6th Cyber and SCADA Security for Oil & Gas Industry 2019

prospero EVENTS GROUP

Adopting Optimal Strategies to Make Your Systems More Resilient to External Attacks

18th – 20th of September 2019
Amsterdam, The Netherlands
PARK HOTEL AMSTERDAM

SPEAKER PANEL

Benedict Olaoya
Chief Information Security Officer
&
Mo Ahddoud
Advisor
SGN
UK

Shah Rizal Dahlan
Custodian Engineer and Group Technical Authority for Instrument and Control
Petronas
Malaysia

Jesper Bork Olsen
IT Security Manager
&
Ole Debess
Senior Electrical Engineer
Maersk Drilling
Denmark

Fredrik Gratte
Senior Principal Engineer, Cyber Security and Network Infrastructure
Aker Solutions
Norway

Senan Largey
Alliances and Partnerships
International Operational Technology Security Association (IOTSA)
UK

Jana Puskacova
Chief Information Security Officer
SLOVNAFT, a.s.
Slovakia

Segun Yayi
Head of Cyber Security
EP Energy
USA

Ruud Timmermans
Global Lead Automation
VTTI
The Netherlands

Margrete Raaum
CEO, Norwegian ICS CERT
KraftCert
Norway

Erwin Kruschitz
Head of NAMUR Security Working Group
NAMUR
Germany

Tomi Lahti
Product Manager NAPCON Understand
Neste Engineering Solutions - NAPCON
Finland

Workshop Leader

Bert Willemsen
Managing Director
aXite Security Group
The Netherlands

Topics to be addressed

- Prioritizing **Cyber Security** in **E&P projects** - Challenges and Proposals
- **A 360° view** on asset inter-network-dependencies and the **role of ics /scada security**
- Can we all become **Trilingual?**
- **Risk assessment** for Critical Infrastructure
- **Legal Challenges** for Critical Infrastructures
- **Unrealistic exercises** only renders you good at exercising
- **Network Segmentation** in a typical storage terminal
- **Incident resposnse** in OT Environment
- **Advanced persistent threats (APT)** Protection and Perimeter Security strategies for SCADA
- **Social engineering** aspects of Cybersecurity
- **Security for Safety:** The NAMUR **NA163 Method**
- Managing **supply chain security risks**

Benefits of attending

- Meeting selected **senior decision-makers** from IT, ICT & Information Security divisions of leading global **Oil & Gas** companies
- Learning from the selected examples of **practical approaches**
- Knowledge and expertise **exchange**
- Direct **networking** with industry decision makers in a **business - friendly** environment

ASSOCIATION PARTNER

International Operational Technology Security Association

MEDIA PARTNERS

CRITICAL INFRASTRUCTURE PROTECTION REVIEW
Unique content | Global reach | In print and online

Cyber Security Review
Unique content | Global reach | In print and online

CYBER DEFENSE MAGAZINE

6th Cyber and SCADA Security for Oil & Gas Industry 2019

prospero EVENTS GROUP

18th of September

18th – 20th of September 2019

Amsterdam, The Netherlands

PARK HOTEL AMSTERDAM

INTERACTIVE WORKSHOP

Led By aXite Security Group

15:30 *Registration & Welcome Coffee*

16:00 *Opening Address from the Workshop Leader*

Bert Willemsen
Managing Director
aXite Security Group, *The Netherlands*

A 360° VIEW ON ASSET INTER-NETWORK-DEPENDENCIES AND THE ROLE OF ICS / SCADA SECURITY

16:10 **Introduction of scenario thinking and Digital Twin**

- How is cybersecurity evolving in ICS environments
- ICS and NIST 800-82r2 / IEC-62443 compliancy
- Change management and configuration integrity

18:00 *Closing Remarks from the Workshop Leader, Coffee & Networking*

Workshop Outline

Cyberattacks can have a massive impact on the physical world. Administrators might have a clear picture of their own grids, but their notion on infrastructures managed by other operators and how these affect each other is still not optimal.
We have to understand, how critical infrastructures, networks and the environment interact. Can we control change of controls and secure program integrity, put data in context and become NIST 800-82r2 and or IEC 62443 compliant? How can we combine risk management with the impact on financials or safety for each event before we decide to override?
In this workshop we will discuss a 360° view on critical infrastructures, taking into account network and asset interdependencies and the ability to run various near-real time simulation scenarios.
This approach of cyber risk management and business continuity, should enable you to assess impact and mitigate damage and gives you the ability to prepare for remediation and recovery scenarios, while staying operational. Could a Digital Twin be a possible solution?

About aXite Security Group

aXite is an independent, specialized advisor and partner of system integrators in the area of physical- and cybersecurity. aXite is experienced in the field of industrial cyber security strategies and cyber risk management. aXite defines and implements cyber security strategies throughout organizations, including energy and critical infrastructure.

aXite introduced Location Based (cyber)Security in critical SCADA/ICS environments and performs monitoring of critical infrastructure including scenario analyses with override possibilities during operations.

6th Cyber and SCADA Security for Oil & Gas Industry 2019

prospero EVENTS GROUP

19th of September
Conference Day One

18th – 20th of September 2019

Amsterdam, The Netherlands

PARK HOTEL AMSTERDAM

8:30 Registration & Welcome Coffee

9:00 Opening Address from the Chairman

EVOLUTION OF ICS CYBER SECURITY & NOT PETYA

9:10 **A 360 view on asset inter-network-dependencies and the role of ICS / SCADA security**

- Network and asset interdependencies
- Ability to run various near-real time simulation scenarios
- Cyber risk management and business continuity

Bert Willemsen
Managing Director
aXite Security Group, *The Netherlands*

9:50 **In the wake of notPetya…**

- What actually happened?
- What are the key learnings following the notPetya Cyber incident?
- What do we foresee as the main challenges in the future?
- Recommendations from Maersk Drilling

Jesper Bork Olsen
IT Security Manager
Maersk Drilling, *Denmark*

Ole Debess
Senior Electrical Engineer
Maersk Drilling, *Denmark*

10:30 *Coffee and Networking Break*

CYBER SECURITY EXCERCISES

11:00 **Unrealistic exercises only renders you good at exercising**

- Creating the right level & depth exercises for the right people including ICT, OT & vendors
- Recognising the given premises
- Getting all parties on board
- Introducing friction: what should & should not be included

Margrete Raaum
CEO, Norweign ICS CERT
KraftCert, *Norway*

11:40 **Table Top Excercise**

Incident resposnse in OT Environment

An attack targeting your OT assets is a matter of when, not if. Therefore, being prepared to respond is crucial. One element of your readiness plan is having an Incident Response Plan (IRP). While having an IRP is important, testing it periodically is the only way to ensure that all stakeholders are aware of their respective responsibilities when responding to a cyber incident. This Incident Response Tabletop Exercise will use a common incident scenario to discuss response activities as well as roles and responsibilities when responding to the incident. The aims of this exercise are to:

- Create awareness on the importance of testing your own IRP
- Learn from other participants
- Identify potential gaps in your own Plan, and
- Improve your response readiness

Segun Yayi
Head of Cyber Security
EP Energy, *USA*

12:50 *Lunch Break, Coffee and Networking*

14:00 **Risk assessment for Critical Infrastructure**

- Developing a cyber risk framework and building a cyber risk profile
- Specific processes, methods and tools used to perform cyber risks assessments
- Practical examples of risk assessment

Time Slot Reserved for Sponsors

ADVANCED PERSITENT THREATS

15:20 **Advanced persistent threats (APT) Protection and Perimeter Security strategies for SCADA**

- Real time protection and remote monitoring management
- Identifying variables that can influence security performance
- OT & SCADA Infrastructure security
- Advanced persistent threat protection

Time Slot Reserved for Sponsors

16:30 **Can we all become Trilingual?**

- The language of finance.
- The language of IT Security.
- The language of OT security.
- Information sharing between operators and suppliers
- Addressing Suppliers risks with Limited resources

Senan Largey
Alliances and Partnerships
International Operational Technology Security Association (IOTSA), *UK*

16:00 *Coffee and Networking Break*

11:40 **Panel Discussion**

The Current state of ICS maturity and awareness

- How mature is cyber security in ICS?
- Greatest threat to critical infrastructure
- What are the levels of «Probability," in relation to critical infrastructure cyber attacks?
- How does it look for a C-Level executive. Is reputational & financial damage the only concern or is there a concern in relation to safety
- Where is the weakest link in people, process & technology

17:50 *Closing Remarks from the Chair & Wrap up of Day 1*

18:00 ***Cocktail Reception***

Conference Producer: Abhishek Swami **tel:**+420 255 709 520 **fax:**+420 255 709 599 **email:** abhis@prosperoevents.com

6th Cyber and SCADA Security for Oil & Gas Industry 2019

prospero EVENTS GROUP

20th of September

Conference Day Two

18th – 20th of September 2019
Amsterdam, The Netherlands
PARK HOTEL AMSTERDAM

8:30 Registration & Welcome Coffee

9:00 Opening Address from the Chairman

PRIORITISATION OF CYBER SECURITY IN E&P & SOCIAL ENGINEERING

9:10 **Prioritizing Cyber Security in E&P projects - Challenges and Proposals**

- Strategy and methodology
- Adaptations of IEC 62443
- Network architecture design decisions
- Simplifications and optimizations

Fredrik Gratte
Senior Principal Engineer, Cyber Security and Network Infrastructure
Aker Solutions, *Norway*

9:50 **Social engineering aspects of Cybersecurity**

- Statistics show that 38% of the cyber-security threat comes from inadvertent insiders where Erratic Behavior can be part of it. Social penetration attacks through manipulation of human flaws are more effective than the technical ones
- Social engineering is therefore needed to be put into focus to reduce the risk of our employees from being exploited for malicious objectives by the irresponsible cyber attackers
- Awareness, education and fostering trust are key in combating social engineering exploits
- Fostering understanding that "we can be out of business" if we remained inaction/uneducated in Cyber Security risk is key to obtain full conviction from all the employees
- A holistic approach needs to be developed to include employees in the company's cyber defence protocol

Shah Rizal Dahlan
Custodian Engineer and Group Technical Authority for Instrument and Control
Petronas, *Malaysia*

10:30 *Business Card Exchange and Coffee Break*

Opportunity for the participants to share their contact information with each other dedicated specifically to strengthening business connections with the industry peers

11:00 **SLOVNAFT ICS Cyber Security Program**

The objective of ICS Cyber Security Program is to bring the industrial area system to desired cyber security level. The Assessment phase of the Program consisted of 8 projects that assessed current status and proposed how to close identified gaps in ICS

Jana Puskacova
Chief Information Security Officer
SLOVNAFT, a.s., *Slovakia*

11:40 **Panel Discussion**

Current State of Threat Detection

- Do organisations have the resources or intel to identify where attacks are originating
- Maturityof threat detection market reached and how can we make wise investment decisions?
- Are detection solutions taking a holistic approach to assessing risk, identifying complete characteristics of complex threats and escalating appropriately?

12:20 *Lunch Break, Coffee and Networking*

13:30 **Building secure production information platform with OPC UA -based communication**

- OPC UA and its built-in security features
- How to apply OPC UA for building company wide production information platform
  - to enable operational intelligence and seamless SCADA implementations
  - make full use of existing information assets
- Use case: Transferring operational data securely to cloud analytics

Tomi Lahti
Product Manager NAPCON Understand
Neste Engineering Solutions - NAPCON, *Finland*

14:10 **Security for Safety: The NAMUR NA163 Method**

Regulations ask for an IT-Security Risk Assessment for Safety Systems. But:

- Who is doing it? and How often?
- What needs to be risk assessed?What are the acceptance criteria?

The NAMUR NA 163 provides the answers…

Erwin Kruschitz
Head of NAMUR Security Working Group
NAMUR, *Germany*

14:50 *Coffee and Networking Break*

SUPPLY CHAIN RISKS & NETWORK SEGMENTATION

15:10 **Network Segmentation in a typical storage terminal**

- Segregating the operational networks in a production site to ensure reliability and availability of production automation
- How does a typical storage terminal segregate the networks?
- What challenges come up when doing this?

Ruud Timmermans
Global Lead Automation
VTTI, *The Netherlands*

15:50 **Managing supply chain security risks**

- How have vendors come along in making security a core part of product development
- How one can address suppliers risks with limited resources
- Legal/procurement to operational monitoring of their security
- Information sharing between operators & suppliers

Benedict Olaoya
Chief Information Security Officer
SGN, *UK*

Mo Ahddoud
Advisor
SGN, UK

16:30 *Closing Remarks from the Chair & Wrap up of Day Two*

Conference Producer: Abhishek Swami **tel:**+420 255 709 520 **fax:**+420 255 709 599 **email:** abhis@prosperoevents.com

6th Cyber and SCADA Security for Oil & Gas Industry 2019

prospero EVENTS GROUP

18th – 20th of September 2019

Amsterdam,The Netherlands

ASSOCIATION PARTNER

International Operational Technology Security Association

The International Operational Technology Security Association (IOTSA)

With active participation from organisations and individuals from around the world, the International Operational Technology Security Association (IOTSA) is rapidy growing. Our aim is to become the largest and most influential community of interest association for Operational Technology (OT) security professionals and the associated community The IOTSA provides a valuable platform that allows members and sponsors to connect, share knowledge, expertise and know-how on cyber resliiance and online security for OT, IoT, IIoT, ICS, IT and AI. Join us today, go to www.iotsa.info and together let us make the industrial world a safer place.

MEDIA PARTNERS

Cyber Security Review

Unique content | Global reach | In print and online

The Cyber Security Review is designed to draw on the combined knowledge, skills and expertise of the cyber security community to identify the emerging threats and facilitate the development of coherent policies and robust capabilities. Our mission is to promote dialogue and provide a platform for information exchange and cooperation between stakeholders, industry, academia and security experts worldwide. For more information, please visit: www.cybersecurity-review.com

CRITICAL INFRASTRUCTURE PROTECTION REVIEW

Unique content | Global reach | In print and online

Critical Infrastructure Protection Review is the go-to destination for the latest news, insights and expert knowledge, and designed to assist governments, public and private sectors in improving security and resilience of vital critical infrastructures, strengthening their preparedness to withstand and recover from the physical and cyber attacks. For more information, please visit: http://www.criticalinfrastructureprotectionreview.com/

CYBER DEFENSE MAGAZINE

Cyber Defense Magazine is by ethical, honest, passionate information security professionals for IT Security professionals. Our mission is to share cutting edge knowledge, real world stories and awards on the best ideas, products and services in the information technology industry. For more information, please visit: https://www.cyberdefensemagazine.com/