Day 1

17 June 2019 (Monday)

Workshop - for IT/OT personnel and management responsible for cybersecurity in the energy/industrial sector. It is aimed to provide knowledge and an opportunity to check in practice the hardware and software used in different cybersecurity areas.

<table>
<tr><th colspan="6">WORKSHOPS</th></tr>
<tr><td>08:00 - 09:00</td><td colspan="5">Registration</td></tr>
<tr><td rowspan="2">09:00 - 13:00</td><td rowspan="2">What is an ICS and why should you care[1] – group I</td><td rowspan="2">Computer forensics</td><td rowspan="2">Risk Adaptive Security for the Era of Connected Critical Infrastructure [2]</td><td rowspan="2">Effective execution of security (penetration) tests</td><td rowspan="2">Web Application Penetration Testing</td></tr>
<tr></tr>
<tr><td>13:00 - 14:00</td><td colspan="5">Lunch break</td></tr>
<tr><td>14:00 - 16:00</td><td rowspan="2">What is an ICS and why should you care – group II</td><td>Computer forensics – continuation</td><td></td><td>Effective execution of security (penetration) tests – continuation</td><td>Web Application Penetration Testing - continuation</td></tr>
<tr><td>16:00 - 18:00</td><td colspan="4"></td></tr>
<tr><td>18:00 - 22:00</td><td colspan="5">Networking and dinner</td></tr>
</table>

[1] The workshop will be in English (with an interpreter available).
[2] The workshop is recommended for cybersecurity, CERT and SOC senior managers. The workshop will be in English (with an interpreter available).

CC4ES
CYBERSECURITY CONFERENCE FOR ENERGY SECTOR

Day 2

18 June 2019 (Tuesday)

08:00 - 09:00 Registration

09:00 - 09:25 **Official opening and welcome**

Piotr Naimski, Secretary of State, Government Plenipotentiary for Strategic Energy Infrastructure

Eryk Kłossowski, President and CEO of PSE

Part I **Global landscape of threats**

09:30 - 10:00 ***Securing the Energy Sector through Collective Security***

Gen. Keith Alexander, (Ret.), CEO and President, IronNet Cybersecurity; Former Commander, U.S. Cyber Command and Former Director, National Security Agency

10:00 - 10:20 ***Cybersecurity – PSE approach and preference***

Grzegorz Bojar, CIO, ICT Department, PSE S.A.

10:20 - 10:45 ***Active, Passive or Hybrid - What's The Right Monitoring Approach for Your ICS Network?***

Alon Barel, VP Sales EMEA and APAC of Indegy

10:50 - 11:10 Coffee break

Part II **Cybersecurity in the United States. Best practices and solutions**

11:10 - 11:40 ***Developing National Structures and Policies for Cybersecurity***

Tim Roxey, Vice President, E-ISAC Chief Operations Office, North American Electric Reliability Corporation (NERC)

11:40 - 12:10 ***What Makes Industrial Control Systems Such Attractive Targets?***

Tim Conway, Certified Instructor and Technical Director, ICS and SCADA Programs, SANS Institute

12:10 - 12:40 ***The Importance of Human Centric Security in the age of Digital Transformation***

Christian Patrascu, Senior Director, Sales NPC (Nordics, Poland & Czech Republic), Forcepoint

12:40 - 13:00 Debate: ***Building a better future for the energy sector***

13:00 - 14:00 Lunch break

Part II **Cybersecurity for the energy sector – recommended solutions**

14:00 - 14:30 ***A Data-Driven Analysis of Hidden Vulnerabilities in IIoT & ICS Networks***

Igor Zbyryt, ICS Cybersecurity Operations Director, ASTOR

14:30 - 15:00 ***Incident Response: We've been hacked! Now what?***

Joe Doetzl, Cyber Security Practice Leader, Grid Automation, ABB

15:00 - 15:20 Coffee break

Part IV **Cybersecurity in Europe and Poland. Cooperation and experience sharing**

15:20 - 15:50 ***Experiences of the CERT Team at Energa Group***

Bogusław Kowalski, Chief Information Security Officer, Head of CERT, Energa

15:50 - 16:20 ***Approach to managing cyber risks to PSE's critical systems***

Jeremi Gryka, Deputy Director of IT Security, PSE S.A. and Michał Paulski, Manager, ICS& IIoT Security, Accenture Security

16:20 - 17:00 ***Network reconnaissance – live!***

Michał Sajdak, IT security consultant in Securitum, trainer, pentester and founder of sekurak.pl

17:00 - 17:15 Wrap-up

18:00 - 22.00 Networking and dinner

Day 3

19 June 2019 (Wednesday)

SANS ICS NETWARS training

Grid NetWars is a suite of hands-on, interactive learning scenarios that enable Operational Technology security professionals to develop and master the real-world, in-depth skills they need to defend real-time systems. It is designed as a challenge competition and is split into separate levels so that advanced players may quickly move through earlier levels based on their expertise. The Grid Netwars experience has been themed for the electricity industry and the scenario has been coordinated to align with industry exercise events.

09:00 - 09:30 – Coffee

09:30 - 10:00 – Opening NetWars Presentation

10:00 – 13:00 - Open Game server for live competition

13:00 - 14:00 – Lunch Break

14:00 - 16:30 - Re-Open game server for live competition

16:00 - 17:00 - Close game and announce winners

18:00 - 18:15 - Closing remarks

Description of the workshop:

1. **What is an ICS and why should you care (workshop in English, with an interpreter available).**

In this four hour workshop, students will learn the basics of an Industrial Control System, ICS attack vectors, and defender specific proactive measures used to mitigate the effect of an attack. The workshop will focus be on establishing an understanding of basic ICS components, tools, architectures, standards, security frameworks, and risk management in operational environments. The workshop is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology security)
- Engineering
- Corporate, industry, and professional standards

Trainer: **Tim Conway (SANS)**

Duration: **4h**

Maximum number of participants: **20**

Two groups: **9:00-13:00 and 14:00-18:00**

2. Computer forensics: acquisition of information in electronic form from computers and mobile devices.

The workshop will be divided into two parts. The theoretical part during which the participants will be familiarized with the best practices in computer and mobile forensics. The practical part of the workshop will focus on providing the participants with knowledge of the methods of extraction, protection and analysis of data from computers and mobile devices.

Workshop agenda:

1. Part I:
   - Practical lecture: Computer forensics – definitions; Best practices in computer forensics; Data security tools and their functions; Basic rules for securing data and operating procedures;
   - Interactive technical workshop, aimed to present the capabilities of the AXIOM platform. Case study: leakage of sensitive project data from a small business; Protection and analysis of data from multiple sources (computers, carriers, mobile devices, cloud) – possibilities and challenges. Analysis of protected information, benefits of reporting and data analysis.
2. Part II
   - Practical lecture: What is Mobile Forensics? Best practices in mobile forensics; Methods of data acquisition from mobile devices; Alternative methods of data acquisition from mobile devices (Qualcomm EDL Mode, JTAG/ISP, Chip-Off); Methods of breaking/bypassing security features; Methods of analyzing the HEX code;
   - Technical workshop involving the participants: Scenario-based case execution; Presentation of the capabilities of the XAMIN analytical platform;

Duration: **6.5h**

Maximum number of participants: **30**

3. Effective execution of security (penetration) tests

The workshop will consist of the 3 thematic blocks mentioned below, and they will contain numerous elements of interaction with the trainees, in particular in the form of practical exercises.

- **Thematic block No. 1** – includes an overview of:
  - stages of penetration tests and their scope – an introduction to the subject of the training and recollection/introduction of key notions and terms.
  - recognition stage (all points to be discussed based on practical examples), including:
    - recognition types (passive, active);
    - type of information that can be acquired;
    - toolkit (browser extensions, crawlers, etc.):
      - choosing the right tools (what to pay attention to, what a complete toolkit for a specific ICT system should contain);
      - configuration of individual tools – which configuration options are important and when they should be used;
      - interpreting results and clarifying incompatibilities;
      - identification of false-positive notifications.
- **Thematic block No. 2** – includes an overview of:

- automatic tests (all points to be discussed based on practical examples), including:
  - toolkit (as in recognition);
  - non-standard vulnerability scanners;
  - tests from the logged-in user level;
    - use of special options of security scanners;
    - using tools that allow scanning from the logged-in user level with any security scanner;
    - proxy servers (and their appropriate configuration).

- **Thematic block No. 3** – includes an overview of manual/expert tests (all points to be discussed based on practical examples), including:
  - examples of specialist tools (e.g. sqlmap);
  - verification of (selected) vulnerabilities reported by automatic software tools;
  - using a specific/advanced configuration;
  - manual detection of vulnerabilities – based on selected examples from the OWASP Top 10 classification;
  - selected vulnerabilities of ICT systems (for different types of services, e.g. web applications, WebServices);

Duration: **6h**

Maximum number of participants: **20**

4. **Risk Adaptive Security for the Era of Connected Critical Infrastructure.**

- What are the prevailing trends in the energy sector, and what innovative approaches to security are emerging to protect the sector and its supply chain?

- The NIS Directive requires “appropriate and proportionate technical and organisational measures” – but who decides what is appropriate and proportionate? How can operators of essential services implement a defensible security architecture, that meets both national requirements and organisational priorities?

- As GDPR compliance beds in, how can you become efficiently compliant and more effective in protecting your most valuable data assets? The workshop will be in English (with an interpreter available).

Facilitator: **Duncan Brown,** Chief Security Strategist, EMEA at Forcepoint

Specializes in IT Security market strategy, and security & corporate alignment. Business development experience in new territories, markets and cultures, with accompanying evidence of growth. Currently leading CISO engagement in EMEA, focusing on security strategy, positioning security as a business enabler/accelerator, CISO coaching, security/privacy balance, mapping security outcomes to business strategy, privacy regulation trends & impacts, and all things GDPR.

Duration: 4**h**

Maximum number of participants: **30**