Cevn Vibert CITP MIET MIMC MBCS MISA MISSA MCSA MISACA MIoD

Industrial Cyber Security – Manufacturing, Industry and Critical National Infrastructures.

Speaks "Technical" in "Human".

Speaking/Chairing at Industry Events

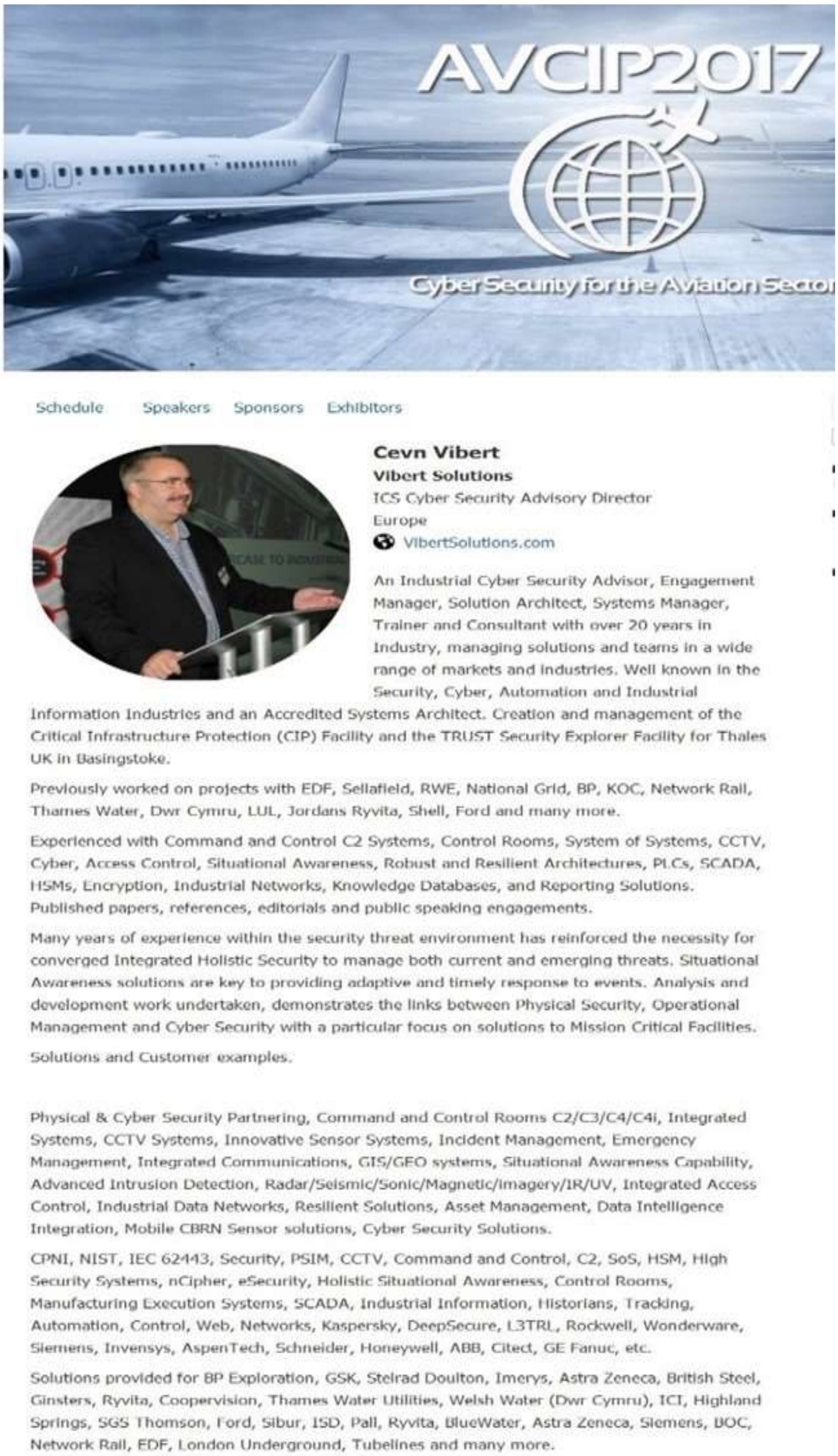
VIBERT SOLUTIONS

A Selection of Speaking Events

Chair: Aviation Cyber Security AVCIP2017

https://aviationcybersecurity2017.sched.com/speaker/cevn

London Nov 2017



Cevn Vibert

Vibert Solutions

ICS Cyber Security Advisory Director

Europe

VibertSolutions.com

An Industrial Cyber Security Advisor, Engagement Manager, Solution Architect, Systems Manager, Trainer and Consultant with over 20 years in Industry, managing solutions and teams in a wide range of markets and industries. Well known in the Security, Cyber, Automation and Industrial Information Industries and an Accredited Systems Architect. Creation and management of the Critical Infrastructure Protection (CIP) Facility and the TRUST Security Explorer Facility for Thales UK in Basingstoke.

Previously worked on projects with EDF, Sellafield, RWE, National Grid, BP, KOC, Network Rail, Thames Water, Dwr Cymru, LUL, Jordans Ryvita, Shell, Ford and many more.

Experienced with Command and Control C2 Systems, Control Rooms, System of Systems, CCTV, Cyber, Access Control, Situational Awareness, Robust and Resilient Architectures, PLCs, SCADA, HSMs, Encryption, Industrial Networks, Knowledge Databases, and Reporting Solutions. Published papers, references, editorials and public speaking engagements.

Many years of experience within the security threat environment has reinforced the necessity for converged Integrated Holistic Security to manage both current and emerging threats. Situational Awareness solutions are key to providing adaptive and timely response to events. Analysis and development work undertaken, demonstrates the links between Physical Security, Operational Management and Cyber Security with a particular focus on solutions to Mission Critical Facilities.

Solutions and Customer examples.

Physical & Cyber Security Partnering, Command and Control Rooms C2/C3/C4/C4i, Integrated Systems, CCTV Systems, Innovative Sensor Systems, Incident Management, Emergency Management, Integrated Communications, GIS/GEO systems, Situational Awareness Capability, Advanced Intrusion Detection, Radar/Seismic/Sonic/Magnetic/imagery/IR/UV, Integrated Access Control, Industrial Data Networks, Resilient Solutions, Asset Management, Data Intelligence Integration, Mobile CBRN Sensor solutions, Cyber Security Solutions.

CPNI, NIST, IEC 62443, Security, PSIM, CCTV, Command and Control, C2, SoS, HSM, High Security Systems, nCipher, eSecurity, Holistic Situational Awareness, Control Rooms, Manufacturing Execution Systems, SCADA, Industrial Information, Historians, Tracking, Automation, Control, Web, Networks, Kaspersky, DeepSecure, L3TRL, Rockwell, Wonderware, Siemens, Invensys, AspenTech, Schneider, Honeywell, ABB, Citect, GE Fanuc, etc.

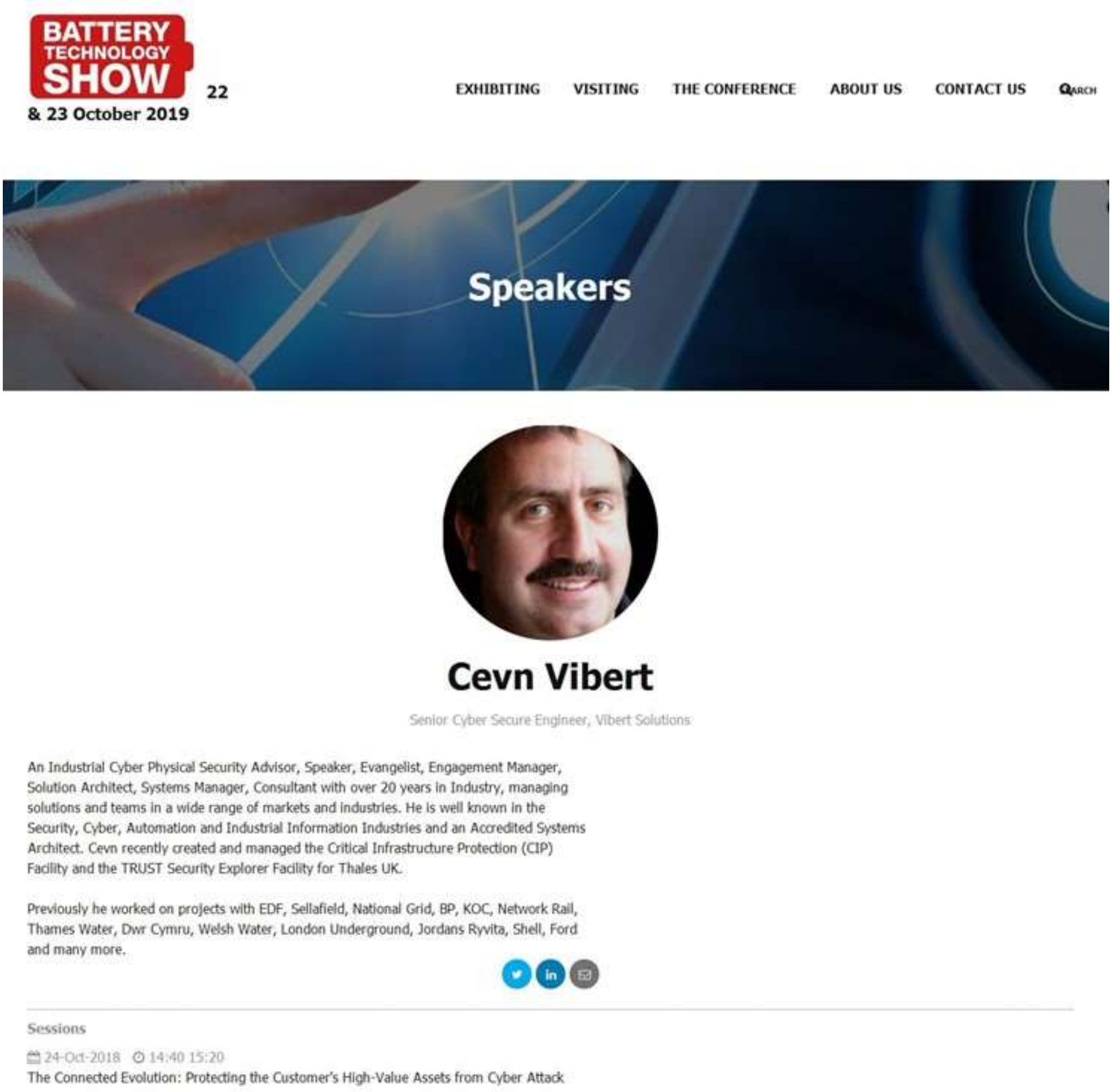
Solutions provided for BP Exploration, GSK, Stelrad Doulton, Imerys, Astra Zeneca, British Steel, Ginsters, Ryvita, Coopervision, Thames Water Utilities, Welsh Water (Dwr Cymru), ICI, Highland Springs, SGS Thomson, Ford, Sibur, ISD, Pall, Ryvita, BlueWater, Astra Zeneca, Siemens, BOC, Network Rail, EDF, London Underground, Tubelines and many more.

Speaker: Battery Technology Show

Excel London

Oct 2019

http://www.batterytechnologyshow.com/speakers/cevn-vibert



Speakers

Cevn Vibert

Senior Cyber Secure Engineer, Vibert Solutions

An Industrial Cyber Physical Security Advisor, Speaker, Evangelist, Engagement Manager, Solution Architect, Systems Manager, Consultant with over 20 years in Industry, managing solutions and teams in a wide range of markets and industries. He is well known in the Security, Cyber, Automation and Industrial Information Industries and an Accredited Systems Architect. Cevn recently created and managed the Critical Infrastructure Protection (CIP) Facility and the TRUST Security Explorer Facility for Thales UK.

Previously he worked on projects with EDF, Sellafield, National Grid, BP, KOC, Network Rail, Thames Water, Dwr Cymru, Welsh Water, London Underground, Jordans Ryvita, Shell, Ford and many more.

Sessions

24-Oct-2018 14:40 15:20

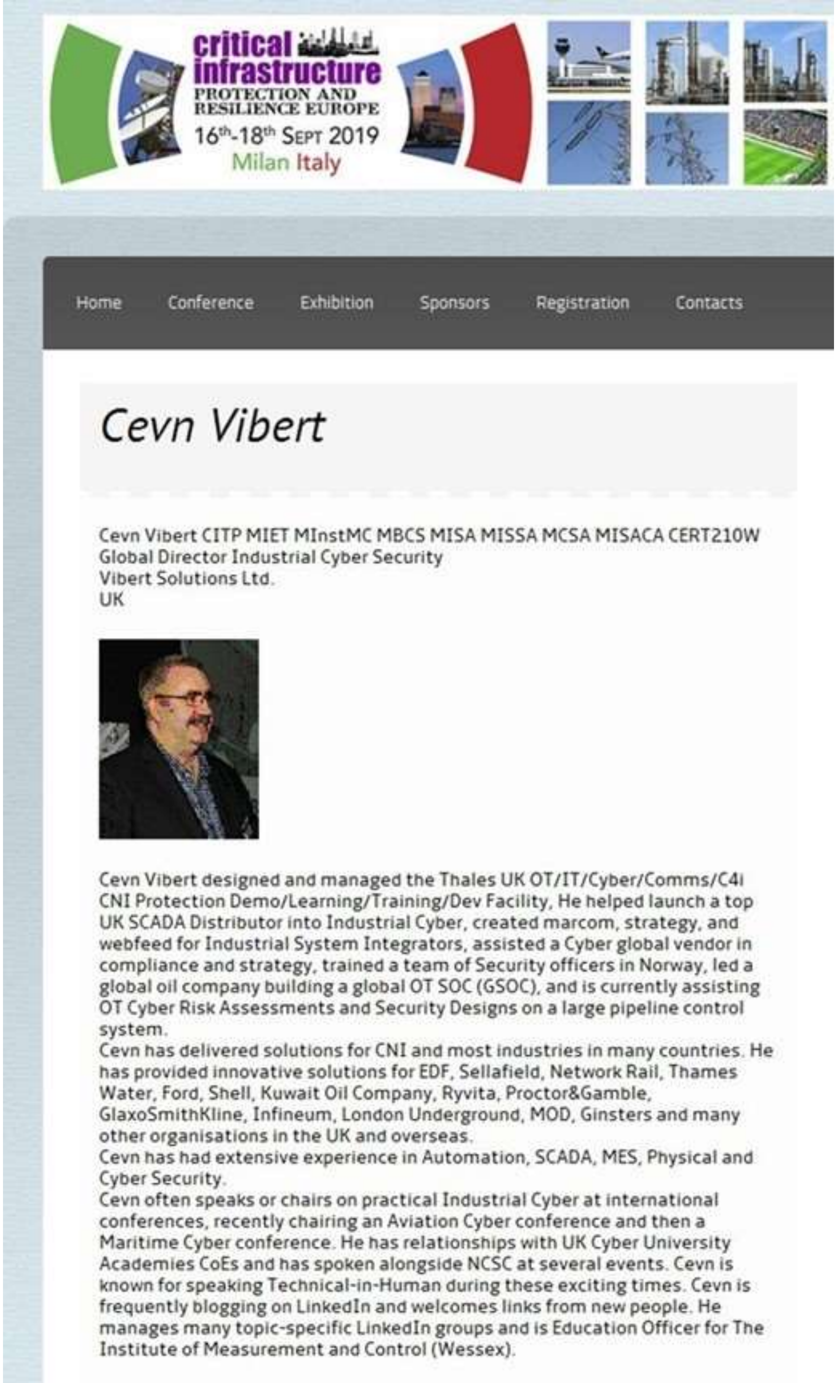
The Connected Evolution: Protecting the Customer's High-Value Assets from Cyber Attack

Speaker: Critical Infrastructure Protection and Resilience Europe

CIPRE The Hague

2018

http://www.cipre-expo.com/cevn-vibert



Cevn Vibert

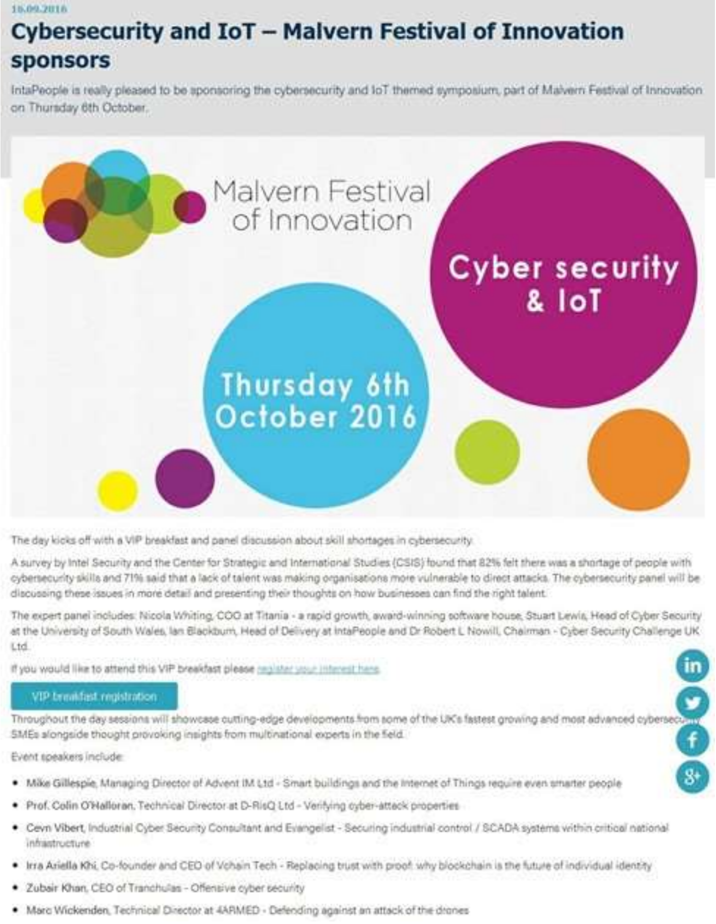
Cevn Vibert CITP MIET MInstMC MBCS MISA MISSA MCSA MISACA CERT210W
Global Director Industrial Cyber Security
Vibert Solutions Ltd.
UK

Cevn Vibert designed and managed the Thales UK OT/IT/Cyber/Comms/C4i CNI Protection Demo/Learning/Training/Dev Facility, He helped launch a top UK SCADA Distributor into Industrial Cyber, created marcom, strategy, and webfeed for Industrial System Integrators, assisted a Cyber global vendor in compliance and strategy, trained a team of Security officers in Norway, led a global oil company building a global OT SOC (GSOC), and is currently assisting OT Cyber Risk Assessments and Security Designs on a large pipeline control system.
Cevn has delivered solutions for CNI and most industries in many countries. He has provided innovative solutions for EDF, Sellafield, Network Rail, Thames Water, Ford, Shell, Kuwait Oil Company, Ryvita, Proctor&Gamble, GlaxoSmithKline, Infineum, London Underground, MOD, Ginsters and many other organisations in the UK and overseas.
Cevn has had extensive experience in Automation, SCADA, MES, Physical and Cyber Security.
Cevn often speaks or chairs on practical Industrial Cyber at international conferences, recently chairing an Aviation Cyber conference and then a Maritime Cyber conference. He has relationships with UK Cyber University Academies CoEs and has spoken alongside NCSC at several events. Cevn is known for speaking Technical-in-Human during these exciting times. Cevn is frequently blogging on LinkedIn and welcomes links from new people. He manages many topic-specific LinkedIn groups and is Education Officer for The Institute of Measurement and Control (Wessex).

Speaker: Cyber Security & IoT - Malvern Festival of Innovation

Malvern Oct 2016

https://www.festival-innovation.com/archives/2016-programme/2016-cyber-security-iot



16.09.2016

Cybersecurity and IoT – Malvern Festival of Innovation sponsors

IntaPeople is really pleased to be sponsoring the cybersecurity and IoT themed symposium, part of Malvern Festival of Innovation on Thursday 6th October.

The day kicks off with a VIP breakfast and panel discussion about skill shortages in cybersecurity.

A survey by Intel Security and the Center for Strategic and International Studies (CSIS) found that 82% felt there was a shortage of people with cybersecurity skills and 71% said that a lack of talent was making organisations more vulnerable to direct attacks. The cybersecurity panel will be discussing these issues in more detail and presenting their thoughts on how businesses can find the right talent.

The expert panel includes: Nicola Whiting, COO at Titania - a rapid growth, award-winning software house, Stuart Lewis, Head of Cyber Security at the University of South Wales, Ian Blackburn, Head of Delivery at IntaPeople and Dr Robert L Nowill, Chairman - Cyber Security Challenge UK Ltd.

If you would like to attend this VIP breakfast please register your interest here.

Throughout the day sessions will showcase cutting-edge developments from some of the UK's fastest growing and most advanced cybersecu
SMEs alongside thought provoking insights from multinational experts in the field.

Event speakers include:

- **Mike Gillespie**, Managing Director of Advent IM Ltd - Smart buildings and the Internet of Things require even smarter people
- **Prof. Colin O'Halloran**, Technical Director at D-RisQ Ltd - Verifying cyber-attack properties
- **Cevn Vibert**, Industrial Cyber Security Consultant and Evangelist - Securing industrial control / SCADA systems within critical national infrastructure
- **Irra Ariella Khi**, Co-founder and CEO of Vchain Tech - Replacing trust with proof: why blockchain is the future of individual identity
- **Zubair Khan**, CEO of Tranchulas - Offensive cyber security
- **Marc Wickenden**, Technical Director at 4ARMED - Defending against an attack of the drones

Securing industrial control / SCADA systems within Critical National Infrastructure

Critical infrastructure, with its complex legacy systems and bolt-on connections to the Internet, sits in a cyber security category of its own. Attacks occupy the boundary between the physical and the cyber-world and are rapidly increasing in number and complexity. The attacks often focusing on industrial systems, production lines, transport and telecommunications networks, hacking into SCADA systems, sometimes through basic tactics such as spear-phishing or malware, before spreading out to manipulate or even disable the infrastructure. As more of a nation's infrastructure becomes interconnected, so the security of basic services is of paramount importance.

Cevn Vibert, Industrial Cyber Security Consultant and Evangelist

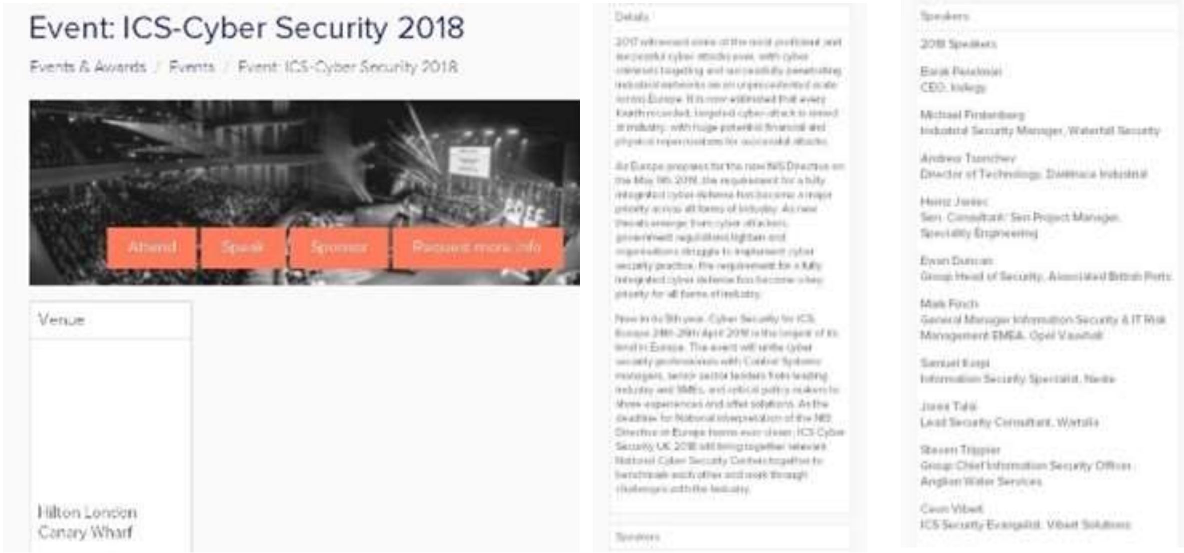
Cevn has over 25 years of experience in Security Solutions, C2, Emergency Management, Industrial Automation and ICS Industrial Information Systems, Manufacturing Production and Industrial Information Solutions, and Critical Infrastructure Protection. Cevn has worked in UK, and places like France, Italy, Norway and Colombia for many systems integrators and blue-chip multinationals.

Speaker: ICS-Cyber Security 2018

London Canary Wharf

April 2018

https://app.qwoted.com/opportunities/event-ics-cyber-security-2018



Event: ICS-Cyber Security 2018

Events & Awards / Events / Event: ICS-Cyber Security 2018

Venue

Hilton London
Canary Wharf

Details

2017 witnessed some of the most proficient and successful cyber attacks ever, with cyber criminals targeting and successfully penetrating industrial networks on an unprecedented scale across Europe. It is now estimated that every fourth recorded, targeted cyber-attack is aimed at industry, with huge potential financial and physical repercussions for successful attacks.

As Europe prepares for the new NIS Directive on the May 9th 2018, the requirement for a fully integrated cyber defense has become a major priority across all forms of industry. As new threats emerge from cyber attackers, government regulations tighten and organisations struggle to implement cyber security practice, the requirement for a fully integrated cyber defense has become a key priority for all forms of industry.

Now in its 5th year, Cyber Security for ICS Europe 24th-25th April 2018 is the largest of its kind in Europe. The event will unite cyber security professionals with Control Systems managers, senior sector leaders from leading industry and SMEs, and critical policy makers to share experiences and offer solutions. As the deadline for National interpretation of the NIS Directive in Europe looms ever closer, ICS Cyber Security UK 2018 will bring together relevant National Cyber Security Centres together to benchmark each other and work through challenges with the industry.

Speakers

Speakers

2018 Speakers

Barak Perelman
CEO, Indegy

Michael Firstenberg
Industrial Security Manager, Waterfall Security

Andrew Tsonchev
Director of Technology, Darktrace Industrial

Heinz Jaskec
Sen. Consultant/ Sen Project Manager,
Speciality Engineering

Ewan Duncan
Group Head of Security, Associated British Ports

Mark Finch
General Manager Information Security & IT Risk
Management EMEA, Opel Vauxhall

Samuel Korpi
Information Security Specialist, Neste

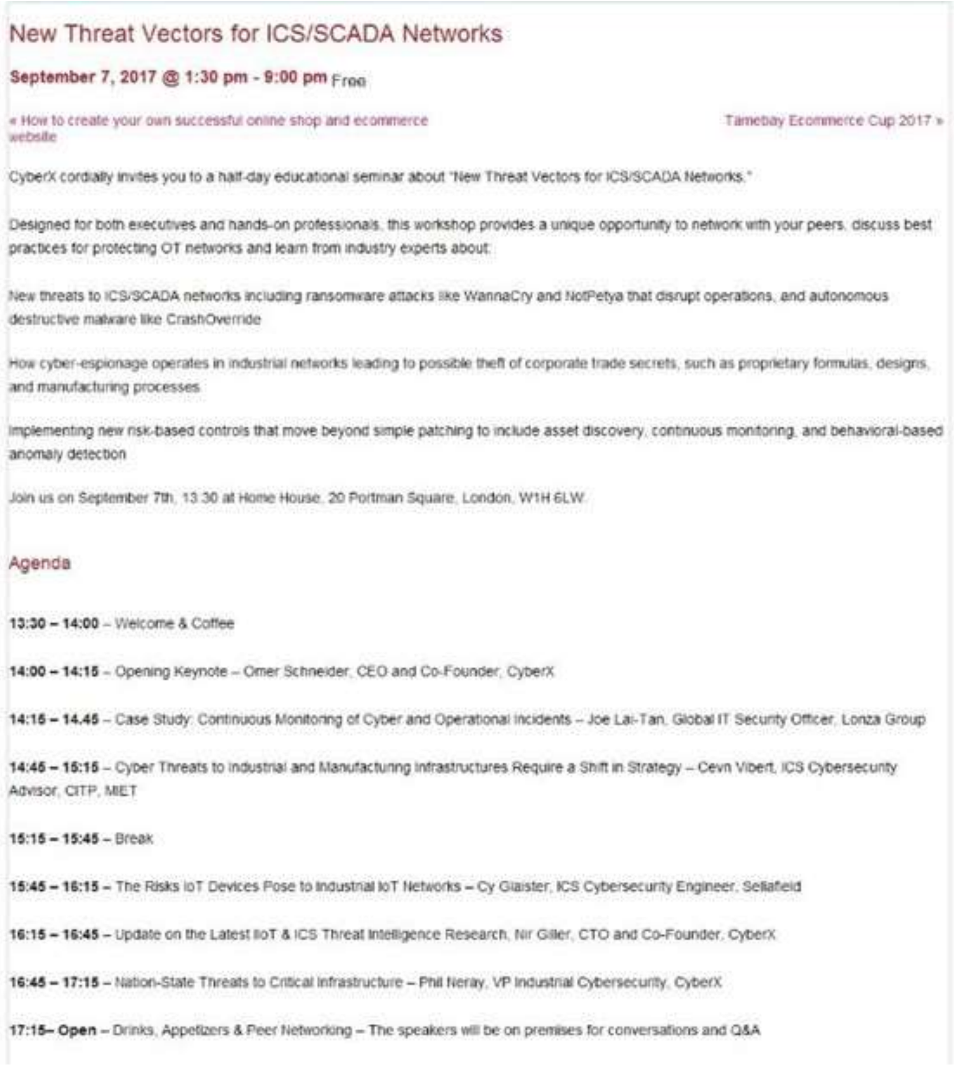
Joona Tala
Lead Security Consultant, Wärtsilä

Steven Trippier
Group Chief Information Security Officer,
Anglian Water Services

Cevn Vibert
ICS Security Evangelist, Vibert Solutions

Speaker: New Threat Vectors for ICS/SCADA Networks

CyberX Conference. London. Nov 2017



New Threat Vectors for ICS/SCADA Networks

September 7, 2017 @ 1:30 pm - 9:00 pm Free

« How to create your own successful online shop and ecommerce website

Tamebay Ecommerce Cup 2017 »

CyberX cordially invites you to a half-day educational seminar about "New Threat Vectors for ICS/SCADA Networks."

Designed for both executives and hands-on professionals, this workshop provides a unique opportunity to network with your peers, discuss best practices for protecting OT networks and learn from industry experts about:

- New threats to ICS/SCADA networks including ransomware attacks like WannaCry and NotPetya that disrupt operations, and autonomous destructive malware like CrashOverride
- How cyber-espionage operates in industrial networks leading to possible theft of corporate trade secrets, such as proprietary formulas, designs, and manufacturing processes
- Implementing new risk-based controls that move beyond simple patching to include asset discovery, continuous monitoring, and behavioral-based anomaly detection

Join us on September 7th, 13.30 at Home House, 20 Portman Square, London, W1H 6LW

Agenda

13:30 – 14:00 – Welcome & Coffee

14:00 – 14:15 – Opening Keynote – Omer Schneider, CEO and Co-Founder, CyberX

14:15 – 14.45 – Case Study: Continuous Monitoring of Cyber and Operational Incidents – Joe Lai-Tan, Global IT Security Officer, Lonza Group

14:45 – 15:15 – Cyber Threats to Industrial and Manufacturing Infrastructures Require a Shift in Strategy – Cevn Vibert, ICS Cybersecurity Advisor, CITP, MIET

15:15 – 15:45 – Break

15:45 – 16:15 – The Risks IoT Devices Pose to Industrial IoT Networks **–** Cy Glaister, ICS Cybersecurity Engineer, Sellafield

16:15 – 16:45 – Update on the Latest IIoT & ICS Threat Intelligence Research, Nir Giller, CTO and Co-Founder, CyberX

16:45 – 17:15 – Nation-State Threats to Critical Infrastructure **–** Phil Neray, VP Industrial Cybersecurity, CyberX

17:15– Open – Drinks, Appetizers & Peer Networking – The speakers will be on premises for conversations and Q&A

Speaker: UK 2017: Roundtable: With the Rise of the Politically Motivated or Sanctioned Attacks

Dec 2017 webinar

In recent times we have seen attacks against victims such as the Ukrainian power grid, which took out the electricity grid for a quarter of a million people, the ransomware attack impacting the NHS system, attributed to actors in North Korea, and that of the Democratic National Committee in the USA, which potentially influenced the outcome of the US presidential elections. Critical infrastructure has become a high-profile target attacked remotely and attributed to state actors, if hackers can gain control over our utilities, critical infrastructure or influence our political systems, what could be the potential outcomes? Is this truly politically motivated or is it just a financial attack masked?

Takeaways:
•What difference does this make, if this is a trend that continues what change will you make in your approach to developing your defences for the future?
•With this changing attack vector, what staff will you need to secure or grow in the future?
•How does this change what capabilities you will need?

Recorded Dec 12 2017 54 mins

Presented by
Paul Taylor Senior Partner, Risk Consulting, KPMG
Dr. Ciarán Mc Mahon
Cevn Vibert
Mark Stokes
Ibukun Adebayo
Joe Hancock

Speaker: ICS Cyber Security Conference 2017

April 2017 London

2016 saw cyber criminals continue to become ever smarter, more efficient and increasingly successful at penetrating industrial networks. This was seen with ICS operators reporting more security incidents to the authorities than in any year previous.
As the potential attacks on water, electricity and other features of a nation's critical infrastructure are being increasingly linked to international cyber criminals, security practices within private companies are becoming public business – as such practitioners must scrutinise their operations in order to minimise their exposure to such attacks.
Cyber Security for ICS, Europe **25th – 27th April 2017** is the must attend event that will unite cyber security professionals with Control Systems managers and SMEs to address the key challenges faced in the market

Why Should You Attend?

- Benefit from a panel of speakers with a wide range of expertise, including SCADA controllers, Plant Managers and Heads of Information Security, at some of the world's biggest companies, in sectors ranging from Energy to Transport to Manufacturing
- Learn about the guidelines and legislation being developed to monitor and control the quality of the cyber security solutions protecting these ICSs
- Further your understanding of the current solutions available in the market and how they can protect your control systems from malicious intrusions
- Hear an update on the developing cyber threats to ICSs, both human and technical, in the world today

2017 Speakers

- Abeed Hossain, Global Director, IT Operations and Infrastructure Services, INEOS Styrolution Group GmbH
- Steven Trippier, Senior Manager – Global Product Security, Anglian Water
- Alan Capon, SCADA & Communications Engineer Network Services – Asset Management, manx utilities
- Jeff Melrose, Principal Cyber Security Manager, Yokogawa
- James Curran, Control Systems Engineering, Electrical Engineering, European Space Agency
- Mike Mackintosh, IT Manager, Barhale
- Chris Rivinus, Head of Business Systems, Tullow Oil
- Wendy Arrowsmith, Business Security Liaison, National Grid
- William Horner, Process Automation Consultant, Horner Technologies
- Cevn Vibert, Vibert Solutions
- Rossella Mattioli, Security and Resilience of Communication Networks Officer, ENISA
- Stephen Cummins, Head of Rail Cyber Security, Department for Transport
- William Fitzgerald, Senior Manager – Global Product Security, Tyco
- Confirmed Speaker, Senior Representative, National Cyber Security Centre
- Trevor Goldman, Industrial Systems Architect, Waterfall Security Solutions
- Alexander Wood, Cyber Security Account Manager, Darktrace
- Shmulik Aran, Chief Executive Officer, NextNine

Speaker: ISC2 Event London Dec 2017

https://blog.isc2.org/isc2_blog/2017/12/exploring-industrial-cyber-physical-security-enhancement.html

By Cevn Vibert, ICS Industrial Cyber Physical Security Advisor

Cevn will be hosting the session Grass Roots Industrial Control Security at (ISC)² Secure Summit UK, between 12th and 13th December 2017.

The industrial cybersecurity market is facing rapid changes as more threats are discovered, more impact is felt by end-users and cybersecurity vendors vie for leadership.

My session will highlight both alerts and advice for end-users of automation and control systems (ICS/OT), as well as selected advisory notes for practitioners of Industrial Cyber Physical Security. Strategic methodologies and programmes of activities for mitigation of impacts on IIOT, IOT and how holistic integrated security can provide comprehensive situational awareness will additionally be provided. Multiple types of security are addressed, together with some mythical attack and defence scenarios. The history of industrial cyber-attacks are mentioned briefly, to counterpoint the prevalent myths of defence, and finally some alerts to the cyber arms race.

End-users face increased pressure to improve their security stance, and I will discuss some successful methods for implementing these improvements including a “stairway”, a “jigsaw” and an “A-Team”.

The cyber physical bad guys are now attacking IOT and IIOT. They are constantly getting better at attacking, so the good guys must also constantly get better at defending. There is much evidence that most good guys have not even properly started to improve their security stance yet, so my session will be a serious ‘call-to-action’ too.

Our modern society is built on automation, control systems and their management. The “Things”, mentioned often in the Internet of Things (IOT) and the Industrial Internet of Things (IIOT), are becoming smarter and more ubiquitous. If you think about all the automation controlled “Things” that have contributed to your day and try to list them, you may be surprised and perhaps a little worried to know that they are also being invisibly attacked.

Food manufacturing, transport (planes, trains, automobiles etc.), clothing, water treatment, waste processing and management, pharmaceutical manufacturing and testing, logistics, medical device manufacturing, energy (generation, transmission and distribution), power, defence, hospitals, cashpoints, and beverage dispensers are just some of the examples of the vast variety of “Things” in our personal lives.

Critical national infrastructures are under immense pressure from Government, regulators, and themselves to enhance their defences, improve cyber monitoring and to re-work the gargantuan quantities of legacy systems. This is not an easy task with industrial IT, due to a range of largely legacy problems. The aging and legacy Industrial systems were not designed to be monitored and interrupted and scanned by active defence solutions. These security problems are both procedural, legislative and technical, so all end-users are now having to review remediation against enormous business and operational risks.

The rise in attacks on these 'Things' has started to concern people. National Infrastructures are investing in improvement plans, many markets are ahead of the game, but so much more is needed to be done. Meanwhile the bad guys get better at the attacking.

We now know of so many new cyber perpetrators or threats, that there is a veritable 'cyber zoo' of attackers: Yetis, Bears, Dragons, Dragonfly, Worms, Penguins and more.… A whole new cyber genus is perhaps yet to come?

There are also many new words and references in our evolving cyber weapons vocabulary: Cyber Zombies, Watering holes, Slammer, Nachi, Mahdi, Shamoon, Red October, Petya, ShadowBrokers, Conficker, Duqu, Flame, Havex, APTs, Blasters, Dumpsters, Drive-bys, Honeypots, Pastebin, Phishing, BotNets, Trojans, Heartbleed, Modbus, CANbus and more are all being aired or created on social media and on news sources around the world.

Many conferences now are haranguing the audience as being 'incompetent', merely in tongue-in-cheek, but still aiming at both the vendors and integrators who do not implement security-by-design in their products and systems together with the security industry which has not yet eradicated cyber-attacks by leap-frogging the bad guys with new innovative defences and solutions.

The steps to climb the stairway to security can be very high, certainly for organisations with extensive legacy systems, but the steps do need to be climbed, and sooner rather than later. The best approach is often to build small steps, parallel steps and think differently.

Remember, the bad guys are always improving, so it is essential for organisations to also keep improving, but more than that, looking for that giant leap ahead in defences. There is talk of new secure operating systems, new secure trusted computer systems, and of the increased lock-down and monitoring of The Internet. While all these advances are being made, are they appearing on the market quickly enough to make that giant leap forward in the cyber arms race?

The industry must now stop talking about Stuxnet and start talking about innovation and new ways of thinking. Keynote speakers are talking about the soft skills of the cyber war. Cyber-attacks are made by humans, often exploiting human weaknesses as key building blocks of their attacks. The cyber defence industry must therefore recognise this more and build security improvement programmes which include humans as the core to the solution.

Speaker: Cyber days in London

05th December 2017

Artificial Intelligence, the IOT (Internet of Things) and compliance with GDPR are among the topics for (ISC)2 – the US-based not-for-profit membership body of cyber, information, software and infrastructure security people – at their Secure Summit UK in London, on December 12 and 13.

Speakers include Paul Taylor, Partner at the audit firm KPMG and Mark Stokes, Head of Digital and Electronics Forensic Services at the Metropolitan Police.

In the wake of the attacks on Ukraine's nuclear plants, the summit has a session examining cybersecurity in industrial control systems by Cevn Vibert, who has worked on cybersecurity projects with clients including Thames Water, Network Rail and Sellafield.

With the full force of the EU-wide general data protection regulation (GDPR) months away in May 2018, some attendees will participate in a workshop aimed at charting cybersecurity professionals' experiences on the road to GDPR, led by David Higgins and Yves Le Roux. Other confirmed speakers include Ken Munro, Founder of Pen Test Partners Ltd, James Packer, Cybersecurity and Cloud Specialist at KPMG and Joe Hancock, Cybersecurity Lead at the law firm Mishcon de Reya. A workshop on Security Awareness, Behaviour and Culture, will cover how to educate the biggest component of cybersecurity – people.

Dr Adrian Davis, Managing Director for EMEA at (ISC)² says: "As the world's largest body of cybersecurity professionals, we have a significant opportunity and a responsibility to bring together cross-sector, front-line cybersecurity expertise, spanning governments, multinational companies, academia and those at the forefront of law enforcement to shine a light on the very latest threats and trends within our digital economy. Our summits draw on a unique breadth of talent and experience to inform policies and help businesses and governments alike contend with the major issues of our time, while looking forward to the future. Secure Summit UK is the last of five Secure Summits, a series of two-day events hosted by (ISC)2 within the EMEA region this year. Each event features varied sessions designed to showcase a range of perspectives and levels of practice, including hands-on cyber workshops to keynotes and panels with technology industry leaders tasked with protecting banks, governments and multinationals."

Secure Summits are free to members of (ISC)2. The UK event is sold out; recordings of select sessions will be available through the (ISC)2 EMEA webinar channel. For more information, or to register for and watch recordings of other (ISC)² Secure Summits, visit: https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars/EMEA-Recordings.

Institute of Measurement and Control

Speaker: Industrial Cyber Security for Measurement & Control Systems Seminar

- Date: 06 June 2018
- Subject: Industrial Cyber Security for Measurement & Control Systems
- Presenter: Cevn Vibert, Vibert Solutions Ltd
- Location: University of Southampton, Building 19, Room 3011 (Nav Post code SO17 1BJ)

https://www.instmc.org/Special-Interest-Groups/Cyber-Security

A new Special Interest Group (SIG) has just been launched in the Institute of Measurement and Control (InstMC).

The Institute members have shown great interest in the hot topic of Industrial Cyber Security. The security of IIoT, Industrial Automation Control Systems (IACS), Supervisory Control and Data Acquisition Systems (SCADA), Distributed Control Systems (DCS) and Intelligent Electronic Devices (IEDs) are all under threat from Cyber Security Attacks and mistakes.

Safety Systems could also be impacted with the results of cyber-attacks being very much in the global news media.

The initial scope of work for the SIG is listed below:

- The SIG will promote greater understanding of the rapidly evolving subject, assist with learning aspect, ratification of education programs and providers, offer thought leadership and promote expertise and awareness amongst its membership and the wider community.
- The SIG will provide representation at conferences and collaborative meetings, papers and guides, roadshows and knowledgeable subject matter content internally and externally.
- The specialised nature of Industrial Cyber Security together with the rise in public awareness should also assist in providing attractiveness to new membership
- The SIG will provide a user base for regular meetings and shared information to our community.

The SIG is currently supported by a growing group of InstMC volunteers and led by co-Chairs :- Cevn Vibert of Vibert Solutions Consultancy and Dil Wetherill of =Method Safety and Security

InstMC is a member of the Alliance of cyber security professionals which brings together most of professional bodies in the UK working in this area.

Speaker: SOS Security – Norway

Cyber Security – Breakfast Briefing – 2 hours

March 2017 - Yttersø Businesspark

This Exclusive Breakfast Briefing is a basic introduction high-level view of Cyber Security.
Suitable for Business Leaders, Management and Engineers tasked with enhancing security.
The Breakfast Briefing is a taster on the current threats, some technologies and services to mitigate the threats, and an introduction to security enhancement strategies. The Briefing is usually a 1 hour presentation, and a 1 hour round-table discussion tailored to suit the audience.

· Traditional IT systems and rising threats in the news
· Cyber, Operational and Physical Security convergence
· Cyber Attack Surfaces
· Risk, Threats, Vulnerabilities and Impacts
· Cyber security incident management
· Cyber Security mitigation programmes
· Security enhancement strategies

Courses are delivered by Cevn Vibert.
An Industrial Cyber Physical Security Advisor, Speaker, Evangelist, Engagement Manager, Solution Architect, Systems Manager, Consultant with over 20 years in Industry, managing solutions and teams in a wide range of markets and industries. He is well known in the Security, Cyber, Automation and Industrial Information Industries and an Accredited Systems
Architect. Cevn recently created and managed the Critical Infrastructure Protection (CIP) Facility and the TRUST Security Explorer Facility for Thales UK.
Previously he worked on projects with EDF, Sellafield, National Grid, BP, KOC, Network Rail, Thames Water, Dwr Cymru, Welsh Water, London Underground, Jordans Ryvita, Shell, Ford and many more.
Experienced with Industrial IT, Industrial IOT, Command and Control C2 Systems, Control Rooms, System of Systems, CCTV, Cyber, Access Control, Situational Awareness, Robust and Resilient Architectures, PLCs, SCADA, HSMs, Encryption, Industrial Networks, Knowledge Databases, and Reporting Solutions. Throughout his career has produced many papers, references, editorials and industry speaking and chairing engagements.
Years of experience within the security threat environment has reinforced the necessity for converged Integrated Holistic Security to manage both current and emerging threats.
Situational Awareness solutions are key to providing effective and timely response to incidents at Mission Critical facilities.

Advises and presents to CxOs, Boards, Management or shop-floor teams on many security and industrial information subjects such as: -
· SCADA and Automation basics.
· MES/ Middleware/MOM for business benefits.
· Industrial ICS IIOT Cyber Security basics.
· Industrial ICS IIOT Cyber Security advanced.
· Basic high level Risks and Information Assurance in Industrial Control Systems.
· Building winning teams for Industrial Cyber Security programmes.
· The Stairway to Security.
· Holistic Integrated Security - the Security Convergence Revolution.
· The Security Jigsaw - Onion Rings - The Architectures of Defence.
· Assisting companies to select and engage with new partners for Cyber Security, Physical Security, MES/MOM and Automation.
· The cultures of Customer and Partner engagements.
· Engaging and aligning collaboration with Academia.
· Innovation.
· Building Demonstration Facilities.
· Business Development for Engineers.
· Training your teams and others.
· Evangelising - Companies, Products and Services

Speaker: Kaspersky Press Event

London – British Science Museum 2016

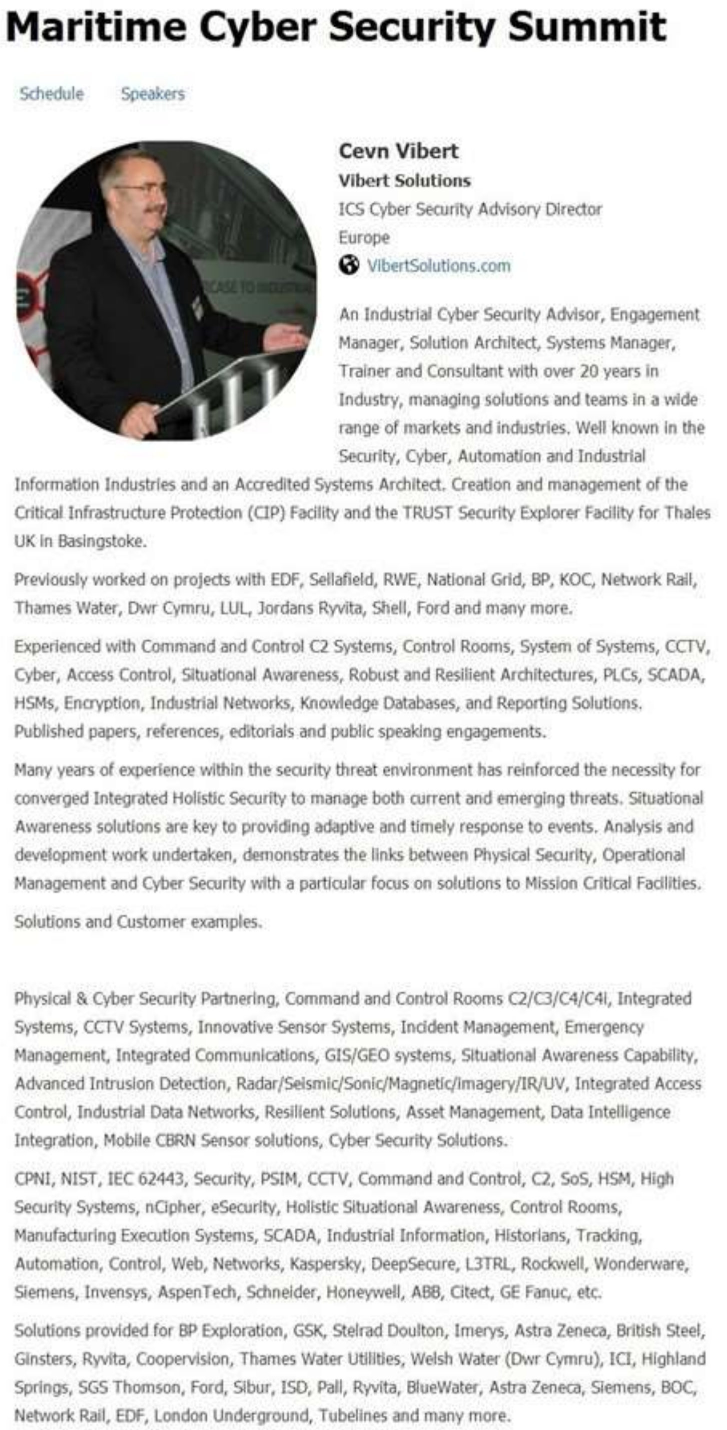
LONDON (UK). On 14th April 2016 at the Science Museum, a selected panel of experts, among which **Eugene Kaspersky, CEO and founder of Kaspersky Lab** Jose Palazon, CTO of Eleven Paths/Telefonica, Andrew Comer of Institute of Engineering member and partner at Buro Happold, **Cevn Vibert,** Industrial Control Systems Security Consultant and Andrea Tonini, Sales Director of BM Group, discuss and debate the cyber threats to critical infrastructure which seek to disrupt communications, transport, utilities and industrial industries in Britain today. British press had the chance to hear insight on assessing the potential dangers and how organisations operating in such industries might deploy defences to reduce risk and build a more resilient nation. Over 30 journalists present (BCC, THE DAILY MAIL, ZDNET, FINANCIAL TIMES, and more).

Full Panel video

https://www.youtube.com/watch?v=2uCBPMFXCTs&nobanner=1

Chair: Maritime Cyber Security Conference

London Mar 2018



Maritime Cyber Security Summit

Schedule Speakers

Cevn Vibert

Vibert Solutions

ICS Cyber Security Advisory Director

Europe

VibertSolutions.com

An Industrial Cyber Security Advisor, Engagement Manager, Solution Architect, Systems Manager, Trainer and Consultant with over 20 years in Industry, managing solutions and teams in a wide range of markets and industries. Well known in the Security, Cyber, Automation and Industrial Information Industries and an Accredited Systems Architect. Creation and management of the Critical Infrastructure Protection (CIP) Facility and the TRUST Security Explorer Facility for Thales UK in Basingstoke.

Previously worked on projects with EDF, Sellafield, RWE, National Grid, BP, KOC, Network Rail, Thames Water, Dwr Cymru, LUL, Jordans Ryvita, Shell, Ford and many more.

Experienced with Command and Control C2 Systems, Control Rooms, System of Systems, CCTV, Cyber, Access Control, Situational Awareness, Robust and Resilient Architectures, PLCs, SCADA, HSMs, Encryption, Industrial Networks, Knowledge Databases, and Reporting Solutions. Published papers, references, editorials and public speaking engagements.

Many years of experience within the security threat environment has reinforced the necessity for converged Integrated Holistic Security to manage both current and emerging threats. Situational Awareness solutions are key to providing adaptive and timely response to events. Analysis and development work undertaken, demonstrates the links between Physical Security, Operational Management and Cyber Security with a particular focus on solutions to Mission Critical Facilities.

Solutions and Customer examples.

Physical & Cyber Security Partnering, Command and Control Rooms C2/C3/C4/C4I, Integrated Systems, CCTV Systems, Innovative Sensor Systems, Incident Management, Emergency Management, Integrated Communications, GIS/GEO systems, Situational Awareness Capability, Advanced Intrusion Detection, Radar/Seismic/Sonic/Magnetic/imagery/IR/UV, Integrated Access Control, Industrial Data Networks, Resilient Solutions, Asset Management, Data Intelligence Integration, Mobile CBRN Sensor solutions, Cyber Security Solutions.

CPNI, NIST, IEC 62443, Security, PSIM, CCTV, Command and Control, C2, SoS, HSM, High Security Systems, nCipher, eSecurity, Holistic Situational Awareness, Control Rooms, Manufacturing Execution Systems, SCADA, Industrial Information, Historians, Tracking, Automation, Control, Web, Networks, Kaspersky, DeepSecure, L3TRL, Rockwell, Wonderware, Siemens, Invensys, AspenTech, Schneider, Honeywell, ABB, Citect, GE Fanuc, etc.

Solutions provided for BP Exploration, GSK, Stelrad Doulton, Imerys, Astra Zeneca, British Steel, Ginsters, Ryvita, Coopervision, Thames Water Utilities, Welsh Water (Dwr Cymru), ICI, Highland Springs, SGS Thomson, Ford, Sibur, ISD, Pall, Ryvita, BlueWater, Astra Zeneca, Siemens, BOC, Network Rail, EDF, London Underground, Tubelines and many more.

Our Chairman and Moderator
Cevn Vibert, ICS Cyber Security Advisory
Director, Vibert Solutions Limited

Speaker: International Nuclear Industry Security Conference

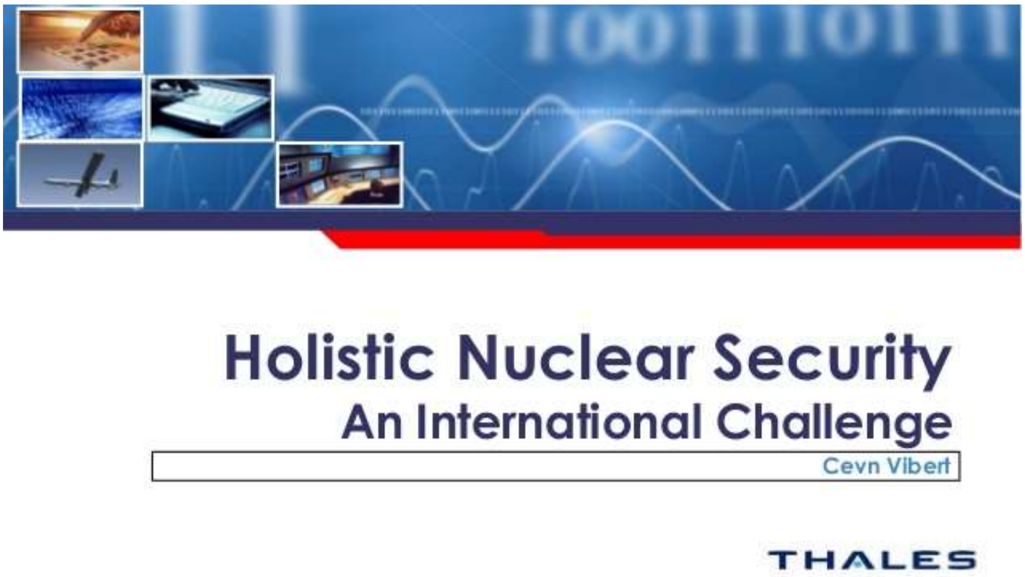
London 2014

Holistic Nuclear Security – An International Challenge

Cevn Vibert CITP MIET MInstMC MBCS. Solutions Architect & CNI Facility Manager Security and Consulting Thales UK

Cevn has over 25 years in Industry in a wide range of markets and industries. Projects with EDF, Sellafield, RWE, National Grid, BP, KOC, LUL and Network Rail, together with Thames Water, Dwr Cymru, and many more. Experienced with Command and Control C2 Systems, Control Rooms, System of Systems, CCTV, Access Control, Situational Awareness, Robust and Resilient Architectures, PLCs, SCADA, Industrial Networks, Knowledge Databases, Incident Management, CBRN systems, Emergency Management, Reporting Solutions, Communications and Mobile Systems. Years of experience within the security threat environment has reinforced the necessity for integrated holistic security to manage current and emerging threats. Situational Awareness solutions are key to providing adaptive, effective and timely response to events.

Cevn designed and Manages the Thales UK CNI Security Facility.



Holistic Nuclear Security

An International Challenge

Cevn Vibert

THALES

Speaker: ICS Cyber Security

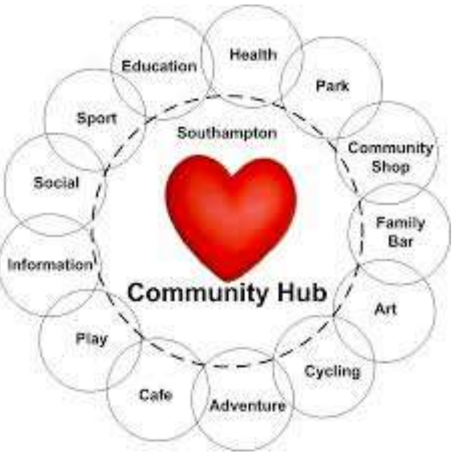
Cranfield Chevening Fellows

2016

Cevn Vibert: I had the pleasure to speak with the Chevening Fellows this week.

Spoke about ICS Cyber Security market and methodologies, the challenges and the current thinking and advice. The Fellows shared their views on experience from Defence Marine, IT Cyber Security, Legal and a range of professions. Some great Q&A. Many thanks for the beautiful gifts from the group. Wishing you well in your careers.

Other Community work and Projects



"Cyber risk reviews must consider IT in your facilities such as aircon, lifts, doors, alarms & CCTV - not just networks."
CEVN VIBERT
• Industrial Cyber Security Advisory Director, Vibert Solutions Ltd •

VIBERT SOLUTIONS

The 2017 Cyber Security
Game Experience Tour
Vibert Solutions
De Montfort University Leicester
Kaspersky lab
Lancaster University
Roke
Part of the Chemring Group
University of Southampton

Industrial Cyber Security Network
Cevn Vibert
+447909 992786
cevn@vibert.co.uk

Inst
MC

Abstracts

Cevn Vibert designed and managed the Thales UK OT/IT/Cyber/Comms/C4i CNI Protection Demo/Learning/Training/Development Facility, He helped launch a top UK SCADA Distributor into Industrial Cyber, created marcom, strategy, and webfeed for Industrial System Integrators, assisted a Cyber global vendor in compliance and strategy, trained a team of Security officers in Norway, led a global oil company building a global OT SOC (GSOC) with new NIST GRC, and assisted OT Cyber Risk Assessments and Security Designs on a large pipeline control system.

Cevn has delivered solutions for CNI and most industries in many countries. He has provided innovative solutions for EDF, Sellafield, Network Rail, Thames Water, Ford, Shell, Kuwait Oil Company, Ryvita, Proctor & Gamble, GlaxoSmithKline, Infineum, London Underground, MOD, Ginsters and many other organisations in the UK and overseas.

Cevn has had extensive experience in Automation, SCADA, MES, Physical and Cyber Security.

Cevn often speaks or chairs on practical Industrial Cyber at institute, government and international conferences, recently chairing an Aviation Cyber conference and then a Maritime Cyber conference. He has relationships with UK Cyber University Academies CoEs and has spoken alongside NCSC at several events. Cevn is known for speaking Technical-in-Human during these exciting times. Cevn is frequently blogging on LinkedIn and welcomes links from new people. He manages many topic-specific LinkedIn groups and is Education Officer for The Institute of Measurement and Control (Wessex) and co-Chair of the InstMC Cyber Special Interest Group SIG.

Vibert Solutions advises, consults, trains and presents to C-suite, boards, senior management or shop-floor teams at mission critical facilities in all aspects of industrial information and control security.

Cevn Vibert CITP MIET MIMC MBCS MISA MISSA MCSA MISACA MIoD
Global Director ICS Industrial Cyber Security.
Vibert Solutions Limited.
24 Lumsden Ave, Southampton. UK. SO15 5EL
Registered Company: 10438532
VAT Reg. 279635452
cevn@VibertSolutions.com
https://www.vibertsolutions.com
+44(0)7909 992786
https://www.linkedin.com/in/vibertprofile

Other speaking events:

Deep Secure at Breakfast Briefing London, 1 Victoria Street. – April 2016

NCSE - UK CNI Research Program Event London, 1 Victoria Street.

ICS Europe Cyber Senate (Multiple Chair and Speaking events)

CSC 2016 Conference, North West Cyber Cluster, Blackpool 2016 (with Langer)