Second Annual API-IOGP Europe Cybersecurity Conference

27-28 June, 2018 | Hyatt Regency London - The Churchill | London, England | www.api.org and www.iogp.org

Wednesday, 27 June, 2018

8:30 AM – 9:00 AM	**Registration and Continental Breakfast – *Sponsored by ABB***
9:00 AM – 9:15 AM	**Welcome: Opening Remarks and Safety Moment** **Speaker: James Crandall, Policy Analyst, API**
9:15 AM – 10:00 AM	**Opening Keynote Session** **Speaker: Dr. David Stupples, City University of London**
10:00 AM – 10:45 AM	**How Secure are your Industrial Control Systems?** **Speaker: Jamie Walker, Director – Safety, Projects & Associate Membership** **UK Petroleum Industry Association** *The development and deployment of 'smart' technology in the energy sector, along with the expansion of intelligent network devices throughout the energy distribution system, has created several specific challenges. For one, this has resulted in an expansion of the 'cyber-attack surface'. As energy systems are widely connected, cyber security threats carry potentially wider repercussions for the whole critical infrastructure network and for society. The result is that of new security risks in the cyber arena. The presentation will review recent global attacks on Industrial Control Systems, vulnerabilities, lessons that can be learned and key strategies to ensure the threat of cyber-attacks can be mitigated.*
10:45 AM – 11:15 AM	**Coffee/Tea Break – *Sponsored by Nozomi Networks***
11:15 AM – 12:00 PM	**Developing a Combined Lifecycle Management Approach for Both Functional Safety and Security for SIS** **Speaker: John Walkington, Manager - FSM Technical Authority OGC, ABB Limited** *IEC 61511 Ed 2 2016 now calls for a mandatory security risk assessment as part of the requirements specification of a safety instrumented system (SIS). It therefore follows that once the security requirements specification is developed, a lifecycle management approach is required to transpose such requirements into the design of a SIS to ensure that the functional design specification and scope is engineered, installed, commissioned, operated and maintained via an appropriate lifecycle management system which should be in alignment with the relevant IEC functional safety and security lifecycle expectations. This paper will present one approach to developing a combined lifecycle management requirement in bringing together the similar processes and competencies that are necessary to achieve a combined IEC 61511 and IEC 62443 set of procedures, processes and competencies to achieve compliance to the industry good practice standards for safety and security.*
12:00 PM – 1:00 PM	**Lunch – *Sponsored by SecurityMatters***
1:00 PM – 1:45 PM	**Guidelines for Baseline Cybersecurity for Drilling Assets** **Speaker: Siv Hilde Houmb, CTO, Secure-NOK AS** *The rate of cybersecurity attacks and the attackers' level of sophistication and organization are increasing. Cyber-attacks represent a significant financial and environmental risk to firms with O&G operations. The attacks may cause environmental or*

	human damage or impact, disrupt or shut down operations, steal information, impact production schedules, increase operational costs, expose the organizations to legal liabilities, and damage the organizations' reputations. Furthermore, increased automation and Internet connectivity of drilling assets makes these systems more susceptible not only to cyber-attacks, but also to accidental and non-malicious user behavior. This presentation will provide an overview of the guidelines on baseline cybersecurity for O&G drilling assets developed by the International Association of Drilling Contractors (IADC). The guidelines are derived from the NIST Cybersecurity Framework and apply to the digital systems involved in modern drilling operations, including information technology (IT) systems, operational technology (OT) systems, industrial controls systems (ICS), and automation systems found on drilling assets.
1:45 PM – 2:30 PM	**Securing the Supply Chain: Managing Risks Inside and Outside Your Walls** **Speaker: Ed Turkaly, Cyber Security Leader, Baker Hughes, a GE Company** *Energy operators rely on an extensive network of business partners and suppliers to operate efficiently and safely. This network can contribute to increasing cyber security risks if best practices aren't adopted and followed diligently. The importance of resilience in a vendor's supply chain is critical and should be evaluated near the same level as safety and integrity. Those operating industrial control environments should take a deeper look at security by reviewing key areas that can contribute to increased risk within the supply chain.* *This presentation will address:* 1. *What previous compromises tell us about our future* 2. *The impact of regulations on supply chain security* 3. *The importance of a long-term partner when choosing security solutions* 4. *What shared responsibility looks like before, during and after commissioning* 5. *Looking beyond greenfield; shared responsibility with legacy devices* 6. *Expectations during a compromise* 7. *When and where the reduction of vendors equals a stronger security posture* 8. *How to effectively evaluate vendors, from both OT and IT perspectives*
2:30 PM – 3:15 PM	**Coffee/Tea Break – *Sponsored by Nozomi Networks***
3:15 PM – 4:00PM	**ICS Security across the Value Chain** **Speaker: Jeff Foley, Business Development Manager, Siemens** *Cyber Attacks on Critical Infrastructures have risen more than 24% over the course of the past year. As time goes on, more and more Intelligent Electronic Devices (IEDs) are being deployed in Bulk Electric Systems (BES), Oil & Gas, and Transportation in order to be able to gather more data, and to help optimize efficiency. In turn, this is causing cybercriminals to turn their attention to Industrial Controls Systems (ICS) as targets. In order for operators to be able to defend against these attacks, they must implement a Defense in Depth strategy utilizing standards such as IEC 624423 and ISO 27001 along with guidelines such as the NIST Cybersecurity Framework, NCCOE Situational Awareness Planning Guide NIST SP 1800-7, and the BDEW whitepaper.*
4:00 PM – 4:45 PM	**Industrial Control Systems (ICS) Security:** Innovations and IT-OT Convergence **Speakers: Trevor Goldman, Pre sales Manager, Waterfall Security** **Siv Hilde Houmb, CTO, Secure-NOK AS** *Firstenberg's presentation explores the question 'how much is enough' and draw some simple conclusions. We discuss how classic 'natural disaster' risk models and other IT-centric security risk models that attempt to quantify the likelihood of attacks are poor fits to physical or cyber security problems. A good understanding of the characteristics of control system networks, industrial processes, safety systems, protection systems, security systems and attack capabilities are all prerequisites to an effective risk assessment. Assembling all this knowledge and these costs into a simple matrix for business leaders to understand and evaluate is very much possible.* *Houmb's presentation will provide an overview of the guidelines on baseline cybersecurity for O&G drilling assets developed by the International Association of Drilling Contractors (IADC). The guidelines are derived from the NIST Cybersecurity Framework and apply to the digital systems involved in modern drilling operations, including information technology (IT) systems, operational technology (OT) systems, industrial controls systems (ICS), and automation systems found on drilling assets.*
4:45 PM – 6:30 PM	**Opening Reception – *Sponsored by Indegy***

Thursday, 28 June, 2018

8:00 AM – 8:30 AM	**Continental Breakfast**
8:30 AM – 9:30 AM	**What exactly are the threats to ICS/SCADA networks?** **Speaker: Ken Munro, Consultant, Pentest Partners** *As the sector becomes more and more connected it's coming under threat from emerging technologies. The Internet of Things is already seeing CNI increasingly exposed, with ICS publicly identifiable on websites such as Shodan and locatable via geolocation websites - it is only a matter of time before deployed IoT is weaponized. This session will look at the evolution of malware and the potential for DDoS, black starts, hijacking and ransomware over ICS and SCADA networks. It will explore how OSINT may be combined to help attackers formulate and target attacks and what vested parties can do to mitigate these threats.*
9:30 AM – 10:30 AM	**European Public Policy Trends Legal Panel** **Moderator: Jennifer Gorman, Managing Counsel, API** **Speakers: Edward McNicholas, Partner, Sidley Austin** **Craig Rogers, Partner, Eversheds Sutherland** **Eduardo Ustaran, Partner, Hogan Lovells** *The panel will discuss General Data Protection Regulation (GDPR), the Directive on Security of Network and Information Systems (NIS Directive), and other pertinent European regulations as well as key compliance issues*
10:30 AM – 10:45 AM	**Coffee/Tea Break – *Sponsored by Nozomi Networks***
10:45 AM – 12:15 PM	**Cyberattacks & Emerging Threats:** Ransomware, Other Threats from the Cutting Edge and Lessons Learned from Recent Breaches **Moderator: James Crandall, Policy Analyst, API** **Speakers: Laurens Binken, Head of Incident Management, Monitoring, Forensics, Shell** **Levone Campbell, ASC IT Security Operations Lead, Aramco Services** **Andy Holmes, Schlumberger Europe and Africa IT Security Manager, Schlumberger** **Roberto Minicucci, Sr Director - Product Security, Baker Hughes, a GE Company** *The session will touch on the changing IT threat landscape, phishing mitigation programs, the Triton attack, and successful incident response plans.*
12:15 PM – 1:15 PM	**Lunch – *Sponsored by Waterfall Security***
1:15 PM – 2:00 PM	**Designing a Cybersecurity Program based on the NIST Cybersecurity Framework** **Speaker: Larry Wilson, Chief Information Security Officer, University of Massachusetts** *Dr. Wilson's presentation will focus on how companies design, build and maintain a comprehensive cybersecurity program based on the NIST Cybersecurity Framework (CSF). It will focus on three key elements of a security program, engineering, technical and business capabilities. The output from the presentation includes a comprehensive design document and executive summary report.*

2:00 PM – 2:50 PM	**Next Generation Cybersecurity Solutions/Technologies:** What's on the Horizon? Part I **Moderator: Aaron Padilla, Senior Advisor, International Policy, API** **Speakers: Alon Barel, VP Sales, EMEA & APAC, Indegy** **Alejandro Rivas-Vásquez, Director, Head of Cyber in Energy & Infrastructure, KPMG** *The session will look at the anatomy of ICS cyber attacks and discuss recent critical infrastructure hacks as well as how IT departments interact with internal stakeholders who regularly digest security event data.*
2:50 PM – 3:40 PM	**Coffee/Tea Break – *Sponsored by Nozomi Networks***
3:40 PM – 4:55 PM	**Next Generation Cybersecurity Solutions/Technologies:** What's on the Horizon? Part I**I** **Moderator: James Crandall, Policy Analyst, API** **Speakers: Howard Eakin, Information Protection Lead, EMEA, ConocoPhillips** **Erland Engum, Product Director, Secure NOK** **Kenneth Frische, Director of Cybersecurity, 3eTI, an Ultra Electronics** *The session will examine risks and security standards in Robotic Process Automation, behavioral-based detection of cyber-attacks on Programmable Logical Controllers (PLCs), and the Purdue Model.*
4:55 PM – 5:00 PM	**Closing**