

Post event report



The 14th e-Crime & Cybersecurity
Germany

28th January 2020 | Frankfurt, Germany

Strategic Sponsors



Education Seminar Sponsors



Networking Sponsors



“ What I liked most about the event was the nature of the fast paced schedule of presentations. This allowed me to get a high-level view around multiple technical solutions and dynamics in play. ”

Product Manager, Deutsche Bank AG

Inside this report:

Sponsors

Key themes

Who attended?

Speakers

Agenda

Education Seminars



Speakers

- Babak Badkube, Global and Major Account Manager, **Demisto**, A Palo Alto Networks Company

- Henrik Becker, Director of Compliance & Risk Management, **Unitymedia**

- Helmut Brachhaus, Chief Technology Officer, **Patecco**

- Eward Driehuis, Senior Vice President Strategy, **Cybersprint**

- Gennadij Feldstein, IT Security Officer, **Commerzbank**

- Matthias Heise, Sales Manager, **Pulse Secure**

- Sebastian Hess, Cyber Risk Executive, **American International Group**

- Stefan Hornke, Senior Manager, **4C Group AG**

- Matthias Jungkeit, Chief Information Security Officer / DPO, **Münchener Hypothekenbank**

- Alexander Kehl, Regional Director, D/CH, **Accellion**

- Dr. Andreas Lober, Partner, **BEITEN BURKHARDT**

- Maurits Lucas, Director of Intelligence Solutions, **Intel 471**

- Marco Ratzmann, Enterprise Sales Account Executive, **OneTrust**

- Andrea-Julia Reichl, Information Security Officer (CISO), **Klinikum Ingolstadt**

- Carsten Renth, Director Operational Data Protection & Special Affairs, **Unitymedia**

- Christoph Ritzer, Partner, **Norton Rose Fulbright LLP**

- Michael Schneider, Data Protection Officer, **IKEA IT Germany GmbH**

- Jasbir Singh, Partner and Managing Director Europe, **Seclore Technologies**

- Nikolei Steinhage, Sr. Sales Engineer, **CrowdStrike**

- Peter Vahrenhorst, Kriminalhauptkommissar, **Landeskriminalamt Nordrhein-Westfalen**

- Peter van Zeist, Sr. Solutions Consultant, **LogMeln**

Key themes

- Security versus privacy?
- Risk management for CISOs
- Digital transformation in the driving seat
- Behavioural analysis: solving for the human element
- Who's who? Improving identity analytics
- Securing yourself against digital fraud

Who attended?



Agenda			
08:00	Breakfast and registration		
08:50	Conference welcome		
09:00	FAIL: How to acquire great technical solutions and then mess up their implementation Stefan Hornke , Senior Manager, 4C Group AG <ul style="list-style-type: none"> • Why do cybersecurity and IT projects fail? • A tongue-in-cheek analysis of the commonest mistakes in project management • How to ensure successful cybersecurity solution implementation 		
09:20	Overcoming today's most pressing third-party risk management challenges Marco Ratzmann , Enterprise Sales Account Executive, OneTrust <ul style="list-style-type: none"> • Review the drivers and challenges organisations face when managing third-party vendor risk • Identify priorities before, during and after vendor procurement • Takeaway a six-step approach for automating the third-party vendor risk lifecycle • Hear real case studies from privacy experts on how to practically tackle the third-party vendor risk 		
09:40	How do I implement a 'Zero Trust' security policy throughout your organisation? Matthias Heise , Sales Manager, Pulse Secure <p>Our dynamic world of mobile and cloud computing requires advancing secure access capabilities based on continuous verification and authorisation. How can you improve managing and governing user access? Pulse Secure will show how you can implement a single access policy to your data, regardless of where it is located, from wherever the person is accessing it from on whatever device. Key takeaways:</p> <ul style="list-style-type: none"> • How to achieve total user and endpoint visibility, and up-scaling device security • How you can enable IoT identification in a secure way and set relevant profiles 		
10:00	Crisis communication and CRITIS – a new dimension in the perception area of IT security Andrea-Julia Reichl , Information Security Officer (CISO), Klinikum Ingolstadt <ul style="list-style-type: none"> • Hospital care as a critical infrastructure (KRITIS): information security challenge • What does the kDL (critical service) mean in the implementation of (IT) security? • The media 'paradox of consternation' vs. real crisis communication: a practical discussion 		
10:20	Education Seminar Session 1 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;"> Accellion Enterprise content firewall – how to establish a secure content communication platform Alexander Kehl, Regional Director, D/CH, Accellion </td> <td style="width: 50%; padding: 5px;"> Patecco True security comes from within – dealing with privileged accounts Helmut Brachhaus, Chief Technology Officer, Patecco </td> </tr> </table>	Accellion Enterprise content firewall – how to establish a secure content communication platform Alexander Kehl , Regional Director, D/CH, Accellion	Patecco True security comes from within – dealing with privileged accounts Helmut Brachhaus , Chief Technology Officer, Patecco
Accellion Enterprise content firewall – how to establish a secure content communication platform Alexander Kehl , Regional Director, D/CH, Accellion	Patecco True security comes from within – dealing with privileged accounts Helmut Brachhaus , Chief Technology Officer, Patecco		
11:00	Networking & refreshments break		
11:30	Cloud security: a security benefit or a risk factor? Sebastian Hess , Cyber Risk Executive, American International Group <ul style="list-style-type: none"> • What makes an effective security programme and how is the cyber-risk posture shifting when moving to the cloud? • Are there trade-offs that accompany a cloud-centric IT service provision and/or cybersecurity approach? • The broader picture of non-technical considerations: Is there clearly preferred choice for one approach over the other? 		
11:50	Modern identity: unifying access and authentication Peter van Zeist , Sr. Solutions Consultant, LogMeIn <p>An overwhelming 92% of businesses are experiencing identity management challenges, from lack of resources to lack of security experience. The biggest challenge? Balancing ease of use for employees with increased security for the business. These two goals are critical, yet always at odds. How can IT securely manage users – their devices, apps, behaviour, and more – without making it more difficult for employees to do their job? Join us to discuss why having a comprehensive identity solution can balance the control IT needs with the experience users expect, and how LastPass Identity provides simple control and unified visibility across every access point, without the hassle of managing multiple solutions. Three key takeaways from the session:</p> <ul style="list-style-type: none"> • The most common challenges that businesses face when managing user identity • How to achieve both control for IT and a seamless experience that users expect from their identity solutions • How to get started with evaluating identity and access needs at your business 		
12:10	Investigations in fast mode: empowering SOC Analysts Nikolei Steinhage , Sr. Sales Engineer, CrowdsStrike <ul style="list-style-type: none"> • How SOC workflow can be automated to speed up analysis • What tools can be used to improve SOC efficiency • How to turn attacks into an opportunity to improve your defence 		

Agenda	
12:30	Education Seminars Session 2 Cybersprint Lessons learnt from monitoring Germany's digital footprint Eward Driehuis , Senior Vice President Strategy, Cybersprint
	Demisto, A Palo Alto Networks Company Journey to the centre of the SOC Babak Badkuba , Global and Major Account Manager, Demisto, A Palo Alto Networks Company
13:10	Lunch and networking
14:10	Catch me if you can – business, privacy, security & compliance – OneTeam! Henrik Becker , Director of Compliance & Risk Management, Unitymedia, and Carsten Renth , Director Operational Data Protection & Special Affairs, Unitymedia
	<ul style="list-style-type: none"> • Data protection, security and compliance – all for one (goal) • Requirements and chances in the area of tension between the 3 disciplines • Understanding risk as the basis for joint and sustainable action • One Team – an experience report • Conclusion, do's and don'ts
14:40	e-Crime in court: collect facts, convince judges! Spying on employees? Dr. Andreas Lober , Partner, BEITEN BURKHARDT
	<ul style="list-style-type: none"> • Not all judges are digitally native – how can you secure evidence and win the lawsuit? • Evidence is in the email inbox of a (former) employee – what to do? • Being right, getting justice, and enforcing the law: there's more than one option!
15:00	Education Seminars Session 3 Intel 471 Measuring and increasing the ROI on cyber-threat intelligence Maurits Lucas , Director of Intelligence Solutions, Intel 471
	Seclore Technologies Protecting confidential data from unauthorised access and espionage Jasbir Singh , Partner and Managing Director Europe, Seclore Technologies
15:40	Networking & refreshments break
16:00	EXECUTIVE PANEL DISCUSSION Is privacy the new security? Peter Vahrenhorst , Kriminalhauptkommissar, Landeskriminalamt Nordrhein-Westfalen Christoph Ritzer , Partner, Norton Rose Fulbright LLP Michael Schneider , Data Protection Officer, IKEA IT Germany GmbH Matthias Jungkeit , Chief Information Security Officer / DPO, Münchener Hypothekenbank Gennadij Feldstein , IT Security Officer, Commerzbank
16:30	Data protection notices and cookie bars (on the web) – sensible or useless? Michael Schneider , Data Protection Officer, IKEA IT Germany GmbH
	<ul style="list-style-type: none"> • Why data protection notices – in their current form – don't work • Cookie bars – do I need consent for each cookie? • Standardised icons: the solution?
16:50	Closing remarks
17:00	Conference close

Education Seminars	
<p>Accellion</p> <p>Enterprise content firewall – how to establish a secure content communication platform</p> <p>Alexander Kehl, Regional Director, D/CH, Accellion</p>	<p>Prevent breaches and compliance violations with secure third-party communication.</p> <p>Know more about the Accellion enterprise content firewall and how it helps IT executives lock down and govern the exchange of confidential enterprise information with the outside world without getting in the way of users. Thousands of global CIOs and CISOs trust Accellion to give their organisations protection, privacy and peace of mind. Get a live impression of the First Enterprise Content Firewall!</p> <p>What do I get out of the presentation?</p> <ul style="list-style-type: none"> • <i>See all content exchanged with third parties.</i> How to enable a total third-party communication visibility for businesses that need to share sensitive information beyond their enterprise borders. How to make sure the businesses have full visibility into how information is shared, who is accessing it, and where it is stored. • <i>Prevent sensitive data breaches and block malicious attacks.</i> How to offer a secure file transfer channel that protects your sensitive information in transit and at rest. Designed with security in mind from the ground up – architecture, data protection, authentication and authorisation – how to offer enterprise-class flexibility and scalability that will accommodate your specific security requirements and infrastructure strategy. • <i>Ease adoption and prevent shadow IT.</i> Figure out when a user clicks the secure sharing button inside email, web, mobile, office and enterprise apps, they know it’s the safe and secure way to share sensitive information with the outside world. How they also meet their more sophisticated needs for secure collaboration, virtual data rooms, managed file transfer, and SFTP on the same scalable platform, simply leveraging the same security infrastructure and compliance policies across human and machine interfaces. • <i>Unify content access, automate workflows, and deploy to fit your environment.</i> How to provide robust enterprise content access and workflow automation that allow users to securely access and share confidential enterprise content from applications, content management systems, network file shares, and cloud storage as easily as sharing local files
<p>Cybersprint</p> <p>Lessons learnt from monitoring Germany’s digital footprint</p> <p>Eward Driehuis, Senior Vice President Strategy, Cybersprint</p>	<p>In this talk, Cybersprint’s Chief Strategist Eward Driehuis will outline what he has learnt from securing dozens of organisations in Germany. By mapping their digital footprint, their strengths and weaknesses become visible. These relate to different kinds of cybercrime, but also regulatory risks such as GDPR misconfigurations. Based on this digital DNA, you’ll learn where opportunities and threats lie, and which steps are needed to increase the cyber-resilience.</p> <p>Key learnings:</p> <ul style="list-style-type: none"> • Insights from analysing thousands of German digital assets • Some of the most relevant risks and their root causes • How your organisation’s digital footprint is key in combating digital threats
<p>Demisto, A Palo Alto Networks Company</p> <p>Journey to the centre of the SOC</p> <p>Babak Badkube, Global and Major Account Manager, Demisto, A Palo Alto Networks Company</p>	<p>It’s easy to feel overwhelmed as part of a security team. Every day, analysts have to stare down the perils hidden at the centre of the SOC: too much noise, too many missed threats and too much manual remediation.</p> <p>It’s time to integrate automation and machine learning into every step of your security voyage.</p> <p>We’re presenting a live, thrill-packed session to help you do just that.</p> <p>Join us for this journey to the centre of the SOC and learn how to:</p> <ul style="list-style-type: none"> • Overcome today’s SOC challenges caused by siloed tools, limited analytics and manual investigations • Eliminate alert fatigue by grouping related alerts into incidents, reducing disparate alerts by 98% • Automate manual tasks with flexible orchestration to consolidate alerts and reduce incident response time

Education Seminars	
<p>Intel 471</p> <p>Measuring and increasing the ROI on cyber-threat intelligence</p> <p>Maurits Lucas, Director of Intelligence Solutions, Intel471</p>	<p>Cyber-threat intelligence can play a key role in managing cyber-risk by guiding strategic, tactical and operational decision making. However, determining the effectiveness and ROI of the results has been challenging.</p> <p>In this session we will show:</p> <ul style="list-style-type: none"> • How using a structured process anchored around intelligence requirements allows you to ensure that you are asking the right questions, getting the right intelligence and are able to measure the effectiveness of your CTI programme and adjust where necessary • Such an approach not only increases ROI but also vastly increases the contribution cyber-threat intelligence can make to reducing risk in your organisation
<p>Patecco</p> <p>True security comes from within – dealing with privileged accounts</p> <p>Helmut Brachhaus, Chief Technology Officer, Patecco</p>	<p>Privileged accounts continue to move into focus. This is partly because almost all cyber-attacks involve the use of hijacked privileged accounts, and partly because the regulatory requirements for privileged accounts are increasing all the time. Therefore it is important to regulate the handling of privileged accounts both organisationally and technically.</p> <p>Visit our seminar and learn more about the key processes, tools, and best practices around Privileged Access Management (PAM), and benefit from our long-term experience in this area.</p> <p>What participants are going to learn:</p> <ul style="list-style-type: none"> • Who you should involve in dealing with a privileged account • Which processes have to be introduced for dealing with privileged accounts • What the technical options are for protecting privileged accounts?
<p>Seclore Technologies</p> <p>Protecting confidential data from unauthorised access and espionage</p> <p>Jasbir Singh, Partner and Managing Director Europe, Seclore Tehnologies</p>	<p>Protecting confidential data from unauthorised access and espionage is a major challenge for every company. Data theft by employees, storing and sharing data in the cloud and compliance rules require companies to combine robust access control with usage rights. Digital Rights Management (DRM) solutions allow access to information to be controlled and monitored, regardless of data location or transmission path. Besides these advantages, many organisations have hesitated or tried and failed to successfully deploy DRM. The main problem is that in today's highly fragmented IT landscape, DRM systems are only efficient and productive if they can be implemented across platforms, consistently and with the ease of use, driving adoption.</p> <p>The session will explain how to approach the above as well as:</p> <ul style="list-style-type: none"> • Introduction of DRM and data centric security • Walk through the protection methods and why automation is important • Why ease of use is important especially for protected documents • Competitive dive, who does what and how • The journey to the cloud while being constantly protected by Seclore