December 2017

Industrial Control Systems Joint Working Group (ICSJWG) Quarterly Newsletter

— ICSJWG EXPANDING THE COMMUNITY —

Upcoming Events

- January 24, 2018: ICSJWG Webinar Series "Life After Ukraine: Industrial Control System Cybersecurity Industry Trends and Strategies" **2:00 pm (EST)**
- January 8–12; January 22–26; February 5–9: Industrial Control Systems Cybersecurity (301) Training Idaho Falls, Idaho **Registration for these respective trainings: *closed***
- March 5–9; March 19–23: Industrial Control Systems Cybersecurity (301) Training Idaho Falls, Idaho **Registration for these respective trainings: *open***
- April 10–12: ICSJWG 2018 Spring Meeting Albuquerque, NM

ICS-CERT Resources

Training Resources
Incident Reporting
Assessments
CSET®
Alerts & Advisories
HSIN
Latest Monitor

Thank you to everyone who submitted content for this newsletter. ICSJWG relies on members like you for our Newsletter, Meetings, and Webinars. Content and opinions are those of the authors and do not represent DHS opinions, endorsements, linguistic styles, or recommendations.

Upcoming ICSJWG 2018 Spring Meeting

As a reminder, the 2018 Spring Industrial Control Systems Joint Working Group (ICSJWG) Meeting will occur April 10–12, 2018, in Albuquerque, New Mexico! We hope you will join us this spring, and we anticipate a large and diverse group of stakeholders to be in attendance.

The ICSJWG team has provided more information for the upcoming Meeting on the ICSJWG web site: https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG. In the meantime, as always, if you have any questions, feel free to send us an email at ICSJWG.Communications@hq.dhs.gov.

On the web site, you will soon find logistical, background, and preparatory information on various components of the Meeting, including the Call for Abstracts. We encourage membership to ultimately submit abstracts for consideration, which will be due by February 23, 2018, and reviewed by ICSJWG Program Management and the ICSJWG Steering Team. Please review the Call for Abstracts, upon its forthcoming release, for full details on abstract submission.

Continuing the ICSJWG Webinar Series

The October 2017 Webinar, "Creating Predictable Fail Safe Conditions for Healthcare Facility-Related Control Systems and Medical Devices by Use of System Segmentation," presented by Michael Schroeder, Director of Programs at 3 Territory Solutions, was well-received with roughly 40 participants present for the session.

We look to continue the success of our Webinars, and are excited to announce the next installment in our series! On January 24, 2018, Brian Proctor (GICSP, CISSP, CRISC) of SecurityMatters, will present "Life After Ukraine: Industrial Control System Cybersecurity Industry Trends and Strategies." The Webinar will commence at 2:00 pm (EST). We are expecting a significant turnout for this session, so please note that at this time, there are a limited number of lines for registration remaining.

If you are interested in joining this session, please email us at ICSJWG.Communications@hq.dhs.gov.

Generally, if you have a topic you would like to share with the ICSJWG community, please consider presenting an ICSJWG-hosted Webinar. For more information, please reach out to the same email address above. The next Webinar is tentatively planned for March 2018; we will inform membership of any changes to this timeframe.

Contributed Content Disclaimer: *The advice and instructions provided in the contributed content are specified as is with no warranties and should be confirmed and tested prior to implementation.*

Industrial Control Threat Intelligence

By: Sergio Caltagirone, Director, Threat Intelligence, Dragos

Modern network and asset defense require far greater visibility into the industrial control system threat landscape than in years past. The threat environment is highly dynamic, and adversaries who invest in the problem are outpacing defenders who do not. Threat intelligence is knowledge of adversaries and their malicious behaviors through which defenders gain better visibility. Threat Intelligence reduces harm by improving decision making before, during, and after cybersecurity incidents reducing operational mean time to recovery, reducing adversary dwell time, and enabling root cause analysis. It is a necessary component of any modern cybersecurity program that significantly improves the efficacy of all existing elements.

However, there is no "universal" threat intelligence product, so, organizations must match threat intelligence products to their threat profile. To continue reading, click here.

The Top 20 Cyber Attacks Against Industrial Control Systems

By: Andrew Ginter, VP Industrial Security, Waterfall Security Solutions

No industrial operation is free of risk, and different industrial enterprises may legitimately have different "appetites" for certain types of risks. Evaluating cyber risk in Industrial Control System (ICS) networks though, is difficult - for example, such evaluations can result in considering explicitly or implicitly up to hundreds of millions of branches of a complex attack tree modelling the interaction of cyber attacks with cyber, physical, safety and protection equipment and processes. Communicating the results of such risk assessments to business decision- makers who are not versed in cyber-physical risk- assessment techniques can be even more difficult. To continue reading, click here.

Utilities Need a Cyber Range for ICS

By: Daniel Ehrenreich, Consultant and Lecturer, SCCE

Upgrading the cyber security for Industrial Control Systems (ICS) serving Electricity, Water and other utilities is no long a question of "if" but rather how and when it shall be done. Cyber security experts clearly say, that enhanced defense can be achieved by combining the three PPT factors; People, Policies/Procedures and Technology. Knowing these facts, you realize that completely outsourcing cyber security related tasks is impossible and not effective. In order achieving the target goals outlined in variety of regulations such as NIST 800-xx, NERC-CIP, ISO 2700x and Best Practice guidelines, you must develop these capabilities and outsource only the mentors and trainers. Having an in-house cyber range will help you with critical tasks such as: a) training your team on operating an ICS similar to your ICS, b) effective practicing on ICS related cyber-attacks, c) testing software programs prior deployment, etc. To continue reading, click here.