WELCOME

TO THE INTERNATIONAL SUMMIT FOR SECURITY IN INDUSTRIAL CONTROL SYSTEMS

STOCKHOLM

23–26 OCTOBER 2017

Organized by

OMNISIENS

PARTNER

Advenica is a leading European provider of cybersecurity. Advenica offers advanced cybersecurity solutions and services for business-driven information exchange, secure digitalisation and high assurance.

For more than 20 years Advenica has enabled organisations and companies to take digital responsibility by providing future-proof, sustainable solutions.

advenica

During the Welcome reception Tuesday 24th Advenica Jonas Dellenvall will give the presentation ”Effective threat mitigation strategies”

WELCOME TO CS3STHLM!

We are proud to host the international summit on Cyber Security in Control Systems for Critical Societal Functions (CS3) in Sthlm, Sweden.

This year, the fourth since the inception, we continue our established traditions at the same time we changed several things - most notably the name.

The summit is more current than ever as we all face many hard challenges. Handling these challenges require expertise and experiences, which comes from exchanges of ideas in a creative and nurturing environment.

That is why we are passionate about our platform – Welcome to CS3STHLM!

Best wishes!

Erik & **Robert**

PRE-SUMMIT TUTORIALS AND TRAINING

Monday Oct 23

08:00	**REGISTRATION OPEN AT NALEN**
09:00	Tutorials starts
10:30	**COFFEE BREAK**
12:00	**LUNCH BREAK**
15:00	**COFFEE BREAK**
ca: 17:00	End of tutorials

Tuesday Oct 24

08:00	**REGISTRATION OPEN AT NALEN**
09:00	Tutorials starts
10:30	**COFFEE BREAK**
12:00	**LUNCH BREAK**
15:00	**COFFEE BREAK**
ca: 17:00	End of tutorials

15.00-18.00	**CS3STHLM** ICS/IoT lab opening in Geeklounge (Stacken) **OPEN BAR** CS3Sthlm Geeklounge hosted by: advenica
18.00-22.00	**WELCOME RECEPTION**
ca: 19.00	**"ENISA TRAININGS FOR CYBER SECURITY SPECIALISTS"** Rossella Mattioli
ca: 19.30	**"EFFECTIVE THREAT MITIGATION STRATEGIES"** Jonas Dellenvall, CTO Advenica

ERIK
HJELMVIK
NETRESEC

Our **two-day Network Forensics** class consists of a mix of theory and hands-on labs, where students will learn to analyze Full Packet Capture (FPC) files. The scenarios in the labs are primarily focused at network forensics for incident response, but are also relevant for law enforcement/ internal security etc. where the network traffic of a suspect or insider is being monitored.

Mon-Tue, Oct 23-24.

MICHAEL
THEUERZEIT
HUDSON CYBERTEC

The IEC 62443 is the worldwide standard for security of Industrial Automation & Control Systems, or Operational Technology (OT). The standard offers your organization grip on the improvement of the digital security of these environments.

An introduction of the IEC 62443,
Tuesday Oct 24.

CS3STHLM &

CPE CREDITS

You are entitled to **13 CPE** credits for the summit and **19,5 or 26 CPE** credits if you also took training in combination with the summit. Please send your CPE claims to

cpe@cs3sthlm.se

and we will send back a Continuing Education Policy Verification of Attendance Form.

MIKAEL
VINGAARD
ENERGINET

This **1-day workshop** would start with a short general introduction to ICS/SCADA **& Honeypots.**

During the day, the students will be guided in the different phases in planning, deploying and analyzing the collected data from a honeypot. During the day, we will deploy live honeypots on the internet and see how attackers would start to probe our honeypots. Furthermore, we will also attack the deployed honeypots ourselves; using SCADA pen testing tools and similar software.

Tuesday Oct 24.

Wednesday Oct 25
CS3STHLM

MAIN STAGE

REGISTRATION OPEN AT NALEN

09:00 **WELCOME + KEYNOTE** Erik Johansson & Robert Malmgren
Moderator: Anne-Marie Eklund Löwinder

• IoT – INTERNET OF THINGS

09:30 **"BACK TO THE IoT FUTURE"** Dan Demeter

COFFEE BREAK

10:30 **"S IN IoT IS FOR SECURITY"** Akriti Srivastava

ca: 11:15 **"IoT IN EUROPE: WHAT COULD POSSIBLY GO WRONG AND HOW YOU CAN FIX IT"** Rossella Mattioli

LUNCH BREAK

• LESSONS LEARNED

13:00 **"PRO-KREMLIN TROLLS, FAKE NEWS AND PROPAGANDISTS AS OPINION INFLUENCERS – AND HOW TO COUNTER THEM"** Jessikka Aro

13:30 **"APT CASE STUDY"** Jon Røgeberg & Martin Eian

14:00 **"PANDORA´S BOX"** Lars Erik Smevold

COFFEE BREAK - SWEDISH FIKA

• STRATEGY AND POLICY

15:30 **"NETWORK AND INFORMATION SECURITY DIRECTIVE: THE ROAD AHEAD"** Paraskevi Kasse

16.00 **"ICS PROGRAM DEVELOPMENT FOR MULTI-NATIONAL CORPORATIONS"** Melissa Crawford

16.30 **"PROTECTING EUROPEAN TRANSPORT INFRASTRUCTURES: THREAT MODELS AND SECURITY MEASURES"** Rossella Mattioli

Wednesday Oct 25
CS3STHLM

CS3STHLM FORUM HARLEM STAGE

12.30 **LUNCH SESSION**

15.00 **COFFEE SESSION**

CS3STHLM ICS/IoT LAB GEEKLOUNGE

17–18.30 Demonstration of ICS/IoT lab, lightning talks
OPEN BAR
CS3STHLM Geeklounge hosted by: advenica

CS3STHLM CONFERENCE DINNER

18.30 CS3STHLM Hallway pre-dinner mingel

19.00 CS3STHLM Conference dinner

ca: 20.00 **”ADVENTURES IN SOCIAL ENGINEERING...**
TALES OF A “PEOPLE HACKER”
Jenny Radcliffe

JENNY RADCLIFFE

”ADVENTURES IN SOCIAL ENGINEERING – TALES OF A “PEOPLE HACKER”

Jenny Radcliffe – aka “The People Hacker” – is an expert in Social Engineering (the human element of security), negotiations, non-verbal communication and deception, using her skills to help clients from corporations and law enforcement, to poker players, politicians and the security industry protect themselves from malicious social engineering attacks.

SPEAKERS day 1

DAN DEMETER
SECURITY RESEARCHER
Back to the IoT Future

AKRITI SRIVASTAVA
SECURITY RESEARCHER
S in IoT is for Security

ROSSELLA MATTIOLI
OFFICER IN NETWORK AND INFORMATION SECURITY
IoT in Europe: what could possibly go wrong and how you can fix it

JESSIKKA ARO
INVESTIGATIVE REPORTER
Pro-Kremlin trolls, fake news and propagandists as opinion influencers - and how to counter them

JON RØGEBERG
MANAGER
APT Case Study

MARTIN EIAN
SENIOR SECURITY ANALYST
APT Case Study

SPEAKERS day 1

LARS ERIK SMEVOLD
SENIOR SECURITY ANALYST
Pandora´s Box

PARASKEVI KASSE
NETWORK AND INFORMATION SECURITY OFFICER
Threat modelling and security measures for ICS/SCADA systems in critical infrastructure.

MELISSA CRAWFORD
GLOBAL CONSULTANT
ICS Program Development for Multi-national Corporations

ROSSELLA MATTIOLI
OFFICER IN NETWORK AND INFORMATION SECURITY
Protecting European transport infrastructures: threat models and security measures

Omnisiens is offering in depth training in ICS/SCADA related areas with world renown specialists.

– please contact us if you have a special request!

www.omnisiens.se
training@omnisiens.se

OMNISIENS

Thursday Oct 26
CS3STHLM

MAIN STAGE

- ICS SECURITY

09:00 **"THREAT MODELLING AND SECURITY MEASURES FOR ICS/ SCADA"** Paraskevi Kasse

09:30 **"CYBERATTACKS AGAINST CRITICAL INFRASTRUCTURE IN UKRAINE: TAXONOMY, CONSEQUENCES, LESSONS LEARNED"** Roman Sologub & Oleksii Yasynskyi

COFFEE BREAK

10:30 **"INDUSTROYER: BIGGEST THREAT TO INDUSTRIAL CONTROL SYSTEMS SINCE STUXNET"** Anton Cherepanov & Robert Lipovský

11.00 **"CYBER WARFARE AND LARGE SCALE CYBER CRIMINALITY"** Panel discussion

LUNCH BREAK

- ATTACKS

13:00 **"CONFIGURABLE CODE-REUSE ATTACKS MITIGATION FOR COTS PROGRAMMABLE LOGIC CONTROLLER BINARIES"** Ali Abbasi

13:30 **"FROM BOX TO BACKDOOR: USING OLD SCHOOL TOOLS AND TECHNIQUES TO DISCOVER BACKDOORS IN MODERN DEVICES"** Patrick DeSantis

14:00 **"SECURITY FOR SAFETY: FORTIFYING THE LAST LINE OF DEFENSE"** Jens Wiesner

COFFEE BREAK, HALLWAY TRACK

Thursday Oct 26
CS3STHLM

- PROTECTION

15:00 "**STRATEGIC NETWORK DEFENSE IN ICS ENVIRONMENTS"** Joe Slowik

15:30 "**DIY INSIDER THREAT DETECTION/PREVENTION WITHIN ICS ENVIROMENTS"** Dieter Sarrazyn

16:00 "**SECURE SCADA PROTOCOL FOR THE 21ST CENTURY (SSP21)"** Adam Crain

16.30 Conference closing session

CS3STHLM FORUM HARLEM STAGE

12.30 **LUNCH SESSION**

CS3STHLM ICS LAB GEEKLOUNGE

During the afternoon – ICS/IoT lab activities summary: statistics, highlights and discoveries
CS3STHLM Geeklounge hosted by: advenica

FIRST Founded in 1990, FIRST consists of internet emergency response teams from more than 300 corporations, government bodies, universities and other institutions from the Americas, Asia, Europe, Africa and Oceania. It leads the world's fight-back against cyber-crime, sabotage and terrorism, and promotes cooperation among computer security incident response teams and law enforcement agencies.

For more information, visit: www.first.org

SPEAKERS day 2

PARASKEVI KASSE

NETWORK AND INFORMATION SECURITY OFFICER

Threat modelling and security measures for ICS/SCADA systems in critical infrastructure.

OLEKSII YASYNSKYI

CYBERSECURITY EXPERT

Cyberattacks Against Critical Infrastructure in Ukraine: Taxonomy, Consequences, Lessons Learned

ROMAN SOLOGUB

GENERAL MANAGER & CEO

Cyberattacks Against Critical Infrastructure in Ukraine: Taxonomy, Consequences, Lessons Learned

ANTON CHEREPANOV

SENIOR MALWARE RESEARCHER

Industroyer: biggest threat to industrial control systems since Stuxnet

ROBERT LIPOVSKÝ

SENIOR MALWARE RESEARCHER

Industroyer: biggest threat to industrial control systems since Stuxnet

ALI ABBASI

PH.D. CANDIDATE

Configurable Code–Reuse Attacks Mitigation for COTS Programmable Logic Controller Binaries

PATRICK DESANTIS

SENIOR SECURITY RESEARCHER ENGINEER

From Box to Backdoor: Using Old School Tools and Techniques to Discover Backdoors in Modern Devices

JENS WIESNER

DIPL. PHYS.

Security for Safety: Fortifying the last line of defense

SPEAKERS day 2

JOE SLOWIK
NETWORK DEFENDER
Strategic Network Defense in ICS Environments

DIETER SARRAZYN
SECURITY EXPERT
DIY insider threat detection/prevention within ICS enviroments

ADAM CRAIN
SOFTWARE ENGINEER
Secure SCADA Protocol for the 21st Century (SSP21)

PARTNER

Atea delivers security solutions to customers within the private and public sector.

Our experts masters information security, cyber security and MSS services, this means that we can offer customers a complete package of services and experts.

Our NIS offering is our latest service to our customers.

ATEA

For more information visit **ATEA.SE**

MENTIMETER

CS3SHLM highly encourage interaction with the speakers and the exchange of ideas and experience. Therefore would we like all of you to go to www.menti.com and use following codes:

20 87 94 –Questions to Speakers

94 56 32 –Answers to Polls

92 06 7 –Speaker Rating

16 17 36 –Summit Evaluation

74 62 01 –Tutorial Evaluation

LETTER FROM OUR MODERATOR

I would like to take this opportunity to welcome you to the Stockholm international summit on Cyber Security in Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA), namely CS3STHLM.

This is the 4th annual CS3STHLM Summit which gathers the most important stakeholders across critical processes and industries. As a matter of fact CS3STHLM has quickly become the premiere ICS Security Summit in Northern Europe. And I am very proud to invite you to a summit with extraordinary speakers with unique skills and knowledge.

Currently the ICS area is rapidly growing. Critical infrastructures, such as power plants, transportation systems, chemical factories and manufacturing facilities of today are large, distributed complexes. In order to ensure a proper operation they must be continuously monitored and controlled by the operators. Remote command and control has been made feasible due to the development of a widespread and highspeed network together with the advent of Industrial Control Systems.

ICS have passed through a significant transformation from proprietary, isolated systems to open architectures and standard technologies, highly interconnected with other corporate networks and the Internet. ICS products are most commonly based on standard embedded systems platforms, applied in various devices, such as routers or cable modems, and they often use commercial off-the-shelf software.

This development has resulted not only in reduction of costs, ease of use and enabled remote control and monitoring from various locations, it has also resulted in the increased vulnerability to computer network-based attacks. Listen and learn from the experts, think security first! Or we will experience more and more attacks, more and more dysfunction, to an extent that will result in loss of trust from people. Loss of trust that will cost us dearly.

Anne-Marie Eklund Löwinder

WE HOPE TO SEE YOU AGAIN AT CS3STHLM

IN OCTOBER 2018!

Follow us on:

#CS3STHLM

WWW.CS3STHLM.SE INFO@CS3STHLM.SE