Draft Programme

SMART GRID FORUMS | Energy Intrusion Detection 2019
29-31 January
Amsterdam, The Netherlands

Energy Intrusion Detection 2019

Advanced IDS Implementation to Futureproof Smart Power Generation, Transmission, and Distribution

3-Day Conference, Exhibition & Networking Forum

29-31 January 2019
Amsterdam, The Netherlands





Event Format:

- ✓ **Case-study driven conference programme**
- ✓ **IDS Solution Testing tutorial**
- ✓ **Technology innovation panel discussions**
- ✓ **Roundtable breakout sessions**
- ✓ **Networking evening reception**
- ✓ **Exhibition area displaying 10+ suppliers**
- ✓ **Live demo labs of the latest tools and technologies**

For more information contact:
Robin Sarfas, *Conference Producer* – Phoenix Forums
Tel: +44 (0)20 8349 6365 | Email: robin.sarfas@smartgrid-forums.com

Keynote Presentation

1. **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

Keynote Presentation

2. **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 which demonstrates a convincing 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 assuage fears of spiralling costs
- Securing timely and significant budget allocation to rapidly establish IDS at the core of Smart Grid cybersecurity

Keynote Panel Discussion

3. **Organisational Alignment – 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

4. **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

5. **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

6. **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
- Upskilling SOC staff with the knowledge and tools necessary to process different alerts and investigate them to identify the cause and nature of any anomalies
- Ensuring coherent lines of communication between control rooms and the SOC to mutually benefit from specific expertise as it pertains to specific alerts
- 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 the growing demands of the organisation

7. **Advanced Machine Learning & AI – leveraging improvements to advanced analytics and machine learning technology to automatically configure IDS and improve its reliability**

- 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

8. **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

9. **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 those based on machine learning to establish the potential benefits of further
- 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

10. **IDS Configuration – tuning your IDS to correctly identify rogue network traffic using multiple analysis techniques to improve reliability and limit false positives**

- Setting out clear roles and responsibilities for collaborating with your IDS supplier to achieve the highest possible standards of accuracy and trust
- Providing a representative and repeatable testing environment and data set to make sure your chosen solution is well suited to monitoring your network traffic
- Tuning your IDS to better discern benign network traffic and automatically recognise it to reduce incidences of false positives
- Exploiting the ability of advanced IDS to build a complete inventory of network devices, identifying potential liabilities, recognising future connections, and alerting the SOC to potentially malicious agents
- Introducing more autonomous IDS solutions to automatically adapt to changes in your control system environment and minimise human intervention while remaining alert to an evolving threat landscape

11. **Communications Architecture – leveraging more powerful IDS tools to support the security of more vulnerable and higher capacity telecoms networks**

- Maintaining security levels as grid communications evolve from secure-by-design, serialised connections to a greater level of interconnection via IP networks
- Implementing the IDS capacity required to process and analyse previously unseen volumes of traffic generated by large-scale AMI and IoT deployment
- Using IDS to mitigate the risks associated with a shift in communications technology towards more vulnerable packet telecoms solutions
- Setting high standards for the interoperability of your IDS with other vendor systems to ensure protection is retained across your entire network
- Enabling the complete, end-to-end monitoring of your communications architecture to maintain the security of your systems as the flow of data grows exponentially

12. **Standards Development – supporting the development and adoption of communications protocols to improve the security and interoperability of network systems and devices across the grid**
Details to be announced

13. **SCADA Protection Use Case – utilising IDS to holistically monitor and secure a more interconnected and automated control environment**

- Implementing a head-end IDS deployment to SCADA/DMS systems to provide top-down, global monitoring of your entire control environment
- Optimising the placement of your IDS based on a balance of internal and external threats to maximise its value and detect as many legitimate threats as possible
- Guaranteeing readiness to adapt to growing levels of data including increased use of real-time data
- Overcoming the specific implementation and operation challenges faced when working in the SCADA environment
- Working together with key internal stakeholders to instil trust in new IDS solutions and ensure confidence in their introduction to your network
- Ensuring the continued security and performance of your most fundamental network control systems by deploying robust IDS without compromising availability

14. **Substation Protection Use Case – identifying the most vulnerable substations and implementing an IDS roll-out strategy that effectively balances minimising cost with maximising security**

- Using a targeted approach to protect the most at-risk substations through centrally controlled, on-site implementation of IDS
- Translating key factors which govern the vulnerability of substations such as size, internal and external connections, and functional importance, into quantifiable metrics for comparison
- Performing a methodical risk assessment based on your chosen criteria to establish the opportunity and cost posed by installing IDS in substations of various profiles
- Using efficient IDS tools to scan bandwidth, protocols and ports, thoroughly monitoring the activity throughout designated substations
- Prioritising and securing the highest value and most at-risk substations through local IDS deployment while still ensuring global coverage within budget

15. **AMI Security Use Case – exploring the potential for IDS to cost effectively mitigate the risks associated with mass AMI deployment**

- Supporting the security and reliability of AMI located in unsecured locations by recognising and responding to security breaches from networks and devices
- Delivering robust monitoring of AMI networks in spite of limits to the computational and communication power at the devices' disposal
- Comparing the threats driving AMI IDS deployments at different network levels including the HAN, NAN, and WAN
- Optimising IDS deployment for AMI to rapidly detect and react to cyber-attacks, preventing fraud and protecting potentially sensitive customer information

16. **Financial Services Case Study – learning from cross-industry examples of successful IDS implementation to leverage a wider pool of cybersecurity expertise**
Details to be announced

17. **Balancing-Market Entrants – using IDS to combat the security risks associated with admitting more players at various levels of the balancing mechanism including small-scale generation and storage**

- Addressing grid operators' concerns over an influx of smaller market participants with less rigorous security by using IDS to scan incoming traffic
- Maintaining high standards of awareness of incoming traffic while facing growth in connections to external parties via public internet and IP comms
- Exploiting IDS to discover and alert to potential threats without compromising the critical real-time balancing of the network
- Ensuring high levels of security in a more diverse and harder to control landscape without jeopardising the crucial process of guaranteeing a balanced network

18. **Distributed Energy Resources – fully preparing the grid to monitor a growing number of DERs connected to your critical control systems via the LV network**

- Developing and maintaining a secure distribution network ecosystem while incorporating decentralised energy assets including microgeneration, EV charging, and battery storage
- Capturing and processing vast flows of data generated by a multitude of assets installed across an ever-increasing number of customer sites
- Optimising IDS architecture to support grid security in response to a growth in potentially vulnerable, publically accessible distributed energy assets
- Preparing for new vulnerabilities for your vital SCADA and substation environments caused by a growth in unreliably secured smart home devices
- Estimating the likely increase in security threats as a result of DER connections and the impact of IDS on your awareness levels

19. **Solution Testing Tutorial – 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