SANS | GIAC CERTIFICATIONS

#ICSAsiaPacific

SANS ICS Asia Pacific Summit 2020

13 November 2020

AGENDA

Friday 13 November 2020 (All times in Singapore Standard Time - SGT)	
08:30 - 09:00	**Live Networking**
09:00 - 09:15	**Welcome & Introductions** *Justin Searle - Summit Chair*
09:20 - 09:45	**Upskilling to Seize Cyber Opportunities** *David Koh - Chief Executive, Cyber Security Agency of Singapore*
09:45 - 10:00	**Break**
10:00 - 10:30	**ICS Cyber Threats and Hunting** *Robert M. Lee - Founder & CEO, Dragos*
10:35 - 11:05	**Building an OT Security Community - A Case Example from NZ** This presentation will outline the steps that kiwis are taking to secure their industrial networks. Using the NZ-specific VCSS-CSO standard, NZ industrial organisations have been working to secure their infrastructure. To support this, a community has been building around communication and collaboration. The NZ Industrial Control System Cyber Technical Network (NZ ICS Cyber TN) has facilitated discussions on a number of topics for the community, allowing sharing on what works, and what doesn't, with a specific NZ flavour. Some case studies will be shared as well as the good, the bad and the ugly of securing industrial networks in NZ. *Peter Jackson - Engineering Manager (Cyber), SGS ECL*
11:05 - 11:15	**Break**
11:15 - 11:35	**From Bad to Evil: Real Security Incidents and Findings from Live ICS Environments Assessments** While conducting health checks and compromise assessments on live ICS environments, interesting stories are behind discovering serious security incidents. This presentation is intended to share some of the evil discovered in live ICS environments in petrochemical, power and utilities industries. The presentation will also go through the stories behind these incidents which are believed to be useful to prevent similar incident in similar environments. *Moath Sakaji - Lead ICS/OT Security Consultant - MEA Region, FireEye-Mandiant*

11:40 - 12:00	**Automating the Compliance Process for Industrial Automation and Control Systems** The objective of this talk is to highlight an approach to implementing automated compliance workflows and concepts, for efficiently assessing the security of industrial automation and control systems, against organizational, national, and international policies, procedures, standards, and regulations. Operators are grappling with the increased burden of demonstrating due care as cybersecurity threats continue to broaden with potential impact on plant operations and reliability. This threat has led to the adoption of a multiple series of compliance mandates by operators and regulators, which requires measuring and reporting. The adoption of these requirements and controls for industrial automation and control systems (IACS) has continued to mature. The analysis and measurement of these controls have posed a challenge, with a significant increase in cost, resource allocation, inaccurate reporting, and continuous monitoring challenges. The development and adoption of an automated compliance assessment and reporting framework, helps to significantly reduce the assessment time and effort, eliminate subjectivity in analysis, address the ever-changing governance expectations, respond to the changing risk landscape, and increase frequency of the assessment and reporting lifecycle. The concept of compliance automation for IACS is not a new challenge; however, considerable obstacles exist which have limited adoption of compliance automation. A few of these risks - such as inconsistent information sources, lack of required skills, complexity, stakeholder engagement, and budget - have hindered its broader adoption. When achieved, compliance process automation will provide significant return on investment, and enable agility and resilience in an ever changing threat landscape. *Uduak J. Daniels CISSP, CISM - ICS Cybersecurity Specialist, Saudi Aramco*
12:00 - 13:00	**Lunch Break**
13:00 - 13:30	**Strategies for Defending the Cyber-Physical Battlefield** In this talk, Chief Information Security Officer of the Singapore Land Transport Authority (LTA) and President of the Singapore Computer Society Cybersecurity Chapter, Huang Shao Fei will share his perspectives on the challenges involved with design, operation and risk management of Industrial Control Systems (ICS), and key strategic considerations for defending the cyber-physical battlefield. *Huang Shao Fei* *Chief Information Security Officer, Singapore Land Transport Authority* *President, Singapore Computer Society Cybersecurity Chapter*

13:35 - 13:50	**Good Practices for ICS Supply Chain Risk Management** ICS supply chain risk management cannot be ignored from the perspective of both the threats and compliance in recent years. The big challenge is how you assess the risk of ICS assets in the procurement process. In the session, the good practices from the several industries and the ongoing activities in Japan will be explained after the short introduction of the current landscape of the threat, policy and certification for ICSsupply chain risk management. *Mr. Hiroshi Sasaki - Special Expert at Cyber Tech Lab* *Information-technology Promotion Agency, Japan (IPA)* *Industrial Cybersecurity Security Center of Excellence (ICSCoE)*
13:50 - 14:00	**Break**
14:00 - 14:30	**Is Zero Trust Possible in OT Environments?** Zero trust is a security concept that advocates for constant monitoring and validation to ensure that only authorised users are accessing authorised devices and applications. No one and no devices are trusted by default. In this presentation, Dr Ong Chen Hui will share research findings and reflect upon the challenges they pose to implementing zero trust in OT environment. *Dr. Ong Chen Hui - APJ CTO, Trustwave*
14:35 - 14:50	**Protect Power Plant and Industrial Infrastructure from Cyber Attack! ICS Security Case Study in Japan** In the past, it has been a given that the control systems are isolated from the internet and information systems, instead operated in closed environments, making them safe. However, as systems become increasingly open due to digital transformation(DX), to connect Internet. This mentality regarding control systems has become out of date, and faces cyber threat. This section describes the challenge of how to mitigate ICS cyber risk based on use-case at Power Plant and Industrial Infrastructure in Japan. *Takashi Amano* *General Manager, Cyber Security Center, Toshiba Corporation* *Technology Executive, CISO, Toshiba Digital Solutions Corporation*
14:50 - 15:00	**Break**

15:00 - 15:30	**The Tools Dogma** Often ICS security tools are sold to asset owners as being the holy grail ... but in reality, they give those same asset owners most of the times a false sense of security as they believe they are well protected. Security tools are only a part of the equation to having a good security plan. Human elements, physical security and logical security go hand in hand. Within this presentation, shortcomings of ICS Security tools are mentioned as well as a potential road to an all-encompassing risk assessment approach is shown. It requires very often to take a step back and look at your environment from different angles to understand the bigger picture. Doing so will allow you to enable present ICS security tools and tackle missing elements in other ways. *Dieter Sarrazyn, ICS Security Consultant at Secudea*
15:35 - 15:55	**Bounding Cyber in Design Basis Threat** The emergence of cyberweapons and the convergence of IT and OT, contribute to the exponential growth in the number and sophistication of cyber-attacks, targeting critical infrastructure. The nuclear sector has recognized that it must employ compensating measures in order to ensure its most critical systems can defend, detect, delay, respond, and recover from cyber-attacks. The NRC has included cybersecurity requirements in the Physical Security and Design Basis Threat (DBT) Orders. *Jacob Benjamin, Principal Industrial Consultant, Dragos*
16:00 - 16:30	**Tips and Tricks from the ICS Assessment and Pen-Testers** At this session there will be presented a set of experiences and challenges in the production critical environment we have seen and how to protect these challenges. The session will not present information about asset inventory and segmentation but will e.g. look into how a hacker can exploit and take control and how you can protect against these attacks. The session will also show some information on what you should expect from an ICS pen-tester and some differences between pen-testing IT vs ICS environments. How secure is your production critical environment? *Soren Egede Knudsen, IT/OT Security Expert, Egede* *Mikael Vingaard, Consultant*

16:35 - 17:00	**ICS Attack Concepts and Demonstrations** In this talk we will start with the assumption that corporate business networks are breached and adversaries have discovered a path into your control system network – and then we consider, what are some common attack approaches that adversaries can pursue within a process environment? In this final presentation of the day, we will walk through a lightning round of attack demonstrations targeting local process network communications, logic analysis, and implementing process attacks that leverage ICS devices as both targets and attack delivery nodes – ultimately attacking the control system from within the control system. *Tim Conway, Technical Director - ICS and SCADA programs, SANS Institute* *Jeff Shearer, Industrial Cyber Security Professional, SANS Institute*
17:00	**Closing Remarks and The ICS Asia Pacific 'Difference Maker' Award**

EVENT TIMINGS

Time Zone	Hours
Pacific Time	17:00 - 01:00 PT
Australian Eastern Time	12:00 - 20:00 AEST
Japan Standard Time	10:00 - 18:00 JST
Singapore Time	**09:00 - 17:00 SGT**
Bangkok Time	08:00 - 16:00 ICT
India Standard Time	06:30 - 14:30 IST
Greenwich Mean Time	01:00 - 09:00 GMT
Central European Time	02:00 - 10:00 CET

SPEAKERS

Justin Searle
Summit Chair

Justin Searle is the Director of ICS Security at InGuardians, specializing in ICS security architecture design and penetration testing. Justin led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and has played key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), National Electric Sector Cybersecurity Organization Resources (NESCOR), and Smart Grid Interoperability Panel (SGIP). Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences. Mr. Searle is currently a Senior Instructor for the SANS Institute.

Tim Conway
Technical Director - ICS and SCADA programs, SANS Institute

Tim serves as the Technical Director - ICS and SCADA programs at SANS, and is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. Additionally, performing contract and consulting work in the areas of ICS cybersecurity with a focus on energy environments. A recognized leader in CIP operations, he formerly served as the Director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO) and was responsible for Operations Technology, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric.

Robert M. Lee
Founder & CEO, Dragos

SANS certified instructor Robert M. Lee brings to the classroom one of the most valuable and respected of credentials: real-world experience. Robert is the CEO and founder of his own company, Dragos, Inc., that provides cyber security solutions for industrial control system networks. Consider the 2015 attack on the Ukraine power grid when for the first time in history a power grid went down due to an intentional cyberattack. Robert and a few others formed a specialized team to analyze the event and passed information to the impacted parties as well as the U.S. government and private sector.

Peter Jackson
Engineering Manager (Cyber), SGS ECL

Peter Jackson is an experienced ICS Cyber Security professional. Peter leads the ECL Cyber team of industrial cyber specialists in supporting the industrial sector in NZ. Peter's background includes control and safety systems experience as a TÜV certified Function Safety Engineer. Peter has spoken at many conferences, nationally and internationally. In conjunction with SANS ICS and ECL Cyber, Peter established the NZ ICS Cyber Technical Network as a community of OT Security professionals.

David Koh
Chief Executive,
Cyber Security
Agency of Singapore

Mr David Koh is the Commissioner of Cybersecurity and Chief Executive of the Cyber Security Agency (CSA) of Singapore. As the Commissioner, he has the legal authority to investigate cyber threats and incidents to ensure that essential services are not disrupted in the event of a cyber-attack. Concurrently, as Chief Executive of CSA, he leads Singapore's efforts to provide dedicated and centralised oversight of national cyber security functions. These include enforcing the cybersecurity legislation, strategy and policy development, cyber security operations, ecosystem development, public outreach and international engagement.

Moath Sakaji
MEA Lead ICS/OT
Security Consultant,
FireEye - Mandiant

Moath is an Industrial Control Systems (ICS) security consultant looking after ICS and Operational Technology (OT) security in Middle East and Africa. He started his career as an automation engineer and following Stuxnet he shifted his focus to ICS/OT security. Since then, he has been helping organizations develop and improve their ICS security programs and advising them on defending against advanced cyber attacks targeting critical infrastructure and industrial control systems.

Uduak Daniels
ICS Cybersecurity
Specialist,
Saudi Aramco

Uduak Daniels has over 20 years of experience, 15 working in Cybersecurity. He is currently an ICS Cybersecurity Specialist with Saudi Aramco. His professional exposure has cut across multiple industries in North America and MEA. Uduak has participated in a wide variety of information and operational technology cybersecurity assessments, consultancy, design and deployments. In addition, he has led first responder and offensive security engagements. Uduak is a current member of the International Society of Automation (ISA), vice-chair of the Saudi Aramco ICS Cybersecurity Standards Committee, and a technical member representative for SA at ISCI ISASecure.

Shao Fei Huang
CISO,
Singapore Land
Transport Authority

As Chief Information Security Officer at Singapore's Land Transport Authority (LTA), Shao Fei spearheads the cybersecurity programme across land transport. He is also concurrently Director for Cybersecurity and Director for Data Science, and oversees IT Governance & Strategy at LTA. Prior to joining LTA, Shao Fei had served in various roles at Singapore's Ministry of Home Affairs, Ministry of Defence, Defence Science Organisation National Laboratories, Centre for Strategic Infocomm Technology and the InfoComm Development Authority.

Hiroshi Sasaki
Special Expert,
Cyber Tech Lab

Joined McAfee Japan in December 2012 after working for 14 years as a developer of industrial control system. Aiming to foster culture of industrial cyber security, providing enlightenment such as lectures, writing and consulting services. From May 2016, assigned as a part-time IT Security Officer of Ministry of Economy, Trade and Industry (METI), and from July 2017, assigned as a part-time subject matter expert in the Cyber Technology Laboratory of the Industrial Cyber Security Center of Excellence, supporting the development of the industrial cyber security industry.

Dr Ong Chen Hui
APJ CTO,
Trustwave

With 20 years of experience in cybersecurity and technology innovation, I have proven capabilities in leading diverse teams towards impactful outcomes in deep tech. Today, I am the APJ CTO in the global CTO office in Trustwave - a Singtel company, and I drive the vision, strategy and oversee execution of emerging technologies in our cybersecurity business. Within the Singtel Group, I am also a member of the task force in group-wide strategic projects such as 5G rollout, digital transformation and inorganic growth, i.e. M&A. I represent the company in the Telco Security Alliance and at the World Economic Forum. I am also a member of the committee for TR68: Technical Reference for Autonomous Vehicles and the Cybersecurity Working Group in the 2018 Services and Digital Economy Technology Roadmap.

Takashi Amano
General Manager,
Cyber Security Center,
Toshiba Corporation

He joined Toshiba in 1991. Currently leading research & development for AI and Security technology for Industrial IoT, after leading development for hardware, software and cloud service for consumer products such as Mobile, PC, Tablet and TV. his extensive ICT background and experiences positions him well in leading Toshiba's industrial IoT security strategy and execution, as well as serving as a consultant to smart manufacturing facility security.

Dieter Sarrazyn
ICS Security
Consultant,
Secudea

Dieter is a freelance SCADA/ICS/OT security consultant who's working extensively on industrial control system security since 2008. He performs different kinds of security assessments within industrial environments including intrusion testing, physical penetration testing, technical system assessments, risk assessments and provides assistance in securing these environments. He also helps customers to manage security of solutions deployed by their industrial suppliers and integrators through doing security requirements management and security FAT and SAT tests. Next to assessing environments, he is also providing training and awareness sessions on scada/ics/ot security and coaches young graduates within this field.

Jacob Benjamin
Principal Industrial Consultant, Dragos

Jacob Benjamin is a Principal Industrial Consultant, at the industrial cyber security company Dragos, Inc. Prior to joining Dragos, Dr. Benjamin was a nuclear cybersecurity researcher at Idaho National Laboratory and a nuclear cybersecurity specialist for Duke Energy. Over the last ten years, Jacob has performed a variety of cyber related tasks at many domestic and international critical infrastructures. He has substantial experience developing cybersecurity programs for nuclear power plants as well as performing cybersecurity risk assessments for critical digital assets, systems, and networks within industrial environments. Dr. Benjamin has provided his expertise internationally on behalf of the U.S. Department of Energy, the National Nuclear Security Administration (NNSA), and the International Atomic Energy Agency (IAEA).

Søren Egede Knudsen
IT/OT Security Expert, Egede

Søren Egede Knudsen is a senior cyber security consultant with more than 25 years of experience in IT network and cyber security. Søren started his professional work with IBM 3270 systems in 1991 and IT network and cyber security from 1993. Since 2009, Søren has worked focused in ICS/OT cyber security and are today considered an expert in Cyber security in the ICS/OT environment and have been engaged in many large and complex projects internationally within his fields.

Besides as working as a senior consultant and subject matter expert in ICS/OT Cybersecurity, Søren is an international public speaker at ICS/OT cyber security conferences.

Mikael Vingaard
Consultant

Mikael Vingaard have 20 years of experience within IT-security and have for the last 6 year worked exclusive within securing critical infrastructure.
Mikael works with ICS/SCADA from a practical security point, and are one of the leading experts within the realm of deception technology (aka. honeypots) within industrial environments. Beside holding a number of security certifications; IACRB CSSA (Certified SCADA Security Architect),CISSP, and GIAC; GRID,GICSP - Mikael has been credited for finding and responsible disclosing a number of 0-days to many leading industrial vendors.

Jeff Shearer
Industrial Cyber Security Professional, SANS Institute

Jeff is a member of the SANS Institute ICS team focused on developing courseware in support of the ICS curriculum. Jeffrey also acted as a Subject Matter Expert (SME) for the Global Industrial Cyber Security Professional (GICSP) certification and is a content contributor for ICS Netwars. He also participates as an advisory board member for the ICS Security Summit and Training events. Prior to joining SANS Institute, Jeff worked at Rockwell Automation for twenty-three years where his most recent role was a Sr. Security Architect for Rockwell Automation's Commercial Engineering group focused on network and security designs for Industrial Automation Control Systems (IACS) and Industrial Demilitarized Zones (IDMZ).