1. Industrial Control Systems security feed

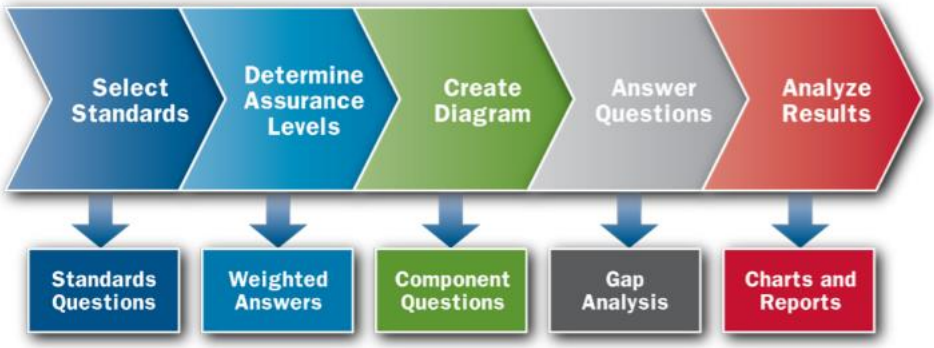
Black Cell is committed for the security of Industrial Control Systems (ICS) and Critical Infrastructure, therefore we are publishing a monthly security feed. This document gives useful information and good practices to the ICS and critical infrastructure operators, furthermore provides information on vulnerabilities, trainings, conferences, books, and incidents on the subject of ICS security. Black Cell provides recommendations and solutions to establish a resilient and robust ICS security system in the organization. If you're interested in ICS security, feel free to contact our experts at cara@blackcell.hu.

List of Contents

ICS good practices, recommendations

Cyber Security Evaluation Tool (CSET)

ICS CERT (*under the Department of Homeland Security*) developed a tool, what could help to identify the maturity level of the IT and OT systems, and provides different compliance recommendations and standards, for example: NIST SP 800-53 r4 and NIST SP 800-82 r2.



The figure above shows the process that helps to determine the level of maturity. The user should select the relevant standards or recommendations, to achieve compliance. CSET provides a list of recommendations in order of priority, and a necessary to-do list, in order to achieve compliance for the organization.

Benefits of using CSET:

- Supports the organizational risk management, and decision making.
- Increases the information security awareness, and fundamental to IT and ICS related dialogues.
- Shows the systems' vulnerabilities, and provides recommendations to mitigate the risks.
- Gives a focus to the strengths and shows the organizational good practices.
- Provides a methodology to ensure monitoring and compliance.
- Evaluates the organizational IT/OT/ICS systems with a holistic approach.

CSET is available to download from GitHub on the following link:

https://github.com/cisagov/cset/releases

More detailed information about the CSET is available on the following links:

https://www.us-cert.gov/ics/Assessments

https://www.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_CSET_S508C.pdf

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in June 2020:

SANS provides online ICS security courses due to the COVID-19 pandemic situation.

The details of the trainings and courses are available on the following link:

https://www.sans.org/course/ics-scada-cyber-security-essentials#results

Periodic online courses:

The Coursera (https://www.coursera.org/) website provides an opportunity to take advantage of online trainings regarding ICS security. The trainings provide video instructions, and the candidates could demonstrate their knowledge in the field of ICS and IoT security. After the course, the University of Colorado, Boulder issues a certificate to the graduates. the following courses are available:

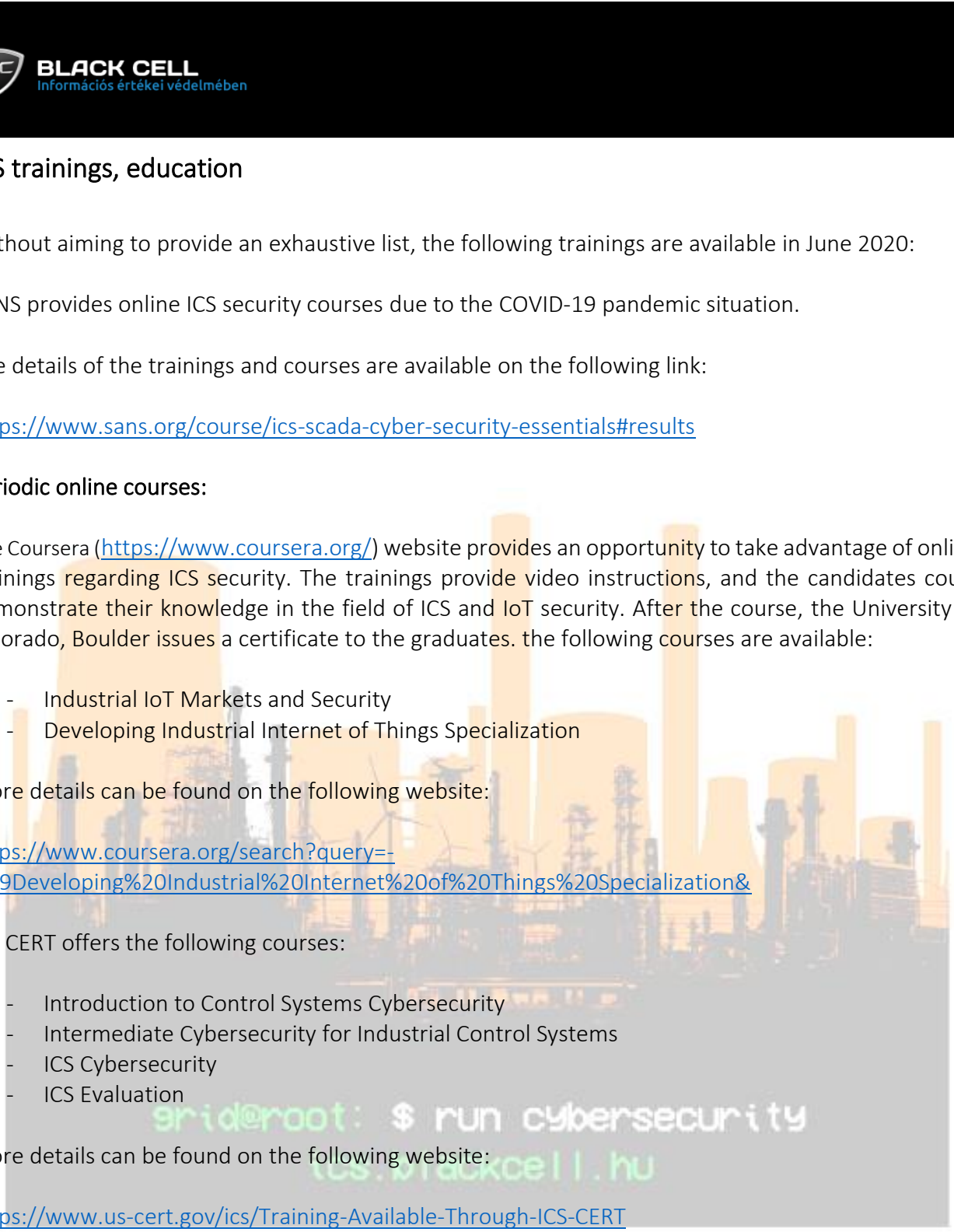
- Industrial IoT Markets and Security
- Developing Industrial Internet of Things Specialization

More details can be found on the following website:

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

ICS CERT offers the following courses:

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems
- ICS Cybersecurity
- ICS Evaluation



More details can be found on the following website:

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

ICS-CERT Virtual Learning Portal (VLP) provides the following short courses:

- Operational Security (OPSEC) for Control Systems (100W) - 1 hour
- Differences in Deployments of ICS (210W-1) – 1.5 hours
- Influence of Common IT Components on ICS (210W-2) – 1.5 hours
- Common ICS Components (210W-3) – 1.5 hours
- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
- Cybersecurity Risk (210W-5) – 1.5 hours
- Current Trends (Threat) (210W-6) – 1.5 hours
- Current Trends (Vulnerabilities) (210W-7) – 1.5 hours
- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours

- Attack Methodologies in IT & ICS (210W-9) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS (210W-10) – 1.5 hours

VLP courses are available on the same website, like the other ICS-CERT courses.

SANS online courses in the field of ICS security:

- ICS410: ICS/SCADA Security Essentials

More details can be found on the following website:

https://www.sans.org/find-training-beta/search?courses=2762&types=10&redirect=beta#__utma=195150004.1547647064.1563952209.1566466056.1568274011.4&__utmb=195150004.2.9.1568274014545&__utmc=195150004&__utmx=-&__utmz=195150004.1568274011.4.3.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)&__utmv=-&__utmk=17428089

Udemy provides online courses in ICS and SCADA security. From the basics of ICS and SCADA security principles to the technological solutions and governance questions, the below course could help to understand the essence of the ICS/SCADA security.

- ICS/SCADA Cyber Security

More details can be found on the following website:

https://www.udemy.com/ics-scada-cyber-security/

The Department of Homeland Security's two days training is useful for the ICS/SCADA operators:

- SCADA security training

The courses are available live online.

More details can be found on the following website:

https://www.tonex.com/training-courses/scada-security-training/

SCADAhacker-com website provides ICS security online courses:

- Understanding, Assessing and Securing Industrial Control Systems

The training takes 40-120 hours, and 8 modules can help to understand the ICS cybersecurity issues. The training focuses on the „Blue teaming" activities, for ICS and SCADA systems.

If you have a certificate, like CISSP, CEH, the course can help to add some ICS and SCADA specific knowledge.

More details can be found on the following website:

https://scadahacker.com/training.html

If you want to be a certified SCADA security architect, the "*ICS and SCADA Systems Security Essentials Training*" is the best choice for you. This online course help the candidates to train for the exams.

This course starts with the basic principles of ICS and SCADA systems, shows the vulnerabilities, risk assessment focus points, security control implementations, server and network security solutions, and the policy and strategy essentials.

The courses are available 0-3- or 4-12-month length timeframes, on demand.

More details can be found on the following website:

https://www.enosecurity.com/training-tutorials-courses/ics-scada-security-essentials-training/

INFOSEC-Flex SCADA/ICS Security Training Boot Camp gives the possibility for ICS/SCADA operators to get ready for external and internal threats.

The 4 days course guarantees the "Certified SCADA Security Architect" certification for the candidates.

The basics of the ICS/SCADA security, governance, security controls, penetration testing and other topics can help the participants to become an ICS/SCADA security expert.

More details can be found on the following website:

https://www.infosecinstitute.com/courses/scada-security-boot-camp/

ICS conferences

In June 2020, in light of the COVID-19 pandemic, many ICS and SCADA security conferences and workshops are either cancelled or postponed to a later date. The following conferences are held in virtual (not comprehensive):

Industrial Control Systems (ICS) Cyber Security Conference

In SecurityWeek's ICS cyber security conference, the participants can learn more about the latest ICS security incidents, participate in their analysis, and research solutions.

Industrial Control Systems (ICS) Cyber Security Conference; (Singapore – virtual), 16-18 June 2020.

More details can be found on the following website:

https://www.us-cert.gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG

CS4CA WORLD: Global Cyber Security Conference

The virtual conference reviews the classic IT vs. OT issues, as well as security processes by prioritizing the protection of critical elements. Secure protocols for critical elements will also be addressed at the online conference.

CS4CA WORLD: Global Cyber Security Conference; Virtual, 30 June, 2020.

More details can be found on the following website:

https://world.cs4ca.com/

ICS incidents

Israel: Hackers are attacking SCADA systems in the water sector

Israel's National Cyber Directorate published the report, which mentioned that hackers attacked the SCADA systems at wastewater treatment plants.

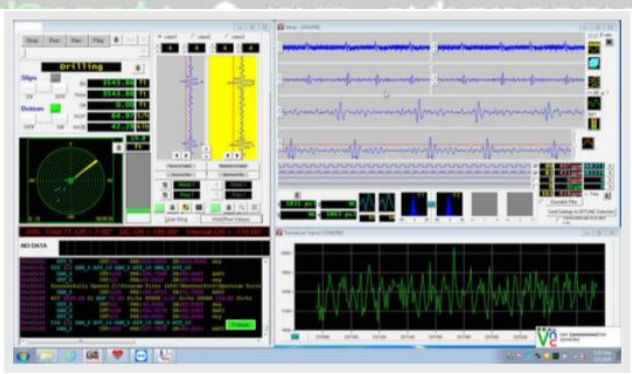
According to the Directorate, in the water and energy sector, the operators have to change the passwords in the systems, which are accessible from the internet, and update monitoring system software as soon as possible.

The report said that many organizations detected attacks against the SCADA systems country-wide, but Israel's Water Authority claimed the attacks didn't cause any operational damage. The Authority requested, that all involved organizations report the attacks.

The updated incident guide mentioned, that not only the SCADA systems were under attack, but all of the ICS elements. According to SecurityWeek's sources, the targeted element was the PLC, which used to control valves. The PLCs' software was modified, which means, that the attackers exactly knew what they were doing. One thing is not clear yet, the final target was the PLC modification, or this was a mistake, that the attackers left behind.

Radiflow, an Israeli-based industrial cybersecurity firm said that remote access was established via mobile/radio communication, because usually network devices are increasingly vulnerable to attacks done this way, these attackers have tried to take advantage of this as well. The other possibility was the exploitation of supply chains, and the incidents were performed by legal access rights.

Wastewater facilities not handling sensitive information, therefore, it is likely that the attackers target was to cause physical damage. According to the SCADAfence IT and OT security firm, the attacks came from the "Gaza Cybergang" anti-Israeli hacktivist group, and further attacks can be expected, not just in the water sector.



More details can be found on the following website:

https://www.securityweek.com/israel-says-hackers-targeted-scada-systems-water-facilities?

https://www.securityweek.com/hackers-knew-how-target-plcs-israel-water-facility-attacks-sources?

Book recommendation

The **Handbook of SCADA/Control Systems Security** book introduces the basic ICS/SCADA systems security principles from the point of view of various experts in the field. There are many photos, figures and illustrations in the book, which makes it enjoyable for the readers.

The book contains 6 chapters, which presents the societal impacts of ICS/SCADA systems and the consequences of their use, regulatory and management issues, architectures and models of those systems, issues of deployment and operation, and future safety factors for ICS/SCADA systems.

There are many cybersecurity and ICS/SCADA security case studies in the book, which can help to deeply understand the topic.

There are many good practices in the book, which addressed the environmental security, strategic and technical issues. These good practices can be easily implemented in case of a critical infrastructure program.

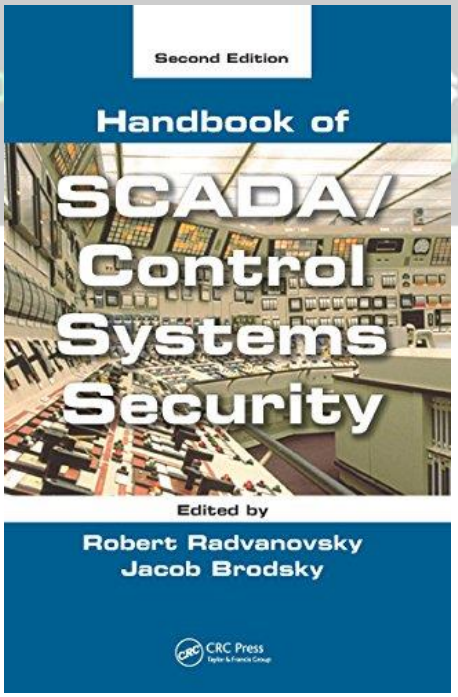
Title: **Handbook of SCADA/Control Systems Security**

Authors/Editors: Robert Radvanovsky, Jacob Brodsky

Year of issue: 2016.

The book available at the following link:

https://www.amazon.co.uk/Handbook-SCADA-Control-Systems-Security-ebook/dp/B01EUQGFGM/ref=sr_1_1?creativeASIN=B01EUQGFGM&dchild=1&imprToken=LM2ftYPP4JaX.CLszMQD-A&keywords=Handbook+of+SCADA%2FControl+Systems+Security&linkCode=g13&qid=1588576752&sr=8-1



Black Cell recommendations

There are many, ICS/SCADA-focused information and websites available internet-wide. To help you find the best and the most trusted sites, we suggest to use the below list:

https://www.securityweek.com/scada-ics

https://securityaffairs.co/wordpress/category/ics-scada

https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada

https://iiot-world.com/cybersecurity/

https://www.cipsec.eu/content/icsscada-networks-threats-and-defenses

https://industrialcyber.co/

https://www.scadahacker.com/

https://icscybersec.blog.hu/tags/SCADA

https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection

https://www.criticalinfrastructureprotectionreview.com/

https://ics.sans.org/ics-library/helpful-websites

https://www.nist.gov/industry-impacts/industrial-control-systems-cybersecurity

https://www.cirint.eu/

This list is not exhaustive, just a sample, to broaden the perspective.

ICS vulnerabilities

In May 2020 the following vulnerabilities reported by National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:

ICSA-20-135-01: **Opto 22 SoftPAC Project**

Critical level vulnerabilities: External Control of File Name or Path, Improper Verification of Cryptographic Signature, Improper Access Control, Uncontrolled Search Path Element, Improper Authorization.
https://www.us-cert.gov/ics/advisories/icsa-20-135-01

ICSA-20-135-02: **Emerson WirelessHART Gateway**

Critical level vulnerability: Improper Access Control.
https://www.us-cert.gov/ics/advisories/icsa-20-135-02

ICSA-19-213-04: **3S-Smart Software Solutions GmbH CODESYS V3 (Update A)**

High level vulnerability: Insufficiently Protected Credentials.
https://www.us-cert.gov/ics/advisories/icsa-19-213-04

ICSA-20-133-01: **Eaton Intelligent Power Manager**

High level vulnerabilities: Improper Input Validation, Incorrect Privilege Assignment.
https://www.us-cert.gov/ics/advisories/icsa-20-133-01

ICSA-20-133-02: **OSIsoft PI System**

High level vulnerabilities: Uncontrolled Search Path Element, Improper Verification of Cryptographic Signature, Incorrect Default Permissions, Uncaught Exception, Null Pointer Dereference, Improper Input Validation, Cross-site Scripting, Insertion of Sensitive Information into Log File.
https://www.us-cert.gov/ics/advisories/icsa-20-133-02

ICSA-20-105-05: **Siemens RUGGEDCOM, SCALANCE, SIMATIC, SINEMA (Update A)**

High level vulnerabilities: Uncontrolled Resource Consumption, Improper Input Validation.
https://www.us-cert.gov/ics/advisories/icsa-20-105-05

ICSA-20-105-08: **Siemens KTK, SIDOOR, SIMATIC, and SINAMICS (Update A)**

High level vulnerability: Uncontrolled Resource Consumption.
https://www.us-cert.gov/ics/advisories/icsa-20-105-08

ICSA-20-042-06: **Siemens SIMATIC PCS 7, SIMATIC WinCC, and SIMATIC NET PC (Update C)**

High level vulnerability: Incorrect Calculation of Buffer Size.
https://www.us-cert.gov/ics/advisories/icsa-20-042-06

ICSA-19-274-01: **Interpeak IPnet TCP/IP Stack (Update D)**

Critical level vulnerabilities: Stack-based Buffer Overflow, Heap-based Buffer Overflow, Integer Underflow, Improper Restriction of Operations within the Bounds of a Memory Buffer, Race Condition, Argument Injection, Null Pointer Dereference.
https://www.us-cert.gov/ics/advisories/icsa-19-274-01

ICSA-19-255-02: 3S-Smart Software Solutions GmbH CODESYS V3 Library Manager (Update A)
High level vulnerability: Cross-site Scripting.
https://www.us-cert.gov/ics/advisories/icsa-19-255-02

ICSA-19-227-04: Siemens SINAMICS (Update C)
High level vulnerability: Uncontrolled Resource Consumption.
https://www.us-cert.gov/ics/advisories/icsa-19-227-04

ICSA-19-190-05: Siemens SIPROTEC 5 and DIGSI 5 (Update C)
High level vulnerability: Improper Input Validation.
https://www.us-cert.gov/ics/advisories/icsa-19-190-05

ICSA-20-128-01: Advantech WebAccess Node
Critical level vulnerabilities: Improper Validation of Array Index, Relative Path Traversal, SQL Injection, Stack-based Buffer Overflow, Heap-based Buffer Overflow, Out-of-bounds Read.
https://www.us-cert.gov/ics/advisories/icsa-20-128-01

ICSA-20-126-01: Fazecast jSerialComm
High level vulnerability: Uncontrolled Search Path Element.
https://www.us-cert.gov/ics/advisories/ICSA2012601

ICSA-20-126-02: SAE IT-systems FW-50 Remote Telemetry Unit (RTU)
Critical level vulnerabilities: Cross-site Scripting, Path Traversal.
https://www.us-cert.gov/ics/advisories/ICSA2012602

ICSA-20-119-01: LCDS LAquis SCADA
Medium level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Improper Input Validation.
https://www.us-cert.gov/ics/advisories/icsa-20-119-01

The vulnerability reports contain more detailed information, which can be found on the following website:

https://ics-cert.us-cert.gov/advisories

Continuous monitoring of vulnerabilities is recommended, because relevant information on how to address vulnerabilities, patch vulnerabilities and mitigate risks are also included in the detailed descriptions.

ICS alerts

In May 2020, ICS-CERT hasn't published alerts.

The previous alerts can be found at the following link:

https://www.us-cert.gov/ics/alerts