INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

QUARTERLY NEWSLETTER

ICSJWG EXPANDING THE COMMUNITY

CISA CYBER+INFRASTRUCTURE

April 2020

Upcoming Events

Industrial Control Systems Cybersecurity (301) Training in Idaho Falls, Idaho

Next open training session
Jul 3 – 10, 2020
Jul 13 – 17, 2020
Jul 20 – 24, 2020
Aug 3 – 7, 2020
Sep 14 – 18, 2020

Training is scheduled for each month throughout the year. Registration for each training session opens about 90 days before the session's scheduled start date.

CISA Resources

COVID-19
Training Resources
Incident Reporting
Assessments
CSET®
Alerts & Advisories
HSIN
Information Products

CISA Service Menus
Federal Government
Private Industry
State-Local-Tribal-Territorial
International Partners

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.

UPDATE! ICSJWG Spring 2020 Virtual Meeting

Over the past several weeks, the IST has been closely monitoring and evaluating the situation around COVID-19 to ensure we are taking the necessary measures to protect the health and wellbeing of ICSJWG attendees. As a result, we made the difficult, but necessary, decision to cancel the ICSJWG Spring 2020 meeting in Salt Lake City, Utah.

Instead, we will hold a Virtual ICSJWG Spring Meeting on June 9–10, 2020. We are excited about the agenda for the virtual meeting, which includes a Keynote by CISA Director Christopher Krebs. June 9 will provide a full day of presentations while June 10 will provide virtual components of the very popular Technical Workshop and a kickoff ICS Training overview session for foundational and advanced training. The training is scheduled to occur during June and July. Detailed information and registration for the meeting and for the training sessions will be provided when it becomes available.

We would like to thank the members of the ICSJWG Community for your patience and understanding.

Up-to-Date Information about the Nationwide Medical Crisis

You can find up-to-date information, releases, and updates regarding COVID-19 at www.CISA.gov/coronavirus. These include:

- The CDC has guidance for discontinuation of isolation for persons with non-test confirmed COVID-19 in a non- healthcare setting. Persons with COVID-19 who have symptoms and were directed to care for themselves at home may discontinue isolation under the following conditions: (1) At least three days (72 hours) have passed since recovery, defined as resolution of fever without the use of fever-reducing medications; (2) Improvement in respiratory symptoms (e.g., cough, shortness of breath); and (3) At least seven days have passed since symptoms first appeared.
- The UK and CISA published a joint advisory on cybercriminals and advanced persistent threat groups targeting individuals and organizations with a range of ransomware and malware; the assessment includes indicators or compromise and guidance on how to decrease the risk of cyber-attacks.
- A Frequently Referenced Contact Information section to advertise the various avenues to access information, including previous recordings of the Tuesday/Thursday CISA ESF 14 Broad Stakeholder calls.
- FEMA created a Rumor Control page to provide ground truth on rumors and facts at https://www.fema.gov/coronavirus-rumor-control.

DHS Telework Guidance "Protection of Remote Technologies in a Telework Environment"

CISA, the FBI, and other federal entities have released various articles to help workers who are currently working from alternative spaces as a result of the COVID-19 pandemic and consequential stay-at-home orders. Alternative technological methods are being accessed by new users who may be unaware of some of the vulnerabilities and limitations of these solutions. Two current sources of information include the CISA TIC Interim Guidance, the CISA Trusted Internet Connections page, and a warning from the Federal Bureau of investigation (FBI) about teleconferencing and online classroom hijacking.

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.*

A National Approach to Control Systems

By: CISA ICS Strategic Initiative

In June of 2019, the National Security Council (NSC) tasked CISA to lead coordination efforts to develop an operational and strategic foundation for a national strategy to improve cybersecurity for control systems (CS). As a result, the Control Systems Interagency Working Group (CSIWG) was established to enable a whole of government approach in the development of this strategy. The CSIWG is working to develop partnerships across government and the private sector and is committed to improving cybersecurity for control systems.

The CSIWG is building on previous government and industry efforts to define its four focus areas: workforce development, supply chain risk management, standards and best practices, and incident management. In December 2019, the CSIWG held its first Industry Engagement Forum. The objective of the forum was to discuss potential solutions and collaboration avenues for both government and private sector to address cross ICS-community issues. The CSIWG hosted a second forum in March 2020 to continue to build on this work and flesh out tangible areas for coordination.

The CSIWG is standing up subgroups focused in each area, which will concentrate on scoping and implementation of projects to help the control systems community be more secure against current and emerging threats and looks forward to continuing to partner with the community.

A Retrospective on the First Two Decades of Control System Cyber Security – Culture Issues Still Prevent Successfully Securing Control Systems

By: Joe Weiss, PE, CISM, CRISC, Managing Partner Applied Control Solutions, Managing Director, ISA99

Control system cyber security was, and should be, about protecting the control system process. That is, keeping lights on, water flowing, pipelines from rupturing, etc. We're now at the end of the second decade of control system cyber security and it has changed from protecting the process to protecting the networks - they are not the same. Because there are so few control system suppliers and they supply essentially all industries globally, control system cyber security applies to electric, water/wastewater, oil/gas, manufacturing, transportation, medical devices, facilities (buildings), etc. Given so much misinformation floating around the Internet about control system cyber security, I thought it might be a good time for a control system cyber security retrospective that could provide a basis for assessing how valid the experts' prognostications for 2020 might turn out to be.
Continue to "A Retrospective" article…

Structuring the Cyber Defense for Industrial Organizations

By: Daniel Ehrenreich, Consultant and Lecturer, SCCE
Deployment of cyber defense for Industrial Control Systems (ICS) is a role for experts who acquired in-depth understanding on SCADA-ICS-IIoT technologies. This is highly important due to the principal differences among cyber defense methods for IT, security surveillance and ICS architectures. While IT systems are built to assure Confidentiality, Integrity and Availability (CIA), ICS operations must assure the Safety and Reliability and Productivity (SRP) of the controlled facilities.

We all know, that the recent cyber-attacks occurred worldwide were supported by well-organized, and politically motivated organizations. They usually hire expert attackers who are capable infecting computers and control systems and shutting down industrial facilities. The goal of this paper is to demonstrate integrated SIEM-SOC architecture for protecting industrial organizations.
Continue to "Structuring the Cyber Defense" article…