SANS EMEA

SANS EUROPEAN ICS SECURITY SUMMIT

27th - 28th September 2015
NH Grand Hotel Krasnapolsky, Amsterdam

✉ training@sans.org ☎ +44 (0)20 3384 3470 www.sans.org/ICSAmsterdam @SANSEMEA #ICSAmsterdam

Sunday 27 September, 2015

8:30 – 9:30 am **Coffee and registration**

9:30 – 9:45 am **Welcome and introduction by Chair Mike Assante**

9:45 – 10:15 am

Panel: State of ICS Cyber Security after 10 years

Karl Williams: *PA Consulting*
Gisele Widddershoven: *Accenture*
Franky Thrasher: *Engie*
Graham Wrights: *National Grid*

10:15 – 10:30 pm **Networking break**

10:30 – 11:15 am

Nexdefense Industrial “Connectivity Surprise Factor” : Can you see me now?

Everyday, Industrial Control Systems perform tirelessly — safely and efficiently producing and delivering power, clean water, moving people and producing most all of the varied products and services on which the world depends. While communications is at the heart of these critical systems, operational challenges continue to be amplified. Technology convergence is often unknowingly blending industrial control, commercial and consumer products and technologies onto common shared infrastructures leading to new risks and greater exposure to threats. In this session, learn about the ‘Connectivity Surprise-factor’ and benefits that can be gained by performing comprehensive and real-time network asset-inventories, by tracing data flows, base-lining normal and expected communication patterns and using passive industrial network anomaly detection technology to help improve and protect a control system’s operational resiliency throughout its lifecycle.

Doug Wylie, *Vice President, Product Marketing & Strategy at NexDefence, Inc.*

11:15 am – 12:00 pm

Ground Truths: The true state of ICS attack and defense

This presentation will focus on lessons learned through active defense and incident response in ICS systems across the world. Topics covered will include: ICS security myths, ICS threat landscape, ICS defensive techniques, and more.

Eric Cornelius, *Cylance*

12:00 – 12:30 pm

Modeling Hard vs Measurement Hard Analyzing control loops from an attacker’s point of view.

In any process of sufficient complexity, there are side effects for any action an attacker takes. Unless he has chosen some subtle form of economic damage, some part of the process will probably be pushed harder or faster than ever before. As the feedback loops kick in to deal with this disturbance, ringing is induced in the adjacent control loops. This sets off alarms and engages automatic shutdown mechanisms and can thwart the overall attack. One approach is to take over the entire process and suppress all of the alarms and defensive behaviors. Anyone that has attempted the full control approach can tell you the complexity of such an attack spirals out of control and the results of the logic introduced by the attacker eventually becomes uncertain. The attacker must bound the parts of the process that need to be actively controlled or suppressed. This presentation will briefly introduce the concepts of modeling hard vs measurement hard as a way of discussing the dynamic behavior of a process during an attack.

Jason Larsen, *IO Active*

12:30 – 1:15 pm **Lunch**

1:15 – 2:00 pm

Building national cybersecurity and Incident handling competence targeted towards critical infrastructure (ICS/SCADA) through training in advanced Cyber ranges.

The presentation will contain the following:

- The role of the Swedish Civil Contingencies Agency (MSB) and the CERT.SE
- What the agency (MSB) does within cybersecurity and CIIP
- The National program for security in industrial information and control systems, what it is and what we do
- The National competence center for security within ICS/SCADA NCS3, what it is and what we do
- The Cyber range (Specification, setup, systems: 300+ servers in a Cluster, 5000+ virtualized systems, up to 2048 unique simulated networks, simulated internet backbone (100 virtualized core routers with Geomapping), bots (simulated users), based on open source)
- Cyber range Content (Complete fictitious companies, “real” networks) and tools, how to make and control the content
- Cyber range Connection (VPNs, Connected to the real world through ICS hardware).
- Training performed, Part 1, (Awareness through among other things hacking examples, Network scanning)
- Training performed, Part 2, (RED/BLUE team. Blue/Blue team training)
- Training performed, Part 3, (Future thoughts)
- Lessons learned

Richard Widh, *Swedish Civil Contingencies Agency (MSB).*

2:00 – 2:45 pm

Secure Bi-directional Data Link between Plants Network and Business Network (Data Tube)

Cyber security is a major concern for companies. Industrial systems DCS and SCADA used to be completely isolated and therefore its security was controlled and safeguarded. The information from these systems used to be limited to monitor and control. With time, these systems evolved and historization functionality added as an integral part of these systems to further support operations. Historization data can be used to analyze failures and project future operational trends. With more diverse operations, management is also became interested in the information provided by these systems, and hence connectivity to the business network evolved. With this connectivity demand, cyber security becomes a major issue as companies work to secure their control systems. The concept can be built using standard tools and software that can be easily integrated in an appliance to form a complete solution.

Saleem Al Harthi & Abdulmajeed A. Al Abdulhadi, *Aramco*

2:45 – 3:00 pm	**Break**
3:05 – 3:45 pm	**Exercise is good for you** Attack techniques are constantly evolving, networks are becoming more complex and our reliance on Industrial Control Systems grows by the day. Despite record spending on defence and detection, it is inevitable that some cyber attacks will be successful. Regardless of whether they are targeted at manufacturing, building management, chemical or water infrastructure, a swift and well-practiced response is vital. Drawing on real-world experience from his time leading national CERT teams, Elliott will educate attendees to what makes a good response. Many people consider incident response to be all about digital forensics and malware indicators – this talk uses a number of case studies to show that to be effective, particularly in modern ICS environments, requires much more than just a technical investigation. Finally, Elliott will give some practical advice on how organisations can begin to build their own cyber exercise programme to practice their response techniques, and survive in the era of cyber-insecurity that we now live in. **Elliott Atkins,** *Exercise 3*
3:45 – 4:30 pm	**Deconstructing ICS Cyber Attacks and Lessons Learned** In this presentation, the course author for ICS 515 will deconstruct reported ICS cyber attacks. Some of the attacks that have been reported - simply aren't true. And the real attacks offer lessons learned. Audience members can expect to learn fact from fiction in ICS attacks and takeaway guidance for actively defending an ICS from targeted threats. **Robert M. Lee,** *Dragos Security LLC*
4:30 – 5:00 pm	**Panel discussion - GICSP**
5:00 – 5:15 pm	**Closing comments**
6:00 – 8:00 pm	**Sponsored reception**
	paloalto NETWORKS® **Palo Alto Networks** Palo Alto Networks is the next-generation security company, leading a new era in cyber-security by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets. Find out more at *www.paloaltonetworks.com*

NB This agenda should be considered a draft and the organisers may make amendments to content and line up.

Monday 28 September, 2015

9:00 – 9:45 am	**Harnessing Industrial Control Systems Security in a global organization** A general misconception on Industrial Control Systems Security is that getting it right is a technical challenge. Looking back at almost a decade of ICS Security (or PCD IT Security, as it's called in Shell), the technical challenges were the least of our challenges. The more significant challenges are about people and process. For an international oil company, this unfolds itself into multiple challenges. Next to the ubiquitous disconnect between Engineering and IT, you need to deal with regional cultural imperatives and legislation, efficacy of de-central assurance and risk management (self-assessment) and the simple fact that you're dealing with large numbers of systems, people and facilities on just about every outskirt of the globe. As there are already lots of technical sessions, this presentation will focus on other topics: how to define an ICS Security standard, what factors come into play? Once you have a standard, how to do ensure (or validate) its effectiveness? Closing the loop with assurance and factoring in cost versus benefit. This presentation will provide experiences and hopefully some new insights to those that are on a journey to improve ICS Security or plan to do so in an similar setting (e.g. in a global setting). **Maarten Oosterink,** *Shell Projects & Technology*
9:45 – 10:30 am	**Maturity assessment on Cybersecurity for critical infrastructures** The systems used for critical infrastructures must meet very specific standards of performance, reliability, availability, maintainability. Cybersecurity solutions for these particular systems therefore need to take all these factors into account and limit their impact on critical processes and operator workload. This presentation will be an opportunity to review the state of the art in cybersecurity for some critical systems, with practical examples and use cases of the solutions and services available to meet the technical, financial and human challenges of different sectors. A strong emphasis will be put on the French state approach and recent published requirements, and how the French market will be able to answer. **Thieyacine Fall,** *Deputy Leader Cybersecurity Business Unit: Cybersecurity Consulting and Evaluation at Thales.*
10:30 – 10:45 pm	**Networking break**
10:45 – 11:30 am	**Cloud Computing, an opportunity or risk too far for critical infrastructure environments?** The evolution of cloud computing, and its impact on critical infrastructure operations. Not only the storage, but management of ICS devices is rapidly being done through public cloud instances. Yet without the appropriate security the impact to society will be could be significant. This session will consider the measures required to deliver trust in such architectures, and deliver information from the author of multiple books within ICS and Cloud computing. **Raj Samni,** *McAfee.*

11:30 am – 12:15 pm

Industrial revolution 4.0.
How to keep up the pace and do not fall of cyber threats' victim.

Industrial Internet of Things, enterprise 4.0, connected everything. These words are not a marketing buzz any longer – it is a reality we live in. And this reality brought us new risks. What are these risks, how to cope with them now and in the future? These questions will be answered during the speech.

Andrey Nikishin & Andrey Doukhalov, *Kaspersky*

12:15 – 12:45 pm

Panel: Industry 4.0

Bart De Wijs: *ABB*
Raj Samni: *McAfee*
Del Rodillas: *Palo Alto Networks*
Andrey Nikishin & Andrey Doukhalov: *Kaspersky*

12:45 – 1:30 pm

Lunch

1:30 – 2:15 pm

ICS Security - Rapid Digital Risk Assessment

Industrial environments are wonderfully complex. Not only do they contribute to the majority of the world's existing digital capability, and will increasingly do so, they also form some of the most difficult environments when dealing with cyber security. The difficulty is not due to technology alone, although that this becoming a future concern, but due to the mix of ancient, old, recent and new computing technologies. Basically a mix of historically based priorities and innovative concept which persist and converge with modern technical capabilities. A pure IT based approach is not only misconceived but totally misplaced. Historical precedents demand creative considerations to managing technical and human cyber security issues on a case by case basis.

Our primary job, at an early stage, is to create this link and provide measured based arguments to defend the need for mature cyber security considerations and processes.

Steve Smith, *ONRIX*
Dieter Sarrazyn, *Toreon*

2:15 – 3:00 pm

Integrating Industrial Control System (ICS) Safety and Security, with Application to the UK Nuclear Industry

The UK civil Nuclear Industry is going through a period of significant change. When it comes to projects involving plant based computer systems (i.e. ICS), safety and functional requirements have been well integrated into a single project lifecycle approach with very positive consequences although operability is sometimes behind the curve. Standards and regulatory approaches are established and evolve, rather than going through large step changes. However, security has historically been considered separately, and whilst this is changing, there is scope to improve integration.

Attendees will acquire an appreciation of fundamental security prioritisation challenges facing ICS designers and operators drawing in particular on the experience of the UK nuclear industry. They will also gain an appreciation of a risk-based way of reconciling apparently conflicting priorities for system design, configuration and investment.

Anna Ellis, *co-Founder, Indigon Consulting Ltd*

3:00 – 3:15 pm	**Networking break**
3:15 – 4:00 pm	**ICS CyberSecurity – Don't forget the people** BG Group is a relatively late entrant into the field of control and safety systems cyber security, or more accurately the provision of secure integrated operations. Following the establishment of minimum corporate standard requirements, a rapid programme covering all operated assets, and expanding to include non-operated, has established the ICS cyber security risks (facility by facility) and embarked upon remediating them. A key output from the risk assessment phase was that by paying attention to people and processes many of the risks could be effectively reduced. This session will thus focus upon the people and process element of the BG ICS Cyber Security journey to date. **Alan Jones & Elizabeth Selvina,** *BG Group*
4:00 – 4:45 pm	**I'm Watching My ICS, Now What Do I Do?** Following up on last year's presentation advocating Network Security Monitoring (NSM) for ICS, this presentation will cover the importance of an Incident Response Plan (IRP) specifically targeted at responding to security incidents in ICS. Responding to security incidents in ICS requires different planning and techniques than those in IT environments. This presentation will discuss what is necessary to develop an ICS-specific IRP, and look at some example ICS incidents that should be in considered. It will also cover a brief overview of NSM for ICS to bring those in the audience unfamiliar with the topic to a basic level of knowledge, as well as hunting for indicators of compromise on systems being monitored. **Rob Caldwell,** *Mandiant*
4:45 – 5:15 pm	**Developing situational awareness for Industrial Control System networks** Today's industrial control systems are highly interconnected environments. Industrial Internet is a way to strive for competitive advantage, but at the same time, industrial business relies more on continuity of networked systems, and is more prone to incidents that interfere with production processes. Rapidly increasing connections to cloud, remote maintenance and remote optimization services opens more attack surfaces to the industrial systems. Some of the most typical challenges organisations face are related to defining operational cybersecurity responsibilities for industrial control systems (ICS), both within their own organization as well as between the asset owners and ICS vendors. This presentation provides a walk-through of a real customer case and introduces some prominent building blocks to mitigate the above-mentioned challenges. Well-managed cybersecurity is a must to take full benefit of the development towards Industrial Internet. **J . Holappa,** *Lead Security Consultant, Nixu Corporation* **K. Luukkainen,** *Head of industrial internet Security, Nixu Corporation*
5:15 – 5:30 pm	**Closing**

NB This agenda should be considered a draft and the organisers may make amendments to content and line up.

Speaker Bios:

Abdulmajeed A. Al-Abdulhadi

Abdulmajeed A. Al-Abdulhadi is a SCADA Specialist with Saudi Aramco's IT/SBAD/Real-Time Systems Division. Abdulmajeed graduated from King Fahd University of Petroleum & Minerals in 1995 with a B.S. degree in Computer Science, and joined Saudi Aramco in 1996. He was the software engineer for the giant video data wall project installed in the Operation Coordination Center (OCC) in Dhahran. His last project was the SCADA Systems upgrade to Oil Supply Planning And Scheduling (OSPAS) and Power Operations Dept. (POD), which was launched in Feb. 2013. Throughout his career he participated in cutting-edge projects that added value to several Saudi Aramco operations.

Robert M Lee

Robert M. Lee is a co-founder at the critical infrastructure cyber security company Dragos Security LLC where he has a passion for control system packet analysis, digital forensics, and threat intelligence research. He is the course author of SANS ICS515 - "Active Defense and Incident Response" and the co-author of SANS FOR578 - "Cyber Threat Intelligence." He is a passionate educator although he should not be confused with the other Rob Lee at SANS - that Rob Lee is cooler but has less hair.

Robert obtained his start in cyber security in the U.S. Air Force where he currently serves as a Cyber Warfare Operations Officer. He has performed defense, intelligence, and attack missions in various government organizations including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles and journals in publications such as Control Engineering, Air and Space Power Journal, Wired, and Passcode. He is also a frequent speaker at conferences and is currently pursuing his PhD at Kings College London with research into the cyber security of control systems. Robert is also the author of the book "SCADA and Me" and the web-comic www.LittleBobbyComic.com

Jarkko Holappa

Mr. Jarkko Holappa is lead security consultant in Nixu. He received his degree of Master of Science (Electrical Engineering) from University of Oulu. Jarkko has more than 15 years experience in information security and risk management. He is member of Finnish Standards Association (SFS) National Advisory Group for JTC1/SC27 (IT Security Techniques) of ISO/IEC Standardization and participates IAEA's work on developing and instructing computer security guidelines for nuclear energy sector He holds GICSP, CISSP and ITILv3 Foundations certificates.

Saleem E. Al Harthi

Is currently a leader of Security Compliance and Access Management at Saudi Aramco Operations Coordination Center (OCC). He has more than twelve years process control systems and network administration. MBAc in Business administration. Bachelor Degree of Science in Computer. CISSP, MCTS, CCNA, JNCIS, ENS and Cisco Cybersecurity Specialist.

Kalle Luukkainen

Mr. Kalle Luukkainen is the head of industrial internet security at Nixu, being responsible for the industrial customer segment. Nixu is a cyber security consulting company with a headcount of 150 security specialists, with service capabilities ranging from security & privacy management to technical audits and 24x7 security operations.

Stephen Smith

Stephen Smith is an independent advisor on digital security risks through ONRIX. He has spent more than 25 years in the IT industry with a focus on information security and dedicated these past 5 years on digital risks associated with industrial control systems. He resides in Belgium and provides digital risk services to local and multinational companies in utilities, manufacturing, transport and nuclear sectors.

His recent work with several companies indicated that there was a growing concern with cyber threats but that the general maturity level to deal with these threats was not ingrained in these organisations risk management culture. To this end, he commissioned a survey on Belgian companies, primarily those that might be utilising industrial systems, to better understand the security maturity level enabling required defences and stances to combat the growing cyber threat.

Dieter Sarrazyn

Dieter has built his career in industrial environments and has gained excellent knowledge on strategic, tactical and operational level regarding security related subjects. He has worked extensively on the security within the industrial control system area including more than 6 years in a large electricity generation company. Within Toreon, he is the assessments team leader as well as the driver for the ICS security solutions Toreon offers.

His main focus exists in performing penetration tests (as well external as internal), performing security audits, creating and evaluating security architectures, creating and setting up vulnerability management frameworks & tools. He deploys this expertise primarily in an Operational Technology (OT) environment, performing SCADA security assessments and securing SCADA environments. These activities are always part of a larger program, aimed at reducing business risks.

He has extensive knowledge concerning penetration testing, social engineering, infrastructure security and has the following certifications: CISSP, GCIH, GSEC, GXPN, GCIH, GSNA, GICSP, CIRM and Scada Security Architect. He's also active within the Tetra project "Safer industrial Networks" and the 3IF project on IIoT & Industry 4.0.

Sven Schriewer

Computation in Bochum, Germany, with implementing computer vision algorithms.

He started with KPMG as an IT auditor in 2000 and gathered a lot of international experience working abroad in China, Russia and the Netherlands.

His main focus is on consulting companies regarding building up IT security services, setting up and improving cyber defense capabilities - in particular building up a Security Operating Center - and evaluating the impact of outsourcing cyber defense functions or parts.
Next to this, Sven is a proud father and supported exchange students to live with a host family in a foreign country.

Richard Widh

Richard Widh (B Sc Computer engineering & electronics, CISSP, GISP) is a part of the Cybersecurity and CIIP Section at The Swedish Civil Contingencies Agency (MSB). Richard have worked as a specialist within the Cybersecurity area for more than 15 years and within IT as a professional since 1993, including but not limited to the Swedish Armed forces (FM), Swedish Defence Materiel Administration (FMV) and the Swedish Radiation Safety Authority (SSM).

Elliot Atkins

Elliott has almost 20 years' experience in cyber security, working with Governments, large multinational companies, dotcom startups and not-for-profit organisations. The former Head of GovCertUK (the UK Government's 24x7 computer emergency response team) he now runs Exercise3, a company dedicated to building and running realistic cyber security exercises and helping companies improve how they respond to incidents.

Elliott holds a BSc(Hons) in Computer Science from the University of Kent, and regularly speaks and writes on the topics of cyber security and incident response. When not working, he can be found restoring a Panavia Tornado GR.1 aircraft, which he acquired in 2013.

Robert Cadwell

Rob has been a Principal Consultant in Mandiant's Industrial Control Systems consulting practice for the past year and a half, leading engagements across a wide spectrum of industries using ICS. Previously, he worked as a Product and Chief Security Architect for a multinational industrial company which builds hardware and software in the Electric Utilities market. Rob has worked in various positions in the IT industry since 1999, which piqued his interest in security early on. Rob earned a BS degree from the University of Florida, an MS from Barry University, and has a CISSP. He has spoken at various conferences, including SANS ICS summits in the US and Europe, Digital Bond's S4 conference, and the TCIPG lecture series at the University of Illinois Urbana-Champaign.

Anna Ellis

Anna is an Instrumentation and Control (I&C) and nuclear safety specialist. Anna has recently co-founded Indigon Consulting Ltd, a people-centric consultancy firm whose ethos is based around integrity and its commitment to delivery of its specialised and high quality support to clients in the nuclear and other highly regulated industries. Prior to that, she spent fourteen years working for UK consultancy firms, where she grew new capabilities, and led teams supporting clients on I&C projects.

Anna has a good understanding of the UK nuclear industry regulatory framework and safety standards, with a developing interest and involvement in the security of plant based computer systems. She has significant experience applying this knowledge and has led or been heavily involved in some high profile, complex and challenging projects.

Thieyacine Fall

Thieyacine Fall has led several initiatives to develop offering for Critical Infrastructure Operators (risks and solutions ICS/SCADA). He is currently the technical interface with Schneider-Electric (Partnership since Fall 2013) for France. He has extensive experience in information security and technology from Management (policy, governance, strategy, and risk assessment) to Processes, Operations (including Outsourcing) and implementation of Technology (Architecture & solutions) in depth.

Past engagements have covered Transportation, Automation industry, retail food, financial services, healthcare, government, defense as well as telecommunication sectors.

Doug Wylie

Doug Wylie is a seasoned business practitioner, industry thought leader and certified security professional with extensive experience as a global market-maker for industrial products, open technologies and contemporary solutions used in mission-critical applications.

In his current role, Doug directs and promotes NexDefense's position and perspective on emerging market demands, industrial networking, and the ever-evolving security trends that affect customers across an array of industries and applications. His focus includes identifying and solving real-world customer challenges, while similarly establishing relevant solutions that increase visibility and operational knowledge to counteract risks that may impact safety, integrity, information security and productivity.

Prior to NexDefense, Doug worked for Rockwell Automation and performed most recently as Director, Product Security Risk Management reporting to the Office of General Counsel and CISO. He earned the prestigious 2013 SANS People Who Made a Difference in Cybersecurity award and actively maintains his Certified Information Systems Security Professional certification (CISSP® 435349). Doug holds his Bachelor of Science in Business Administration from John Carroll University in Cleveland, Ohio and numerous internationally-recognized patents related to industrial communications, control and software technologies.

Alan Jones & Elizabeth Selvina

Alan Jones is currently the Automation Engineering Manager for BG Group, and is based at its Head Quarters in the UK. He has been in BG Group since 2001 and in his current role for the past 3½ years.

Working in the Engineering Function, Alan leads the head office Automation team comprising C&I, Electrical, Functional Safety and Process Control Security disciplines. This team sets the minimum standards in Automation for the BG Group, and provides guidance and assistance to assets across a range of subjects. Development and understanding of the broad Automation community is also a key element of this role. In addition Alan holds the Group Subject Matter Expert (Functional Safety) position.

Alan's background is in Control and Instrumentation Engineering within the oil and gas industry. Previous roles have included Engineering Manager (for an $800m offshore platform project), BG Group Technical Authority (C&I), Network Operations Manager in Transco (now National Grid), together with spells in Research and Technology and Transmission and Distribution.

Elizabeth Selvina is currently the Process Control Security Engineer for BG Group, and is based at its Head Quarters in the UK. She has been in BG Group since 2010 and in her current role for the past 2 ½ years.

Working in the Automation Engineering Function, Elizabeth is responsible for establishing a robust and sustainable Process Control Security that enables BG to effectively manage and mitigate the potential cyber-risk to its Hydrocarbon Production Operations. BG Automation Engineering Function, covers instrumentation, process control, communications, functional safety and electrical engineering.

Elizabeth's background is in Electrical Engineering, however her, previous roles has included working as an Enterprise Architect in BG Group's IT department, where she was responsible for shaping the IT design and strategy.

Prior to joining BG, Elizabeth worked in National Grid in the area of Transmission, Distribution and Metering, responsible for leading, shaping and delivering a number of diverse projects. In these roles, she was responsible for strategic changes, such as establishing a portfolio of technology enablers for downstream gas/electricity sectors, piloting an end-to-end smart metering deployment and redesigning the Transmission business processes in the gas and electricity sectors.

Maarten Oosterink

Starting out his career in IT infrastructure and IT Security in a variety of roles, Maarten has shifted his focus towards IT security of Industrial Automation & Control Systems (SCADA) nearly a decade ago and has since then been bridging the gap(s) between IT and engineering.

Having played many operational and managerial roles in staff and consulting positions, Maarten possesses both technical and leadership skill, business acumen and experience to relate to a variety of situations, organisations and stakeholders at all levels. Maarten is a Technical Authority (TA2) for PCD IT Security in Shell and is responsible for Shell's global standard for PCD IT Security, applicable to all of Shell's projects and operating facilities.

Andrey Nikishin

In a career that stretches back to the early days of Kaspersky Lab, Andrey worked as a Senior Software Engineer and Architect before moving to the Strategic Marketing Department as a Product Strategy Manager. Prior to his present role, Andrey headed the Cloud and Content Technologies Research and Development Department. Before joining Kaspersky Lab, Andrey had several years of experience developing his own antivirus programs. Andrey has a degree from the Baltic State Technical University in St. Petersburg and received his MBA from the London Business School.

Andrey Doukhvalov

Chief Strategy Architect, Head of Future Technologies at Kaspersky Lab. Working in the software business for almost 30 years, Andrey has been employed in various roles – from software engineer to software project leader – in system and application-level software development projects. For the last 17 years Andrey has been developing security software at Kaspersky Lab. One of Andrey's key current projects is the radically new secure operating system being developed as a platform dedicated to a wide range of specialized solutions where trust is of paramount importance.

Del Rodillas

Del's experience in industrial automation goes back to his very first job as an electrical engineer at Xilinx Inc, where he was responsible for optimizing and troubleshooting production yields of advanced semiconductor devices. Today as the ICS and SCADA Solution Lead for Palo Alto Networks, he looks at automation systems through the lens of cybersecurity. Del helps asset owners globally and across multiple critical infrastructure sectors understand the importance of cybersecurity in these environments and how best practices and technologies could be applied to balance the goals of preventing cyber incidents while keeping uptime and safety high. His 19 years of technology industry experience spans Cybersecurity, Networking, Aerospace/Defense, and Semiconductors with roles in strategic marketing and engineering. Del holds a Masters in Electrical Engineering from Santa Clara University and an MBA from the Wharton School of the University of Pennsylvania.

SANS EMEA