CONFERENCE DAY 1 - Tuesday 29 January 2019

08:00 Registration and refreshments

08:45 Opening address from the chair

Yugo Neumorni
Board Member and Chairman of the Cybersecurity Council, EuroCIO Association

09:00 Intrusion Detection Systems (IDS) Roadmap – making IDS a key pillar of your OT cybersecurity strategy to maximise return on investment as security demands evolve in tandem with the Smart Grid

- Leveraging the rapid growth and improvement of IDS technology to better monitor and protect your network control environment in the face of an evolving threat landscape
- Ensuring the readiness of an empowered CISO and technically adept cybersecurity team prepared to face the challenges of procuring and handling new technology and optimise investment
- Exploring a broad range of anomaly detection tools and technologies, thoroughly evaluating them to ensure the best possible fit with your control system environment
- Prioritising high-value IDS use cases to protect your engineering and operational systems as they are integrated into a more connected and digital world
- Providing a clear and considered roadmap to guide decisions and capitalise on IDS, allowing the benefits of a smarter grid to grow unimpeded by security threats

Yugo Neumorni
Board Member and Chairman of the Cybersecurity Council, EuroCIO Association

09:45 Maximising Board Support – translating technical risks and opportunities into a compelling business case for full investment in IDS

- Turning abstract concepts such as threats and vulnerabilities into a concrete risk assessment and demonstrating a compelling business case to prioritise IDS as a key part of your cybersecurity programme
- Leveraging regulatory frameworks including the NIS directive to emphasise the compliance risks associated with a failure to fully secure your critical systems
- Utilising pertinent examples of recent cybersecurity incidents to highlight the growth and evolution of malicious activities globally and demonstrate how IDS can prevent future catastrophes
- Learning from recent deployments to provide realistic projections for IDS investment in order to mitigate fears of spiralling costs
- Securing timely and significant budget allocation to rapidly establish IDS at the core of Smart Grid cybersecurity

Philip Tonkin
Global Head of Cyber Operational Technology, National Grid

10:30 Morning refreshments, exhibition and networking

11:00 Organisational Alignment Panel – ensuring collaboration and cooperation between relevant business units to implement your IDS solutions holistically and maximise their benefits

- Overcoming organisational, technical, and cultural barriers to ingrain an inclusive cybersecurity framework which allows IDS implementation without disrupting the availability of critical systems
- Facilitating and motivating collaboration between OT and IT specialists to leverage their specific expertise without diminishing their functional specialism
- Aligning the implementation of IDS systems at a local scale with the overall strategy and roadmap developed at the highest levels of your organisation
- Working with other utilities and cross-industry partners to share experience and minimise “reinventing the wheel” when building your capabilities and configuring your IDS
- Bringing managers, specialists, and end-users together to make sure that IDS is installed effectively and that the corresponding cybersecurity benefits are realised for the whole company

Agustin Valencia Gil-Ortega
OT Cybersecurity, Iberdrola

Nuno Pereira
OT Cyber Security Officer, EDP Distribuição
Philip Tonkin
Global Head of Cyber Operational Technology, National Grid

11:45 Cyber Impact Assessment – evaluating methods to quantify the business impact of industrial cyber threats and effectively mitigate them

12:30 Lunch, exhibition and networking

14:00 IDS Procurement – designing a thorough and efficient procurement process assessing multiple vendors to select the best solutions and partners for your business

- Setting out well-defined procedures for comparing different IDS solution providers and establishing their fit with your organisation, processes and existing systems
- Developing a comprehensive set of functional requirements and criteria to effectively benchmark different vendors and their portfolios of solutions
- Exploring different strategies and techniques for evaluating vendor solutions and setting up a testing procedure which assesses their technical performance, company fit, and robustness for future requirements
- Engaging key representatives from across your business in the procurement process to ensure maximum buy-in and a robust implementation
- Setting out a rigorous procurement process which maximises return on your investment and fully engages your whole business

Erik Poder
Managing Project Manager, Elektrilevi

14:45 IDS Implementation and Integration – optimising IDS deployment to maximise effectiveness while minimising both investment and potential disruption to critical network operations

- Minimising disruptions while deploying IDS to optimise security while reducing organisational risk
- Appraising your existing architecture and the traffic patterns of your control systems to guide the deployment of your chosen IDS solution
- Fully leveraging the experience and knowledge contained in your control room to get a complete picture of your control architecture and establish how best to integrate IDS
- Balancing the desire for full IDS deployment with the need to minimise or eliminate downtime for your critical systems during implementation
- Identifying areas of particular vulnerability and prioritising their protection to support IDS deployment to the most impactful locations
- Planning for further network decentralisation and likely movement away from traditional star network topology to ensure your IDS provides reliable functionality as the network evolves

Nuno Pereira
OT Cyber Security Officer, EDP Distribuição

15:30 Afternoon refreshments, exhibition and networking

16:00 OT Vulnerability Testing – performing vulnerability tests on OT devices to stress-test the security of your network and address weaknesses

- Performing rigorous tests which are representative of real-world attacks to simulate performance in the real-world threat landscape
- Stressing the importance of software resilience as a key component of overall system security
- Working with vendor equipment to check and test its security performance before introducing it into your network environment
- Drawing on real-world examples of attacks from the field to accurately simulate threats and utilising reverse engineering and vulnerability research to test critical devices
- Managing risk through thorough testing to establish what devices to use, decide how to apply patches and fixes, and identify weak links

Dani Grabois
Security Senior Principal, Accenture Security

16:45 Standards Development – supporting the development and adoption of communications protocols to improve the security and interoperability of network systems and devices across the grid

- Developing the Open Grid Standard Protocol to support the smooth integration of IDS
- Providing greater value to utilities through independently-certified, multi-vendor interoperability
- Processing vast quantities of data from remote IoT deployments throughout the network
- Analysing data using algorithms and rules to identify anomalous behaviour and potential threats
- Fostering collaboration in the utility domain to ensure a well-integrated and secure Smart Grid

Mark Ossel
Vice President, Networked Energy Services Corporation & Board Member Member, OSGP

17:30 Roundtable discussions

19:00 Networking drinks

20:30 End of conference day one

CONFERENCE DAY 2 - Wednesday 30 January 2019

08:00 Registration and refreshments

08:45 Welcome back from the chair

Bas Kruimer
Senior Manager, Accenture Security

09:00 IDS Functionality – understanding the core functionalities of next-generation IDS and examining the different techniques that underpin these

- Investigating different types of IDS solution and implementation based on their ability to reliably deliver key functionality and value-adding benefits
- Comparing NIDS and HIDS implementations based on their suitability for your network architecture, including factors such as effectiveness, cost, and ease of use
- Evaluating the fit for purpose of more traditional signature-based IDS, compared with the capabilities of other technologies including protocol or pattern-based software
- Deploying advanced systems capable of communicating actively with control components to improve the depth of anomaly detection beyond traffic analysis
- Ensuring your IDS solution is supported by the most advanced and futureproof technology to guarantee reliable and consistent performance

Agustin Valencia Gil-Ortega
OT Cybersecurity, Iberdrola

09:45 Risk-Based Threat Detection – identifying and fully evaluating typical cybersecurity risks to utility OT networks and developing fully managed solutions

- Utilising developments in artificial intelligence to increase the autonomy and accuracy of IDS solutions
- Exploiting AI's inherent capabilities for processing and analysis to deal with the growing volume and complexity of network traffic and detect more sophisticated threats
- Using machine learning as part of the system configuration process to better recognise patterns in network behaviour and adapt to benign or planned changes to the network topology
- Specifying key requirements for IDS functional visibility to avoid 'black-box-like' performance while maintaining system integrity
- Assessing the improvements to IDS supported by combining advanced AI and machine learning with traditional capabilities

Christian Koch
Senior Manager GRC & IoT/OT, NTT Security

10:30 Morning refreshments, exhibition and networking

11:00 Technology Innovation Panel - exploring cutting edge IDS tools and solutions, specifically for the implementation in the utility environment

During this session, each technology innovator will give a 15-minute presentation on results achieved from the application of their solution in the electric utility environment, as well as their research and development activity to meet future demands and challenges. The presentations will be followed by 30 minutes of Q&A and panel discussion, whereby you will get the opportunity to quiz the tech experts, understand their innovation plans more fully, and influence the direction of new product development to better meet your OT cybersecurity requirements.

Elisa Costante
Senior Director, Industrial and OT Technology Innovation, ForeScout Technologies
Andrew Tsonchev
Director of Technology, Darktrace Industrial
Johan Straten
Regional Director, Northern Europe, Cyberbit

12:35 Technology Innovation Case Study - studying the lessons learnt and challenges faced in the deployment of IDS to the utility OT environment

- Developing a well-defined project roadmap covering all organisational protocols to deliver effective detection capabilities
- Convening appropriate, cross-functional working groups to ensure smooth cooperation between OT and IT personnel
- Fully defining your complete network architecture to develop the most effective cybersecurity processes for each business unit
- Examining the far-reaching benefits unlocked by heightened visibility of the ICS environment

Alon Barel
VP EMEA & APAC, Indegy

13:00 Lunch, exhibition and networking reception

14:30 Active Monitoring Use Case – increasing the active components of your monitoring capabilities to enable more centralised and efficient IDS deployments

- Developing a centralised remote engineering workstation to monitor behaviour and traffic including in more distributed parts of the network
- Implementing solutions capable of active monitoring to receive process communications from distributed nodes in the network
- Working together with key internal stakeholders to instil trust in new IDS solutions and ensure confidence in their introduction to your network
- Actively requesting information on remote modules and firmware to increase network visibility while optimising investment and deployment costs

Ivo Maritz
Chief Information Security Officer, BKW

15:15 Improved Situational Awareness – incorporating monitoring and analysis of the network's cyberphysical performance to improve anomaly detection and support traditional tools

- Increasing the depth of IDS capabilities beyond the monitoring of network traffic to include behavioural changes which could be the result of malicious activity
- Comparing a variety of packet inspection techniques including machine learning to establish their potential benefits
- Identifying and quantifying the cyberphysical characteristics of malfunctioning apparatus including changes to temperature, frequency, sound, and power quality
- Prioritising key behavioural criteria to efficiently monitor the most pertinent indicators of malicious activity
- Quantifying the potential for increased situational awareness of your control equipment to effectively complement existing IDS technology

Deeph Chana
Deputy Director, Institute of Cyber Security & Technology, Imperial College London

16:00 Afternoon refreshments, exhibition and networking

16:30 Information Sharing and Analysis – fostering trust and facilitating information exchange

between electric utilities to improve the resilience of the grid to cyber attacks

- Developing a platform for the secure exchange of threat data collected by utilities across Europe including data captured by advanced security systems
- Enabling industry-wide responses to localised security incidents happening across the continent
- Comparing security capabilities and solutions to ensure deployment of best-in-class tools
- Improving the timeliness and effectiveness of the response to cyber incidents and ensuring a unified approach to talking threats to grid infrastructure

Gisele Widdershoven
Boardmember, EE-ISAC *(Managing Director – Accenture Global Cybersecurity)*,

17:15 SOC Development for IDS – exploring approaches to embedding IDS into a variety of SOC frameworks to ensure full preparedness for timely and constructive responses to anomalies

- Identifying the optimal integration of IDS into new and establishes SOCs to ensure they effectively react to and investigate alerts
- Ensuring coherent lines of communication between control rooms and the SOC to mutually benefit from specific expertise as it pertains to specific alerts
- Using IDS to mitigate the risks associated with a shift in communications technology towards more vulnerable packet telecoms solutions
- Empowering your cybersecurity team to safely develop and test new use cases in sensitive environments in order to maximise the coverage of your IDS and protect your entire network
- Developing and testing a robust SIEM to detect significant network events from huge volumes of event logs
- Putting in place a fully equipped and staffed SOC to continually develop cybersecurity strategy, manage day-to-day security requirements, and remain adaptable to organisational demands

Nikolaus Wirtz
Research Assistant, E.ON Energy Research Centre

18:00 End of conference day two

CONFERENCE DAY 3 - Thursday 31 January 2019

08:00 Registration and refreshments

08:45 Welcome back from the chair

Matthew Freeman
Global Head of Cybersecurity, DNV GL

09:00 IDS for Communications Networks – monitoring utility telecoms networks to detect threats originating from increasingly vulnerable field locations

- Utilising powerful IDS tools to secure vital and complex utility telecommunications networks connecting at-risk field devices with control rooms
- Protecting communications architecture built on a variety of networks including private and public infrastructure and wireless connections
- Ensuring robust security and interoperability with pre-existing legacy systems in the SCADA network
- Overseeing constant changes and mutations in traffic and connections to differentiate malicious activity from legitimate changes or misconfigurations
- Eliminating blind spots to deliver complete coverage of the communications network, identifying anomalous activities, and taking appropriate steps to correct them

Robin Massink
IT Security Specialist, Alliander

09:45 Vulnerability Assessment – establishing a highly mature vulnerability assessment, mapping technical and business risks, to achieve a focused prioritisation of identified vulnerabilities

- Ensuring the success of SOC and CIRT teams through targeted and efficient responses to business risk

- Effectively processing a vast number of events in an increasingly diverse and complex range of protected environments
- Implementing a SIEM to enable broad and timely identification of threats through the proper correlation of various security events
- Considering vectors of attack, attack propagation and impact, and gaps in cyber defence to inform the design of mitigation plans and continuously improve cyber-readiness
- Fully utilising available resources and knowhow to maximise the impact of SOC and CERT teams

Dragomir Vatkov
Cyber Security Architect, innogy SE

10:30 Morning refreshments, exhibition and networking

11:00 SCADA and Substation Implementation – examining examples and use cases of IDS within various utility environments and optimising deployment in each case

- Developing bespoke IDS implementations for different utilities to ensure specific vulnerabilities and challenges are met with robust solutions
- Growing the skills and competencies which are required by utility SOCs to meet the specific challenges of the OT environment
- Taking a risk-based approach to use case development ensuring optimal prioritisation of a vast array of possible threats
- Surveying the technology market to ensure the most suitable tools are matched to specific utility conditions
- Evaluating the effectiveness of IDS in a number of utility environments to guide your implementation and improve threat visibility

Maarten Hoeve
Researcher, ENCS

11:45 Space and Cybersecurity – examining the potential of space technology to enhance smart grid cybersecurity and intrusion detection capabilities

- Identifying potential opportunities for the application of space-based tools to improve cybersecurity and support a range of new monitoring capabilities
- Investigating how space technology can be integrated into the specifics of the electric utility environment
- Exploring potential use cases including monitoring the behaviour and migration of connected IoT devices to identify possible threats
- Building a roadmap for future collaboration between the space and energy sectors to leverage mutually beneficial technical partnerships

Laurence Duquerroy
Applications and Telecommunications Project Manager, European Space Agency

12:30 Lunch, exhibition and networking

14:00 Solution Testing Tutorial Panel – rigorously testing vendors' IDS tools against a broad range of criteria to ensure they meet key functional requirements, integrate well into your existing architecture, and remain robust in a changing landscape

- Establishing a process for the reliable and fair evaluation of third-party IDS solutions to enable you to choose a system which fits your network and stands the test of time
- Comparing third-party, in-house, and hybrid testing strategies considering cost, effectiveness and independence
- Choosing and prioritising key, quantifiable criteria and performance metrics to assess both the solutions' suitability for your security ecosystem and benchmark products against one another
- Developing a secure and representative testing environment in both laboratory and active network scenarios
- Utilising a range of advanced data sets as well as techniques such as ethical hacking and adversarial machine learning to ensure rigorous stress-testing against the most sophisticated threats
- Measuring solutions' adaptability in the face of changes to network architecture to ensure their robustness in identifying unpredictable future threats
- Implementing a robust, multi-faceted, and clearly defined testing process to provide a watertight case

for the best choice of IDS solution to fit your cybersecurity strategy

Roee Schreiber
Principal Director, Security, Accenture Security
Dani Grabois
Security Senior Principal, Accenture Security
Bas Kruimer
Senior Manager, Accenture Security

16:00 End of conference