS Cyber Kill Chain emphasizes the question "How hard is it really to correlate a physical asset's location with its public domain address?" In this session, we will explore a planning-and-preparation methodology using open-source information to assist in the reconnaissance and targeting of such a threat.

The topics that will be explored include:

- High-value target identification
- Remote cyber-accessible target selection
- Raising the cyber-to-physical identification level of certainty
- Identifying potential cyber-attack vectors
- Identifying potential delivery options

Jason Dely*, Principal Consultant – ICS Security, Cylance*
Jeff Gellner*, Principal Consultant – ICS Security, Cylance*

2:00-2:45 pm

No Stone Unturned

In the world of industrial safety, we're pretty darn good at finding the root cause and taking action to avoid similar incidents—the Chemical Safety Board and the Transportation Safety Board are just a few 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*

2:45-3:15 pm

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*, Author and Instructor, SANS Institute*

Tuesday, February 23

3:15-3:30 pm

Powering Up Your ICS Knowledge is as Easy as 4-5-6

Join us for a quick sneak peek at the next step in the SANS ICS curriculum, ICS456: Essentials for NERC Critical Infrastructure Protection. The course author breaks down what the course covers and how the takeaways will benefit you and your organization.

Tim Conway*, Program Director – ICS, Author, Instructor, SANS Institute*

3:30-3:50 pm **Networking Break and Vendor Expo** (LOCATION: UNIVERSAL A/B)

3:50-4:30 pm

Why 90%+ of the ICS Vulnerabilities Don't Increase Risk – And How to Identify the Important Ones that Do

The most frequent and most 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 even 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.*

4:30-5:15 pm

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. This will also cover 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*

5:15 pm

Closing Remarks

Mike Assante*, Director – ICS/SCADA, SANS Institute*

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat
or turn them in to the SANS registration desk.

@SANSICS **#ICSSummit**