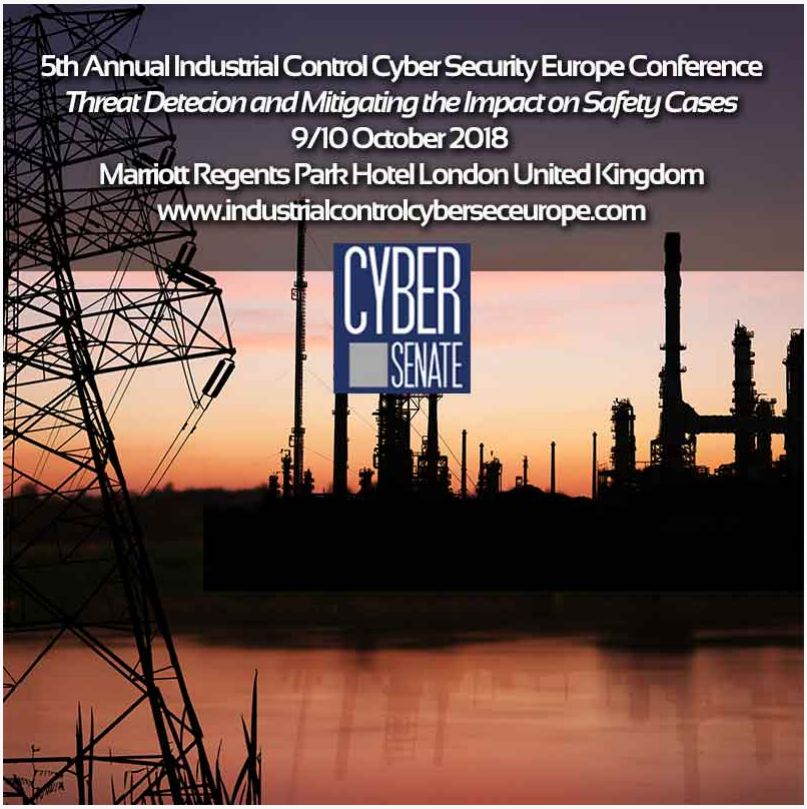
'Think like hackers, act like engineers' says leading cyber expert ahead of major industry conference

Practical steps the industry can take to keep critical assets operational, such as cyber-informed and consequence driven engineering.



LONDON, UNITED KINGDOM, June 11, 2018 /EINPresswire.com/ -- Keynote speaker Marty Edwards, former Director of the US Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and current Managing Director of the Automation Federation, will argue that in order to tackle today's security challenges, industry needs to do more to understand the mind-set and means of hackers, and apply this knowledge to developing the solutions that will keep critical assets operational.

He will discuss the practical steps the sector can take to achieve this, such as applying principles adopted from safety analysis and using concepts such as cyber-informed and consequence driven engineering and other key issues at the conference, where he will be joined by keynote presenter Tim Roxey, Chief Cyber Security Officer for the North American Electrical Reliability Corporation (NERC). A global expert in cyber security, Mr Roxey will share the knowledge he has developed through his background in investigating some of the world's most high-profile cyber attacks – including the Petya malware attack in the Ukraine – in "Beyond the attacks: what teachings can be learned from various attacks that help inform advanced defences". Exploring what industry needs to know about the broader strategic implications of recent cyber attacks, this talk will discuss the emerging profile of the 21st century cyber attacker, which Roxey posits as an adversary seeking to create instability by using many of the key components of traditional conflict, including physical threats, media manipulation and disinformation as well as technological warfare

> We took a big step forward this year as an industry with regard to cyber security and having a forum like Cyber Senate to reflect on our progress and share ideas is a fantastic resource."
>
> *C&I Responsible Engineer, CEng MIET, Nugeneration Ltd*

Taking place at the Marriott Hotel Regents Park in London on 9 & 10th October 2018, the conference – which is made up of a number of presentations, roundtable working groups and panel sessions – will also

explore the intersection between IT and operational technology and how the proliferation of the Internet of Things (IoT) has not only greatly increased capacity for innovation across critical national infrastructure, but also greatly enlarged the scope for devastating cyber attacks.
Key issues to be covered at the event include how to implement effective risk management throughout the supply chain, the latest innovations in detection and mitigation, configuration management and embedding resilience in both critical control systems and business processes.
A key focus across all parts of the event will be cyber security in industrial control systems (ICS), with contributions from experts across the utilities, water, oil & gas, aviation, rail, chemical, nuclear and maritime industries.

Early confirmed speakers and panellists include

Marty Edwards, Managing Director, Automation Federation
Tim Roxy, Chief Security Officer (Interim) and Chief Special Operations Officer, North American Electric Reliability Corporation
Steve Trippier, Chief Information Security Officer, Anglian Water Services
Mo Ahddoud, Chief Information Security Officer, SGN
Martin Fabry, Chief Information Security Officer OT, Mondi Group
Christian Schlehuber, Team Leader CyberSecurity OT, DB Netz
Thomas Murtagh, Technical Information Security Officer, DWR Cymru
Vish Kalsapura, Principal Engineer , Digital Railway, Network Rail
Andre Ristaino, Managing Director, International Automation Association
Representatives of the International Electrotechnical Commission
Chris Blask, Director, Industrial Control Systems Security Unisys, Chair US ICS ISAC
Kim Legalis, CMO, Nozomi
Eric Knapp, Chief Engineer and Global Director of Solutions and Technology, Honeywell
Prashant Pillai, Director, Professor of Cybersecurity, Wolverhampton Cyber Research Institute
Chris Johnson, Head of Computing, University of Glasgow
Mo Javadi, Head of Engineering, Lagoni Engineering
Senior Director, SecurityMatters
Phil Litherland, Principal Consultant, Context Information Security
Cavus Batki, Design Authority cyber security specialist, EDF Nuclear New Build

Discussing the event, James Nesbitt, Director of the event's organiser, Cyber Senate, commented:
"Cyber attacks present a major threat to critical assets and those responsible for defending them need to stay one step ahead in order to ensure the worst doesn't happen.
"Embedding IoT technology in major assets has transformed the operational efficiency of our critical national infrastructure, but it has also opened it up to the threat of potentially catastrophic cyber attacks.

"This event will explore new ways of managing and mitigating this danger by trying to dig deeper into the mind-set and capabilities of hackers and then exploring how robust engineering and maintenance practices can help reduce vulnerability to attacks, both in the design of asset technology and in its ongoing maintenance.

"This is a constantly evolving area on both sides as hackers and those defending our assets strive to improve their technological capabilities as they strive to outsmart each other. We hope that the intelligence this event will provide will help ensure that the right side keeps winning."

The event is supported by a number of strategic partners, including The Automation Federation, the ISA Security Compliance Institute and the International Electrotechnical Commission.

The Cyber Senate are also collaborating with Management Analytics for the Monterey Cyber Security Workshop 2018, October 1st & 2nd, addressing "Influence Operations, Infrastructure protection, Surveillance" See Cybersenate.com for more information.

James Nesbitt
The Cyber Senate
+44 (0)207 096 1754
email us here
