SANS ICS SECURITY

ORLANDO

SUMMIT & TRAINING

Program Guide

@SANSICS #ICSSummit

Agenda

All Summit Sessions will be held in the Windmere Z (unless noted).

All approved presentations will be available online following the Summit at ***https://www.sans.org/summit-archives/ics***

Monday, March 19

8:00-9:00 am	**Registration & Coffee**
9:00-9:30 am	***Modern Malware Demands Modern Defense*** As a community, we often find ourselves trying to balance the significance of ICS attacks and at the same time trying to explain the difficulty of achieving large scale repeatable effects across a diverse control system. While it is difficult to achieve this balanced position without sounding schizophrenic, it is important to have a nuanced discussion around these topics to enable ICS practitioners and leaders by providing the appropriate tools, and capabilities to return to work and defend critical control systems. *Tim Conway and Robert M. Lee (@RobertMLee), Summit Co-Chairs, SANS Institute*
9:30-10:15 am	***The First Safety Instrumented System Malware: TRISIS*** TRISIS/TRITON represents a game-changing development within the ICS security community as the fifth known ICS-specific malware (following STUXNET, HAVEX, BLACKENERGY2, and CRASHOVERRIDE), and the first such malware to specifically target safety instrumented systems. Since identification and public disclosure in early December 2017, much has been written on TRISIS and its implications, but technical deep-dives and analysis of implications remains rare. This discussion aims to fix that discrepancy by providing a detailed walkthrough of TRISIS functionality: how it communicates to its target device, how changes are transferred, and what alterations are made to safety system logic. By providing an overview of "how," we can move on to the next critical step: defending against and defeating TRISIS and similarly styled attacks. Toward that end, we will conclude with an in-depth discussion of how to detect and overcome TRISIS - and future variants - on the network, on host, and as part of overall ICS processes. *Joe Slowik (@jfslowik), Adversary Hunter, Dragos, Inc.* *Jimmy Wylie (@mayahustle), Senior Adversary Hunter, Dragos, Inc.*
10:15-10:35 am	**Networking Break** (LOCATION: WINDMERE Y)
10:35-11:20 am	***You're Probably Not Red Teaming (And Usually I'm Not, Either)*** In a world where it seems everyone and their dog is doing "penetration testing" nowadays, many individuals have started attempting to distinguish themselves by referring to their work as "red teaming." Heck, that's wound up in some bios which have been written for me in the past. However, this term is over-used and often misapplied. In this talk, Deviant will offer up a straightforward metric for untangling these terms, and then share tips, stories, and advice on tools that can help you in future Pen Tests or (if you're truly performing them) Red Team Engagements. *Deviant Ollam (@deviantollam), Security Auditor & Pen Test Consultant, The CORE Group*

Monday, March 19

11:20am – 12:05 pm	***Securing and Integrating Commercial Off-the-Shelf (COTS) Products for Industrial IoT*** Recent advancements in the availability of COTS processors which can operate in industrial / automotive harsh environments have led to a proliferation of new embedded Linux devices in industrial spaces. Customers are clamoring for connected devices and want to realize savings from connecting assets, but traditional industrial and automotive companies are struggling to provide near real time data without compromising machine security. While it's certainly annoying if your connected lightbulb is hacked, it can be a serious problem if heavy machinery is compromised. In this discussion, we'll talk about some of the common pitfalls in using vendor supplied solutions, some best practices for reducing the risk in connected machines, and some basic hardening principals that must be adapted for embedded devices. *Jon Taylor, GICSP, CISSP, Mining Technology – Cybersecurity Implementation Architect, Information Security Risk Management | Global Information Services, Caterpillar Inc.*
12:05-1:30 pm SECURITY MATTERS VERVE INDUSTRIAL PROTECTION PAS	**Lunch & Learn Sessions** ***Defeating Alert Fatigue: Transforming NSM Alerts Into Effective Workflows*** *Dennis Murphy, Lead ICS Security Engineer and Daniel Trivellato, Product Manager* ***Choose the Right Tool for the Job*** A "lessons learned" discussion on the value of breaking tradition in the OT space. *Rick Kaun, VP Solutions* ***ICS Cybersecurity Vulnerabilities and the One Chip Challenge*** *David Zahn, Chief Marketing Officer*
1:30-2:15 pm	***Tales from the ICS Crypt*** Adam and Tyler spend their time making like bad guys trying to attack critical infrastructure, and they've agreed to share experiences and stories from some of their most epic pen tests and red team engagements against ICS clients (all client details will be withheld to protect those involved or in witness protection programs). They've got some horror stories that will make your hair stand on end, sure, but they've also got great insight into what's working well, and how to leverage effective red team operations to ensure the stability, reliability, and security of some of the nation's most critical assets. *Adam Crompton, Senior Security Consultant, InGuardians* *Tyler Robinson, Senior Security Analyst, InGuardians*
2:15-3:00 pm	***Sh*t Happens! (But You Still Need to Drink the Water)*** The threat to our industrial control systems networks is real, dangerous, and growing. The networks used to optimize and operate our water infrastructure are often taken for granted due to the challenges of day-to-day operations and limited resources. Monitoring them is critical for protecting water utility assets and operations whether the threat is simply a configuration issue, failing devices, or even a targeted adversary. In this presentation, the presenter will discuss the process for providing and protecting water, its security, and how it differs from other ICS industries. He'll also share real-world experiences and case-studies to demonstrate the value of taking an active approach to defending these assets. Attendees will also be informed on building partnerships between IT and operations staffs and generating and maintaining appropriate executive sponsorship for security initiatives. Doug Short is the first Chief Information Officer and Chief Information Security Officer for the Trinity River Authority of Texas, a conservation and reclamation district providing water and wastewater treatment, along with recreation and reservoir facilities, for municipalities within the nearly 18,000-square-mile Trinity River basin. Previously, Doug served 28-years in the US Air Force. His experience includes coordinating and implementing national and international cyber strategy throughout the Federal Government and providing strategic analysis and recommendations to national leaders on cybersecurity issues and operations. *Doug Short, CIO & CISO, Trinity River Authority of Texas*
3:00-3:20 pm	**Networking Break** (LOCATION: WINDMERE Y)

Monday, March 19

3:20-4:05 pm	***Attack-Proof Facilities: Designing and Building in Safeguards Against Cyber Attack*** Process Safety Managed (PSM) facilities which process volatile hydrocarbon-based products need to be protected against physical consequences of a release caused by a cyber attack to the digital control systems. While we should and do focus on securing the computer systems themselves, we often overlook facility design, which is actually the most important defense against cyber attack. Basically, it is possible to build plants that are inherently safe by designing in systems and safeguards - such as relief valves and current overload relays - that are not vulnerable to a cyber-attack. This presentation will review the most common methods for process hazards analysis (PHA) of process industry plants, and then supplement those methods with a simple "cyber review," and will include a case study from the oil and gas industry where a Hazards and Operability (HAZOP) study was assessed using a PHA cyber review in order to determine whether or not the facility was inherently cyber-safe, and if not, make recommendations for design modifications that would make the facility cyber-safe. *Jim McGlone, GICSP, CMO, Kenexis*
4:05-4:50 pm	***Recent APT Campaign Targeting Energy Sector Assets*** Over the past year, a concentrated effort has been focused on specific energy sector critical assets, leveraging trusted relationships within supply chains and other partnerships in an attempt to gain access to corporate and control system networks. This technical discussion will review the threat actor's tactics and techniques observed during multiple on-site incident response engagements conducted by the DHS NCCIC Hunt and Incident Response Team related to this campaign. *Jonathan Briney, Sr. Lead Analyst – Industrial Control Systems Group, Hunt & Incident Response Team, U.S. Department of Homeland Security National Cybersecurity and Communications Integration Center* *Jonathan Homer, Cyber Security Hunt and Incident Response - Engagement Lead, U.S. Department of Homeland Security*
4:50-5:35 pm	***The Current and Next Generation CybatiWorks Hands-On ICS Models*** The CybatiWorks cybersecurity education platform is actively in use at universities and colleges, commercial entities, high school and within the SANS ICS curricula. The CybatiWorks platform uses hybrid software and hardware physical models to actively engage participants to interact with real cyber-physical attacks and defenses. CYBATI is also the prime recipient of an award with the Department of Energy to expand the existing platform to incorporate education and models for Power Grid, Pipeline and Building Automation for professionals and students. This presentation will give a brief history of the platform, provide a live display of the five existing models (i.e. Manufacturing, Pipeline, Power Grid, Traffic Light, children's Snap-Circuits) and their capabilities. The presentation will also describe the next generation of the CybatiWorks platform enabled by the DOE cooperative research and development agreement. *Matthew E. Luallen, Executive Inventor, CYBATI*
6:00-8:00 pm	**Summit Night Out in Orlando** (LOCATION: POINTE ORLANDO, 9101 INTERNATIONAL DRIVE) Let's kick back and relax with music, snacks, and drinks at local favorite Lafayette's. 

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.

Tuesday, March 20

8:00-8:45 am	***Registration & Coffee***
8:45-9:00 am	***Lifetime Achievement Award***
9:00-9:45 am	***ICS Threat Intelligence: Moving from the Unknowns to a Defended Landscape*** This talk is a follow up to last year's keynote on the unknown ICS threat landscape. We have learned a lot in the last year about ICS threats. 2017 was full of targeted adversaries and new tradecraft to watch out for in relation to securing industrial operations. In this presentation, attendees will learn about the various activity groups targeting the industrial sector and explore their tradecraft. There will also be a discussion on what ICS-specific threat intelligence is and how to take this knowledge and apply it in a meaningful way. We have very defensible infrastructure, and with knowledge of adversaries and a focus on the human defender we can move from defensible to defended. *Robert M. Lee, SANS Institute*
9:45-10:30 am	***Future Challenges and Changes in Industrial Cybersecurity*** While there are still under-protected plants, ARC research shows that most industrial companies have implemented cybersecurity programs to protect their facilities and SCADA systems. Most of these initiatives have followed recognized standards and guidelines like IEC 62443, NERC CIP, etc. These documents provide comprehensive guidance for a specific set of use cases given certain scope boundaries. These efforts have significantly reduced the risks of cyber-attacks on our critical infrastructure. However, recent developments and trends suggest that more needs to be done. Assumptions underlying current programs are too restrictive for the real needs of industry and infrastructure organizations. The cybersecurity challenges that industrial companies and infrastructure organizations face span the full IT-OT-IoT spectrum. Broader deployment of automation products in smart cities and commercial operations also demands a broadening of the potential use cases. This presentation will include a discussion of these expanded challenges and the gaps that need to be filled. Recommendations on the kinds of changes that are required will also be presented. *Sid Snitkin, Vice President, ARC Advisory Group*
10:30-11:00 am	**Networking Break & Vendor Expo** (LOCATION: WINDMERE Y)
11:00-11:45 am	***ICS Security in the Chemical Sector: Are We Really so Different?*** In discussions regarding technology the chemical sector is sometimes confused with or viewed as part of oil & natural gas, utilities, or other critical manufacturing sectors. It's easy to see why as similarities to all these sectors do exist. In fact, some companies in this sector are made up of various sites of diverse plants producing vastly different products. Independent of the parent company, these individual plants could easily align with another critical infrastructure sector. As a result, ICS security can be challenging. In this presentation, attendees will be introduced to the chemical sector and learn not only about some unique challenges, but specific opportunities which make it more defensible that other sectors. As we talk through a typical plant, we will highlight similarities and differences which influence ICS security decisions. We will take a look at some real-life incidents which were not caused by a cyber attack, but could be reproduced by one. The resulting lessons learned will provide insights into the need for dependency management considerations within architecture and security decisions. *Glenn Aydell, LazyHacker Consulting*

Tuesday, March 20

11:45am-12:30 pm	***Safety First! Injuries Last!: A Cybersecurity Perspective*** Cyberattacks impacting and manipulating critical process control and safety systems have always been the greatest concern throughout the ICS community. Asset owners and operators must look to their vendors and the OEMs for guidance and take appropriate mitigation actions to ensure a safe operating environment. Are you wondering what typical OEMs are doing with regards to vulnerability mitigation, testing, customer notification, patching, secure code development, and incident response? This talk will answer those questions and provide some case study examples to highlight real-world OEM-demonstrated capabilities. *Fred Cohn, Program Director, Product Security Office, Schneider Electric*
12:30-1:45 pm	**Networking Lunch & Vendor Expo** (LOCATION: WINDMERE Y)
1:45-2:30 pm	***Better Security Lies Beyond Hope and Cyber Hygiene: An Introduction to INL's Consequence-driven, Cyber-informed Engineering (CCE) Methodology and DOE Cyber Strike Demo*** In February 2017, the Defense Science Board (DSB) conclusively reported that our nation is unprepared to defend its critical infrastructure, or ensure power grid resilience as deterrence to cyberattack. In surprisingly frank, public language, the DSB made it all too clear that if a determined adversary decides it wants to own a control system, it will be successful. Leveraging deep engineering process knowledge, Idaho National Laboratory (INL) has been leading control systems security for nearly a decade, and today, a solution is at hand. The lab is currently demonstrating the potential of the emerging Consequence-driven, Cyber-informed Engineering (CCE) methodology – a transformative process that provides critical infrastructure owners and operators dramatic new capabilities to mitigate the cyber risks to their most essential industrial controls and embedded processes. *Andy Bochman (@andybochman), Senior Cyber & Energy Security Strategist, INL* *Daniel Noyes, Project Manager, INL*
2:30-3:15 pm	***Adventures in ICS Asset Identification: Physical Inspection Style*** Asset identification is a prerequisite for good network security monitoring, both of which are critical for industrial control system active cyber defense. The most time- consuming method of asset identification is physically crawling through your ICS facilities taking notes. And it's totally worth it! So grab your favourite spreadsheet app, hardhat and boots! Common methodologies for ICS asset identification are reviewed with a focus on physical inspection. Lessons learned from plant inspections in numerous electricity generating facilities, ranging from hydro, combustion turbine and thermal plants, are shared. The audience will be given tips and tricks to maximize on-site visits for accurate asset identification, effective security awareness that build relationships needed for smooth ICS incident response, ways to find rogue assets, and ways to ethically hack the physical security perimeter. The talk is geared towards new or existing facilities looking to increase their cyber defenses, and reinforces how ICS incident response supports the primary goal for safe and reliable plant operations. *Dean Parsons B.Sc., CISSP, GRID, GCIA, GSLC, Information Security Officer, Nalcor Energy*
3:15-3:45 pm	**Networking Break & Vendor Expo** (LOCATION: WINDMERE Y)

Tuesday, March 20

3:45-4:30 pm	***Measuring and Evaluating Cyber Risk in ICS Components, Products and Systems*** With the growth of IIoT in the ICS space, there is a need for cybersecurity testing of components, products and systems to mitigate the risk of cyber incidents in operational networks. While many specifications and guidance documents provide information on secure product development principles, there is still a need to test and measure the security posture of products using comprehensive testing criteria and an important certification management process throughout the life of a component. What should the security testing include and what are important attributes to measure and evaluate? What are supply chain considerations? How do you maintain certified status in the age of ICS vulnerabilities? *Ken Modeste, Director, Connected Technologies – Commercial & Industrial Business Unit, UL*
4:30-5:15 pm	***Jumping Air Gaps*** If you think an air gap prevents communication out of and into your industrial control system, you are wrong. We'll be exploring various ways to send data across an air-gap in Industrial Control Systems and other environments, including a live demo. Is it really possible to send data across an air-gap where no network has been connected? (No we're not talking about wifi, bluetooth, wirelessHART etc.) Can it be done without physical modification to your existing plant? Can we get that paragon of virtue- a data diode -to pass information in both directions without physically touching it? What else do you need to know? Find out. *Monta Elkins, CISSP, GICSP, Hacker-in-Chief, FoxGuard Solutions*
6:30-8:00 pm	**GIAC Certification Reception** (LOCATION: BAYHILL33) SANS will host its annual GIAC Certification Reception to congratulate GICSP, GRID, and GCIP holders on achieving certification. This reception brings together a recognized community of ICS security professionals for an evening of drinks, hors d'oeuvres, and networking. This reception is open to all GICSP, GRID, and GCIP certification holders, as well as those wanting more information about these certifications. The SANS ICS team will introduce the new GIAC Critical Infrastructure Protection (GCIP) certification. Familiarize yourself with available ICS Security certifications and learn first-hand from prominent industry experts as they explain how their certifications have impacted their careers and the organizations they protect.

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.