Asia Pacific ICS Security

SUMMIT

PROGRAM GUIDE

Chairman – Mike Assante

Agenda

All Summit Sessions will be held in the Galleria Ballroom, Level 3 (unless noted).

All approved presentations will be available online following the Summit at ***https://files.sans.org/summits/icsapac13****.*

An e-mail will be sent out following the summit once the presentations are available online.

Monday, 2 December

8:00-9:00

Registration & Coffee

9:00-9:45

A Community Approach to Securing the Cyberspace to Enhance National Resilience

In today's dynamic environment and a connected landscape, people's data usage behavior has changed significantly from desktop to mobile as well as moving data and information into the Cloud. There is also a shift of mindset in-terms of national infrastructure protection. The need for secure, private, and reliable services is growing from a technological concern within the industry to a societal concern for citizens around the world. The topic will discuss how cyber-security professionals have the potential to align the social, economic, political and technical concerns in the cyberspace towards a more secure and resilient platform.

Alan Seow*, MSc (InfoSec), CISSP, CRISC, Cyber-Security Practitioner*

9:45-10:30

The Good, Bad and the Ugly: Certification of People, Processes and Devices

The industrial security industry has been slow to adopt certification, but the last few years have seen a growing increase in the momentum in this area. There are now certification schemes in place or being developed that can cover people, processes and devices/systems. This presentation will cover all of these schemes; compare them to certifications in other areas such as safety, and provide an in-depth analysis of the good, bad and ugly aspects of them. In addition, it will look at how these schemes are (or are not!) improving security in the industrial control arena.

Graham Speake, *Security Architect, Evangelist, Yokogawa*

10:30-10:50

Networking Break & Vendor Expo

10:50-11:20

Innovation in Industrial Perimeter Security

Would you connect your control system servers directly to the Internet with a firewall protecting them? Many critical infrastructure sites do so - and suffer the consequences. IT/OT integration is proceeding apace in most industries, with up to two layers of firewalls separating IT networks from operations networks. This network architecture turns corporate domain controllers and other shared infrastructure into single points of failure for all industrial sites in the enterprise - not from a reliability point of view, but from a cyber-sabotage point of view. The more industrial practitioners learn about network security, the less they trust firewalls. Until recently though, there were no practical alternatives to firewalls.

In this session we will review new and innovative technologies, stronger than firewalls, which are now available.

Lior Frenkel*, CEO and Co-Founder, Waterfall Security Solutions Ltd.*

11:20-Noon

Supply Side: Perspective on Progress and Challenges

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.

Moderator: ***Michael J. Assante****, Director – ICS & SCADA, SANS Institute*

Panelists: ***Markus Braendle****, Group Head of Cyber Security, ABB*
Tim Harwood*, Director, HS&T Consultancy*
Graham Speake*, Security Architect, Evangelist, Yokogawa*

Noon-12:45

The Operator as a Human Sensor

Team members are the first line of defence in keeping ICS environments secure. But to be able to spot possible anomalies and potential unauthorized access, staffers must thoroughly understand what the environment looks like when it's functioning normally. Learn strategies and best practices for bringing your ICS team up to speed so that they can function as Human Sensors.

Tim Harwood*, Director, HS&T Consultancy*

12:45-13:45

Lunch
Sponsored by

13:45-14:45

SCADA Security Assessment Methodology: The Malaysia Experience

With the outbreak of Stuxnet virus to SCADA systems in Iran and worldwide, it is important to have a methodology on how to do an assessment on a SCADA system. Supervisory Control and Data Acquisition (SCADA) is a system that controls industrials systems from nuclear power plants to traffic lights.

In this presentation we shall provide insight on how to do the assessment, provide the do's and don'ts, tools are being used and how to prepared for the assessment. We shall share our experiences from our previous assessment that had been done in Malaysia which includes the oils and gas sectors, transportation, and waterworks. SCADA engineers, security auditors and business owners shall be able to assessed their system in a truly and secure manner in order to find common security threats that may exist in their SCADA systems.

Muhammad Reza Shariff*, Senior Analyst, CyberSecurity Malaysia*

14:45-15:30

10 Steps on the Road to a Successful Cyber Security Program

The complexity of cyber security is constantly increasing, requiring organizations to build cyber security programs that address the evolving challenges in a holistic, effective and sustainable way. This presentation will discuss 10 ingredients that are key factors in the success of a cyber security program and should be of highest importance to any stakeholder.

Markus Braendle*, Group Head of Cyber Security, ABB*

15:30-15:50

Networking Break & Vendor Expo

15:50-16:50

The State of Critical Control System Security in Japan

In Japan, the special organization called CSSC (Control System Security Center), established by Ministry of Economy, Trade and Industry has just started their actions for control systems like SCADA. Also, most of all the utility organizations are drawing up their security policies and assessing the risks for their control system.

In this session, we introduce the current situations of critical control system security in Japan, and consider the forecast for the relationship between the nations, especially ASEAN countries.

***Daisuke Noguchi**, Security Consultant, NRI SecureTechnologies, Ltd.*

16:50-17:30

ICS Security Innovation

Automation continues to expand at a rapid pace. The time for security innovation is now. End users, suppliers, and integrators are seeking common ground to deliver solutions that are safe and reliable. I will discuss the important building blocks to achieve security innovation across the ICS value chain.

***Michael J. Assante**, Director – ICS & SCADA, SANS Institute*

17:30-19:30

Welcome Reception

Hosted by

CODENOMICON

Please join your fellow attendees for a chance to mingle with other attendees and enjoy refreshments.

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

Tuesday, 3 December

8:00-9:00

Registration & Coffee

9:00-9:45

Dream Team: Building the Perfect ICS Team

Protecting our ICS systems is not a one-person job. It takes a team. So how do you build the perfect team? Who should be part of the team? What experience and training do they need? How do you keep their skills current? How do you define the roles and functions of each team member? Learn firsthand from a leader who has built ICS teams about what works – and what doesn't.

***Tyler Williams**, Industrial Cyber Security Solutions Manager, Global Oil and Gas Company*

9:45-10:45

Smart Security : Strengthening Information Protection in Your ICS

Though similar Information and Communication Technologies (ICT) are adopted, when it comes to information protection priorities, the IT world is very different from the Industrial Control Systems (ICS) world where human safety and system reliability are the top concerns. To achieve information protection in an ICS environment, there are many challenges. There is no silver bullet or one size fits all solution. This presentation will cover ways to tackle these challenges systematically.

***Charles Liang** CISSP-ISSMP, CSSLP, CISM, CISA, CGEIT, CRISC, CEH IT Security Policy Manager – Cyber Security, CLP Power Hong Kong Limited*

10:45-11:00

Networking Break & Vendor Expo

11:00-Noon

Cyber Security Features We Need in Next Generation PLCs and RTUs

This presentation compares and contrasts the security features that we take for granted in IT computer hardware (workstations, servers, and network devices), and examines how several basic cyber security features are not currently supported in PLCs, RTUs, and Field Devices. The talk covers an in-depth discussion of security features that the ICS industry would like to see in the next generation PLCs and RTUs, including:

- Authentication
- Encrypted sessions
- Monitoring capabilities
- Forensics
- Services customization

***Jonathan Pollet**, CAP, CISSP, PCIP, Founder & Principal Consultant, Red Tiger Security, LLC*

Noon-13:30

Lunch
Provided by

SANS

13:30-14:15

Leading a 24/7 IT Security Team: When a SOC is more than a SOC

Responding effectively to incidents and remaining proactive requires More Than basic monitoring for the Aramco Overseas Security Operations Center (SOC). As part of the Saudi Aramco family, the Aramco Overseas network is globally dispersed in some very far-flung and challenging locations with a small team of passionate, holistic security analysts. Offering diverse services as perimeter, log and network event monitoring, web application testing, vulnerability management, end point protection, in-depth penetration testing, social engineering exercises, private computer emergency response team, forensics analysis, smartphone and mobile security device management, business analysis with security focus, reverse engineering and lastly a network operations center. A presentation on the strategies utilized regarding the unique challenges of monitoring a very de-centralized network with unique risks whilst positively challenging and continuously developing the team to ensure a safer business environment.

***Christina Kubecka**, Security Operations Center Supervisor, Aramco Overseas*

14:15-15:00

A Compass for the Compliance World

With the growing confusion in North America over the NERC CIP Standards, the FERC Interpretation orders, the potential overlap from the United States Executive Order, and a number of other international Standards activities (ISA99/IEC 62443 and Qatar ICS Standard) that will add to the confusion for vendors manufacturing products in multiple markets; this presentation will provide background and guidance on the Standards in effect and what organizations will need to be prepared for in the future.

***Tim Conway**, Technical Director of ICS & SCADA Programs, SANS Institute*

15:00-15:20

Networking Break & Vendor Expo

15:20-16:15

ICS Attack Surfaces

In today's age, our ICS systems make up the majority of most nations' critical infrastructure. And where it isn't critical infrastructure, our ICS systems often make up the backbone of each nation's manufacturing effort and play a critical part of each nation's gross wealth. Because of this, there are plenty of reasons for malicious actors to attack our ICS systems. This could be launched by individual or organizations for the purpose of financial gain (or ruin), corporate espionage, hacktivism, or terrorist activities. Information warfare is also of grave concern since many nations are now actively involved in cyber espionage and preparation for cyber warfare, And our last group of people that always must be considered are the countless numbers of individuals that like trying to attack organizations to test themselves, enhance their education and gain recognition from their peers. In order to protect a system, you must understand how the attack works. In this webcast, we will look at the various ICS attack surfaces and ways organizations can defend against them.

***Dr. Eric Cole**, Fellow, SANS Institute*

16:15-17:00

Going Global: Global ICS Professional Certification

Cyber security threats continue to increase in both frequency and sophistication. Industries getting more automated, integrated, and interconnected, are facing a real challenge. People are crucial. A standardized foundational set of skills, knowledge, and abilities for ICS across industries was lacking, until now. In this talk you will learn all about the new Global ICS Professional security certification.

- The GICSP is a new certification that focuses on the foundational knowledge that professionals securing critical infrastructure assets should know.
- Holders of the GICSP will demonstrate a globally recognized level of competence that defines the architecture, design, management, risk and controls that assure the security of critical infrastructure.
- The GICSP is the "bridge" to bring together IT, engineering and cybersecurity professionals to achieve security for ICS from design through retirement.
- The GICSP is expected to be adopted on a global basis as a gateway certification for critical infrastructure-industrial control system professionals.

The approach to create this certification program was an industry driven effort, including end-users, ICS suppliers, and subject matter experts.

Moderator: ***Michael J. Assante****, Director – ICS & SCADA, SANS Institute*

Panelists: ***Markus Braendle****, Group Head of Cyber Security, ABB*
Tim Conway*, Technical Director of ICS & SCADA Programs, SANS Institute*
Graham Speake*, Security Architect, Evangelist, Yokogawa*
Tyler Williams*, Global Oil & Gas Company*

Thank you for attending the SANS Summit.

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

Exhibitors

Codenomicon

Codenomicon's fully automated Defensics testing solutions enable you to find zero-day vulnerabilities in over 200 protocols and file formats, including ICS, SCADA and standard Internet protocols. Codenomicon Defensics complies with the Embedded Device Security Assurance (EDSA) Communications Robustness Testing (CRT) requirements of the ISA Security Compliance Institute (ISCI).

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.

Waterfall's Expanded Mission: Stronger than Firewalls

For most of a decade Unidirectional Security Gateways® have enabled secure IT/OT integration and secured the safety and reliability of critical control system networks. Today Waterfall announces an expansion of our mission in the form of three new kinds of technologies: all of them stronger than firewalls.

Waterfall for BES Control Centers is being deployed at a North American Balancing Authority and has two independent unidirectional channels, each replicating ICCP servers. One channel is oriented inward into the Control Center and one is outward.

Waterfall FLIP™ temporarily reverses gateway orientation under the control of the protected network, to allow occasional external inputs, such as production plans and equipment control schedules. Waterfall FLIP™ for Substations applies the FLIP™ technology to the problem of securing DNP3 communications and transmission substations.

The new Waterfall modular architecture reduces rack-space requirements, and allows end-user replacement and expansion of Unidirectional Gateway equipment. New TX and RX modules are still obviously self-contained and so easily certified as free of covert channels.

Waterfall® for BES Control Centers: secure ICCP

Waterfall FLIP™

Waterfall FLIP™ for Substations

New Modular architecture

Secure IT/OT Integration with Unidirectional Security Gateways

A new mission for a new threat environment: replace control system firewalls with stronger solutions

WATERFALL®
Stronger Than Firewalls

www.waterfall-security.com

Global Industrial Cyber Security Professional (GICSP)

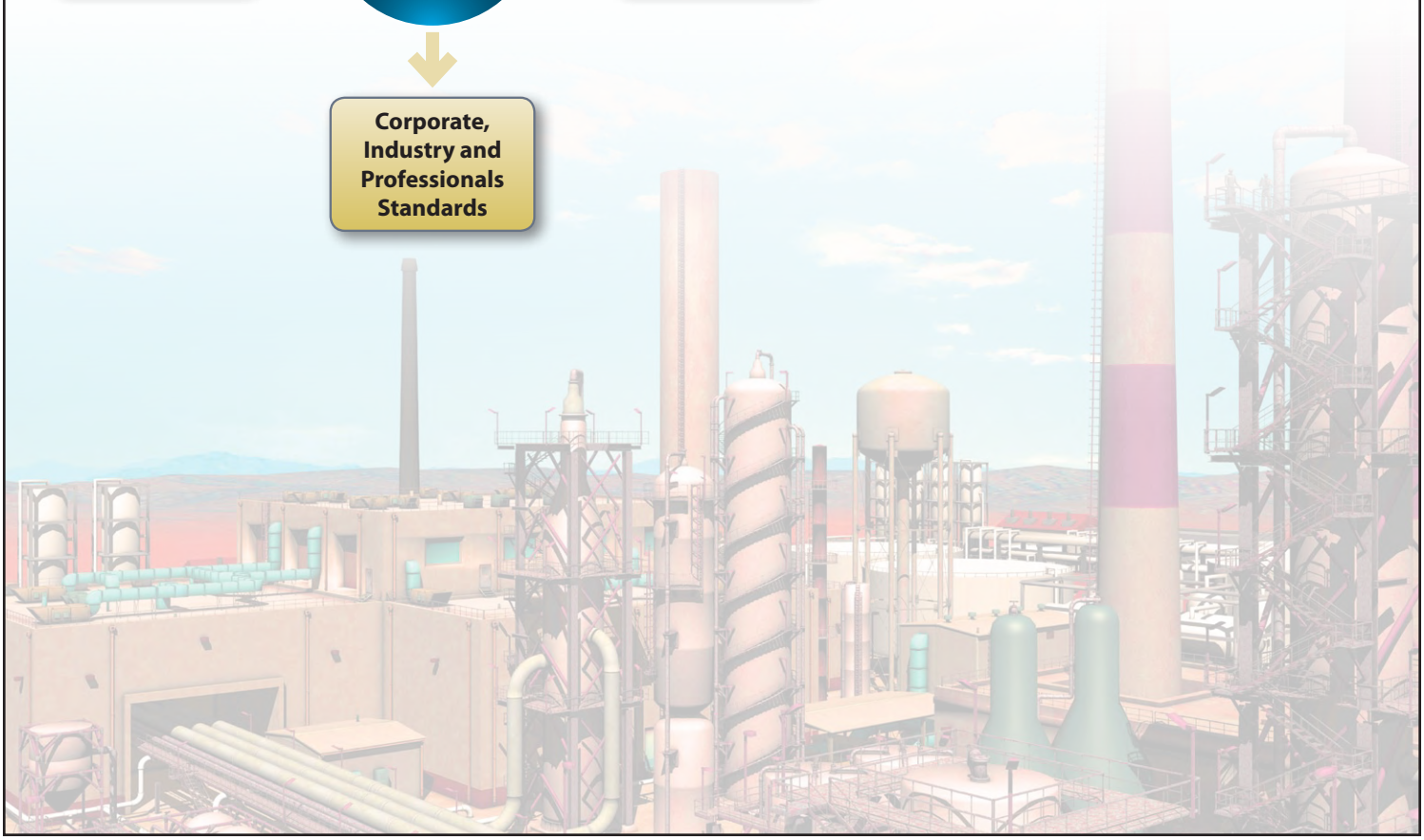
The **GICSP** is the newest certification in the GIAC family and focuses on the foundational knowledge of securing critical infrastructure assets. The **GICSP** bridges together IT, engineering and cybersecurity to achieve security for industrial control systems from design through retirement.

This unique vendor-neutral, practitioner focused industrial control system certification is a collaborative effort between GIAC and representatives from a global industry consortium involving organizations that design, deploy, operate and/or maintain industrial automation and control system infrastructure. **GICSP** will assess a base level of knowledge and understanding across a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments.

This certification will be leveraged across industries to ensure a minimum set of knowledge and capabilities that IT, Engineer, and Security professionals should know if they are in a role that could impact the cybersecurity of an ICS environment.

Industries that are helping to develop and shape this certification include:

- **Oil and Gas**
- **Utilities (Power, Water and related)**
- **Manufacturing**
- **OEM**
- **Information Technology**



The Importance of the GICSP Certification

Warnings about attacks to critical infrastructure have been circulating for years, but real threats have been identified and have had an identifiable impact on critical infrastructure assets and systems. Vital infrastructures, such as power utilities and the oil and gas industry must be able to protect and defend their systems to maintain the safety of workers and well being of customers and communities they serve.

GICSP certification holders will demonstrate a globally recognized level of competence that defines the architecture, design, management, risk and controls that assure the security of critical infrastructure. Below we have highlighted the Certification Objectives as determined industry and subject matter experts:

GICSP Certification Objectives

- **ICS Architecture**
- **ICS Security Assessments**
- **Industrial Control Systems**
- **ICS Modules and Elements Hardening**
- **Cybersecurity Essentials for ICS**
- **Configuration/Change Management**
- **ICS Security Governance and Risk Management**

For a complete list of GICSP certification objectives, visit www.giac.org

Certifications Exam Details

The **GICSP** exam consists of 115 questions and has a time limit of three hours.

How to Register for Certification Exam Attempt

The **GICSP** is open for pre-registration.

To register, go to **www.giac.org**

*The **GICSP** examination is expected to be available for testing in November 2013.*

First Things First

The Top 4 Security Mitigation Strategies

Speaker: Dr. Eric Cole, SANS Faculty Fellow

Thursday, December 5

REGISTRATION: 17:45-18:30 PRESENTATION: 18:30-19:30

Organizations are struggling with cyber security. It seems the more money that is spent, there is an equal increase in attack vectors. While new technologies will help, it is important to focus in on the core areas that will make the biggest impact. These areas need to be aligned with how an adversary breaks into a system.

Targeted intrusions of a computer network can be broken down into three stages, these are:

Stage 1: Code Execution is where an adversary attempts to gain an initial foothold into a computer network. This is typically done by delivering a socially engineered email to a staff member within the organisation containing a malicious attachment or link. If the user opens this link the adversaries malicious code will execute on the endpoint and provide this foothold.

Stage 2: Network Propagation is where an adversary uses this network foothold to spread to other locations inside the compromised computer network. In this stage they are typically looking to gain additional access to multiple internal systems and create reliable methods of accessing these systems in the future, this is also known as gaining persistence.

Stage 3: Data Exfiltration is where an adversary has located data of interest and removes this data from a corporate network.

The Top 4 Mitigation strategies provide coverage across all three stages of the intrusion process and an effective way to implement effective security. According to DSD While no single strategy can prevent malicious activity, the effectiveness of implementing the Top 4 Strategies remains very high. At least 85% of the intrusion techniques that ASD responds to involve adversaries using unsophisticated techniques that would have been mitigated by implementing the Top 4 mitigation strategies as a package. In this webcast learn about how attack vectors work and ways the Top 4 can defend against them.

SANS Industrial Control Systems

ICS Security 2014 Training Events

ICS Security Summit
March 12-18 | Orlando, FL

SANSFIRE
June 23-27 | Baltimore, MD

ICS Training
July | Houston, TX

Network Security
October 20-24 | Las Vegas, NV

Follow us
@SANSICS

More information at
www.sans.org/industrial-control-systems