

# Post event report



The 5<sup>th</sup>  
e-Crime & Cybersecurity Spain

21<sup>st</sup> November 2019 | Madrid, Spain

## Strategic Sponsors



## Education Seminar Sponsors



## Networking Sponsor

## Branding Sponsor



“ Me pareció el evento interesante. Pude contactar con las empresas que hicieron sus presentaciones e intercambiar tarjetas y opiniones. ”

Compliance Expert Consultant CEC,  
Mag Abogados

Inside this report:  
Sponsors  
Key themes  
Who attended?  
Speakers  
Agenda  
Education Seminars



### Speakers

- Maite Avelino, CISO, **Ministry of Finance**
- Manuel Barrios Paredes, CISO, **Solvía**
- Andrea Bellinzaghi, Technical Director Southern Europe, **IntSights**
- Jesús García Bautista, CISO and IT Chief, **Correos Express**
- Paulo Glorias, Regional Sales Director, **BitSight**
- Alvaro Grande, Security Engineer, **Telefónica**
- Héctor Guzmán Rodríguez, Director of Data Protection and Privacy, **BGBG Abogados**
- Eduardo Helering, EMEA Head of Solutions Engineering, **OneLogin**
- Dr. Susana Infantes, Principal Researcher, **Group Institut de Reserca Biomèdica de Lleida**
- Teresa Minguez Diaz, Director Compliance, **Porsche**
- Gabriel Moline, CISO, **Leroy Merlin**
- Alvaro Ortega, Head of Law Enforcement Outreach and Investigations Southern Europe, UK, Ireland & Nordic, **Western Union**
- Axel Pérez, Sales Engineer Iberia, **Zscaler**
- Laura del Pino Jiminez, Discipline Leader of Data and People Information Security, **BBVA**
- Teba Ríos, CIPP/E, CIPM, Solutions Engineer, **OneTrust**
- Ignacio Rodriguez, Lead Security Manager, **BT**
- Irene Rodriguez Ortega, Specialist, EMEA Cybersecurity Center, **Deloitte**
- María Rojo, Information Security Manager, **Airbus Defence & Space**
- Borja Rosales, UK, Spain & EMEA Director, Segasec/Javier Sánchez Salas, CISO, **Haya Real Estate**
- Pablo Rubio, IT Risk Management Engineer and Specialist, **Nationale Nederlanden**
- Siddharth Sharath Kumar, Product Evangelist, **ManageEngine**
- Raúl Vázquez Pastor, IT Risk Control – CyberRisk Manager, **Banco Sabadell**
- Fernando Vegas, former CIO and CRO, **OHL**

### Key themes

- Moving to secure solutions in the cloud
- Complying with new regulations
- Finding solutions that fit your needs
- Achieving the visibility you need
- Securing yourself against digital fraud
- Outsourcing what you cannot do in-house

### Who attended?



Agenda			
08:30	Registration and breakfast networking		
09:30	Chairman's welcome		
09:40	<b>DevSecOps pilot without bumping into the iceberg</b> <b>Javier Sánchez Salas</b> , CISO, Haya Real Estate <ul style="list-style-type: none"> <li>• Addressing security in the developments of a company in continuous evolution</li> <li>• Security as part of the Software Quality process</li> <li>• Securisation of the Development and Production Commissioning cycle</li> </ul>		
10:00	<b>2019 cyber risk – the year of the supply chain</b> <b>Paulo Glorias</b> , Regional Sales Director, BitSight <ul style="list-style-type: none"> <li>• Why supply chain management programmes need to be updated as the risks (hidden and not) presented by suppliers have drastically changed</li> <li>• Why current assurance mechanisms are failing and how companies can gain a deeper understanding of the risks hidden deep within their supplier ecosystems</li> <li>• Managing the types of risks presented by suppliers such as, human rights, diversity, cybersecurity, intellectual property and the handling of personal information</li> <li>• Use cases: how organisations are leveraging BitSight to manage risk in the supply chain framework, meet the demands of the business and manage cyber-risk</li> </ul>		
10:20	<b>Blockchain, new paradigms and its practical application in public administration</b> <b>Ignacio Rodriguez</b> , Lead Security Manager, BT <ul style="list-style-type: none"> <li>• Blockchain, new paradigm</li> <li>• Blockchain and cybersecurity</li> <li>• AAPP and new legislative and practical DNA</li> <li>• Challenges to assume</li> </ul>		
10:40	Refreshments and networking		
11:10	<b>EXECUTIVE PANEL DISCUSSION</b> <b>Women leadership executive panel discussion. Discussions on diversity in the cybersecurity, fraud and compliance industries</b> <b>Irene Rodriguez Ortega</b> , Specialist, EMEA Cybersecurity Center, Deloitte (Chair) <b>Dr. Susana Infantes</b> , Principal Researcher, Grup Institut de Reserca Biomèdica de Lleida <b>María Rojo</b> , Information Security Manager, Airbus Defence & Space <b>Teresa Minguez Diaz</b> , Director Compliance, Porsche <b>Laura del Pino Jiminez</b> , Discipline Leader of Data and People Information Security, BBVA		
11:30	<b>Leveraging the cloud for a successful digital transformation</b> <b>Axel Pérez</b> , Sales Engineer Iberia, Zscaler <ul style="list-style-type: none"> <li>• Cloud and mobility: the end of legacy security perimeter?</li> <li>• Taking advantage of corporate network transformation</li> <li>• App Access: the Zero Trust Network Access (ZTNA) concept</li> </ul>		
11:50	<b>The future of Multifactor Authentication (MFA)</b> <b>Eduardo Helering</b> , EMEA Head of Solutions Engineering, OneLogin <ul style="list-style-type: none"> <li>• What is multifactor authentication (MFA)?</li> <li>• How does it work?</li> <li>• How can it help us prevent a security breach?</li> <li>• The future of multifactor authentication, where are we going?</li> </ul>		
12:10	<b>Education Seminars   Session 1</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;"> <b>IntSights</b>  <b>The IntSights advantage</b>  <b>Andrea Bellinzaghi</b>, Technical Director Southern Europe, IntSights                             </td> <td style="width: 50%; padding: 5px;"> <b>OneTrust</b>  <b>Overcoming today's most pressing third-party risk management challenges</b>  <b>Teba Ríos</b>, CIPP/E, CIPM, Solutions Engineer, OneTrust                             </td> </tr> </table>	<b>IntSights</b> <b>The IntSights advantage</b> <b>Andrea Bellinzaghi</b> , Technical Director Southern Europe, IntSights	<b>OneTrust</b> <b>Overcoming today's most pressing third-party risk management challenges</b> <b>Teba Ríos</b> , CIPP/E, CIPM, Solutions Engineer, OneTrust
<b>IntSights</b> <b>The IntSights advantage</b> <b>Andrea Bellinzaghi</b> , Technical Director Southern Europe, IntSights	<b>OneTrust</b> <b>Overcoming today's most pressing third-party risk management challenges</b> <b>Teba Ríos</b> , CIPP/E, CIPM, Solutions Engineer, OneTrust		
12:50	Lunch and networking		

Agenda			
13:50	<p><b>EXECUTIVE PANEL DISCUSSION</b></p> <p><b>The new cybersecurity rulebook: how to survive in today's changing regulatory landscape</b></p> <p><b>Fernando Vegas</b>, former CIO and CRO, OHL (Chair)  <b>Alvaro Grande</b>, Security Engineer, Telefónica  <b>Héctor Guzmán Rodríguez</b>, Director of Data Protection and Privacy, BGBG Abogados  <b>Gabriel Moline</b>, CISO, Leroy Merlin</p> <p>The £183 million fine imposed on British Airways and the £99 million fine on Marriott for its Starwood breach are evidence that data privacy breaches can cause material financial losses. So is this the beginning of a new era in data privacy and protection? Do these fines finally give information security professionals the numbers they need to demonstrate the true financial value of what they do? In this panel we will look at:</p> <ul style="list-style-type: none"> <li>• GDPR enforcement: the full picture</li> <li>• Lessons from the fines: what does it mean for you?</li> <li>• Managing data governance across multiple regulatory regimes</li> </ul>		
14:10	<p><b>Anti-phishing 3.0: Strategies to REDUCE the phishing that undermines the reputation of your brand</b></p> <p><b>Borja Rosales</b>, UK, Spain &amp; EMEA Director, Segasec</p> <ul style="list-style-type: none"> <li>• Demo: a real IDN and Content Replication Attack-Simulation on a Spanish FS company</li> <li>• Why protecting your customers/consumers starts by bulletproofing your brand</li> <li>• Consumer targeting phishing: deal with the symptoms or tackle the roots</li> <li>• Defensive countermeasures that effectively reduce the number of attacks that use your brand to scam your customers</li> </ul>		
14:30	<p><b>Information security for the C-Level: measuring effectiveness</b></p> <p><b>Pablo Rubio</b>, IT Risk Management Engineer and Specialist, Nationale Nederlanden</p> <ul style="list-style-type: none"> <li>• Both external and internal (corporate) contexts are changing their perception about information security. There is a gap between security level offering and market/regulatory demands</li> <li>• Security topics need to accommodate in the Board of Directors agenda, in the same way other topics are discussed (accounting, sales, marketing, ...). Include information security in the business strategy as standalone security strategies are not considered relevant</li> <li>• Current technologies provide capabilities to measure security advantages business wise and more accurate, showing the outcome to the C-level in terms of business strategy: security Rol, security effectiveness and security culture achievements</li> </ul>		
14:50	<p><b>Education Seminars   Session 2</b></p> <table border="0"> <tr> <td> <p><b>ManageEngine</b>  <b>Advanced security monitoring techniques: augmenting SIEM with UEBA</b>  <b>Siddharth Sharath Kumar</b>, Product Evangelist, ManageEngine</p> </td> <td> <p><b>OneTrust</b>  <b>Bolster your incident response plan across privacy &amp; security teams</b>  <b>Teba Ríos</b>, CIPP/E, CIPM, Solutions Engineer, OneTrust</p> </td> </tr> </table>	<p><b>ManageEngine</b>  <b>Advanced security monitoring techniques: augmenting SIEM with UEBA</b>  <b>Siddharth Sharath Kumar</b>, Product Evangelist, ManageEngine</p>	<p><b>OneTrust</b>  <b>Bolster your incident response plan across privacy &amp; security teams</b>  <b>Teba Ríos</b>, CIPP/E, CIPM, Solutions Engineer, OneTrust</p>
<p><b>ManageEngine</b>  <b>Advanced security monitoring techniques: augmenting SIEM with UEBA</b>  <b>Siddharth Sharath Kumar</b>, Product Evangelist, ManageEngine</p>	<p><b>OneTrust</b>  <b>Bolster your incident response plan across privacy &amp; security teams</b>  <b>Teba Ríos</b>, CIPP/E, CIPM, Solutions Engineer, OneTrust</p>		
15:30	Refreshments and networking		
15:50	<p><b>EXECUTIVE PANEL DISCUSSION</b></p> <p><b>The unsustainable paradigm of the CISO: managing the business demands on today's information security professional</b></p> <p><b>Manuel Barrios Paredes</b>, CISO, Solvia (Chair)  <b>Raúl Vázquez Pastor</b>, IT Risk Control – CyberRisk Manager, Banco Sabadell  <b>Pablo Rubio</b>, IT Risk Management Engineer and Specialist, Nationale Nederlanden  <b>Maite Avelino</b>, CISO, Ministry of Finance</p>		
16:10	<p><b>Staying intelligent about fraud: new lessons in the fight against organised crime</b></p> <p><b>Alvaro Ortega</b>, Head of Law Enforcement Outreach and Investigations Southern Europe, UK, Ireland &amp; Nordic, Western Union</p> <ul style="list-style-type: none"> <li>• The Intelligence Unit in the fight against organised crime</li> <li>• The importance of public-private collaboration in crime-fighting</li> <li>• The evolution of fraud in connection with other criminal activity</li> </ul>		
16:30	<p><b>The unsustainable paradigm of the CISO</b></p> <p><b>Jesús García Bautista</b>, CISO and IT Chief, Correos Express</p> <ul style="list-style-type: none"> <li>• The unsustainable paradigm of the CISO. The responsibility of the CISO has increased substantially in recent years, taking a more defined form and seeing how its recommendations are being considered, but progress is still needed. How does today's information security leader balance the various business demands?</li> <li>• Technology does not stop: infrastructure in the cloud, containers, the loss of roles of systems and development personnel, leads us to think and design new ways to protect ourselves. How do we develop the right strategies and choose the right partners to keep up?</li> <li>• Securing a hyper-connected world. The growth of online commerce and shopping on web services such as Amazon, PC Components, Zara is changing the way we do business. El Corte Inglés, is revolutionising the world of express transport. Case study and actionable takeaways on how to secure the digitalised business</li> </ul>		
16:50	Chairman's close		

Education Seminars	
<p><b>IntSights</b></p> <p><b>The IntSights advantage</b></p> <p><b>Andrea Bellinzaghi,</b> Technical Director Southern Europe, IntSights</p>	<p>With the ever-growing threat universe, cybersecurity teams trying to protect their organisations from every attack are in a losing battle. They are overwhelmed, exhausted, and ultimately ineffective.</p> <p>A smarter approach would be for teams to focus on the attacks that matter most – those specifically targeting their organizations. The problem is how to do this efficiently. Until now, finding the most relevant threats required research that was so time-consuming, it defeated the purpose.</p> <p>IntSights has changed this dynamic. Only IntSights provides cybersecurity teams with an effective, automated way to identify threat data, attack indicators specific to their organisations and automatically mitigate them.</p> <ul style="list-style-type: none"> <li>• External threat protection</li> <li>• The IntSights Intelligence Process</li> <li>• Orchestration, automation and remediation</li> </ul>
<p><b>ManageEngine</b></p> <p><b>Advanced security monitoring techniques: augmenting SIEM with UEBA</b></p> <p><b>Siddharth Sharath Kumar,</b> Product Evangelist, ManageEngine</p>	<p>In the age of advanced threats and sophisticated malicious insiders, security teams face an uphill task. In order to detect and mitigate security incidents, organisations must revisit their security monitoring strategy and ensure that they are equipped with the right set of tools. This session talks about the latest trends in the realm of security information and event management (SIEM) and why it is important to incorporate machine learning techniques by leveraging user and entity behaviour analytics (UEBA).</p> <ul style="list-style-type: none"> <li>• Challenges in security monitoring</li> <li>• Integrating event and non-event information into your SIEM solution</li> <li>• Anomaly-based detection with UEBA</li> <li>• Key concepts and use cases</li> </ul>
<p><b>OneTrust</b></p> <p><b>Overcoming today's most pressing third-party risk management challenges</b></p> <p><b>Teba Ríos, CIPP/E, CIPM,</b> Solutions Engineer, OneTrust</p>	<p>Managing third-party vendor risk before, during and after onboarding is a continuous effort under global privacy laws and security regulations. While outsourcing operations to vendors can alleviate business challenges, managing the associated risk with manual tools like spreadsheets is complex and time consuming. To streamline this process, organisations must put procedures in place to secure sufficient vendor guarantees and effectively work together during an audit, incident – or much more. In this session, we'll breakdown a six-step approach for automating third-party vendor risk management and explore helpful tips and real-world practical advice to automate third-party privacy and security risk programmes.</p> <ul style="list-style-type: none"> <li>• Review the drivers and challenges organisations face when managing third-party vendor risk</li> <li>• Identify priorities before, during and after vendor procurement</li> <li>• Takeaway a six-step approach for automating the third-party vendor risk lifecycle</li> <li>• Hear real case studies from privacy experts on how to practically tackle the third-party vendor risk</li> </ul>
<p><b>OneTrust</b></p> <p><b>Bolster your incident response plan across privacy &amp; security teams</b></p> <p><b>Teba Ríos, CIPP/E, CIPM,</b> Solutions Engineer, OneTrust</p>	<p>In the event of a breach, privacy and security professionals often approach incident response from two different outlooks. Whereas security teams are focused on threat vectors, privacy teams are concerned with personal data leaks and adhering to various global privacy laws. While the two come from different perspectives, it is possible to build an incident and breach response plan that addresses the needs of both teams. In this session, we'll discuss how to build a harmonised response plan that addresses both the security team's technical needs and privacy team's regulatory requirements across the patchwork of US privacy laws, the GDPR and other global privacy regulations. We'll also provide tips to help you map out a 72-hour personal data breach action plan and share practical advice to improve your privacy programme.</p> <ul style="list-style-type: none"> <li>• Learn how to build an incident and breach response plan that fits the needs of security teams and privacy teams</li> <li>• Breakdown what stakeholders, teams, tools and processes should come together in the event of an incident or breach</li> <li>• Understand how to maintain a consistent approach to incident response while complying with privacy regulations across the globe</li> </ul>