

Post event report



The 2nd
e-Crime & Cyber Security Spain

10th November 2016 | Madrid, Spain

Strategic Sponsors



Education Seminar Sponsors



Networking Sponsors



Branding Sponsor



“ Evento muy bien organizado, ajustándose en todo momento a la agenda prevista. Contenidos de las sesiones muy variados e interesantes y presentados por oradores relevantes en el sector, amenos y conocedores de la materia impartida. Presentación de últimas tendencias en productos de seguridad, así como facilidad para establecer contacto con sus fabricantes en el área de exhibición. Oportunidad para relacionarse con profesionales de otras empresas y/o sectores con problemáticas similares e intercambiar experiencias. En definitiva, un día bien aprovechado. ”

Jefe de Sistemas Unix, Sistemas Unix, Cecabank

“ Muchas gracias por darme la oportunidad de poder participar en el evento, me resulto muy interesante, supero al anterior, los ponentes como siempre de primer orden y las ponencias claras, directas, dirigidas a proponer soluciones a los problemas que tenemos todos como usuarios de las redes. ”

Director de Seguridad, Novo Banco

“ Como valoración, creo que la edición 2016 del evento e-Crime Spain ha mantenido y mejorado el nivel y la profesionalidad de la ya celebrada en el año 2015, que fue toda una inesperada sorpresa por la buena organización, la puntualidad en todas las actividades y el interés y nivel profesional de las conferencias y los ponentes. ”

Gerente de Seguridad, Isdefe

Inside this report:

- Sponsors
- Key themes
- Who attended?
- Speakers
- Agenda
- Education Seminars



Speakers

Josep Alborns,
Chief Communications Officer
ESET

Enrique Ávila,
Director
**Centro Nacional de Excelencia
en Ciberseguridad**

Manuel Barrios Paredes,
CISO
Informática El Corte Inglés

Ignacio Berrozpe,
Sales Engineer South EMEA
Vormetric, a Thales company

David Conde,
SOC/CERT Manager
S21sec

Israel Diaz Dominguez,
CISO
Paginas Amarillas

Alejandra Frías López,
Senior Judge.
Advisor at the
Ministry of Justice.
Member of the
National Cybersecurity Council

Anton Grashion,
Senior Director of Product Marketing,
EMEA
Cylance

Aaron Higbee,
Chief Technology Officer & Co-founder
PhishMe

Emmanuel Meriot,
Country Manager France and Spain
Darktrace

Juan Quintanilla,
SOC Service Delivery Manager
Airbus España

Santiago Gómez Sancha,
Director of Information Systems
Uría Menéndez

Juan Carlos Sanchez,
CISO
CESCE

Juan Ramón Caravaca Sánchez,
CCO, CISO

Senior Representative
Guardia Civil

Fernando Vegas,
CIO
Grupo OHL

Key themes

Employee engagement

Is financial sector cyber security up to scratch?

Payments innovation and cyber risk

The foundations of cyber resilience

Understanding the small print of new regulation

Who attended?



Cyber-security

We have a 15-year track record of producing the events cyber-security professionals take seriously



Risk Management

We attract senior risk officers with responsibility for information risk assessment and mitigation



Fraud, Audit, Compliance

We provide the go-to events for fraud prevention and compliance owners at the world's key corporates



Data Protection & privacy

We are a key venue for decision-makers with budget and purchasing authority

Agenda			
08:30	Registration		
09:30	<p>Cyberterrorism: The new threats</p> <p>Senior Representative, Guardia Civil</p> <ul style="list-style-type: none"> Looking at the recent developments and the creation and growth of new ICT technologies being used by terrorists What does Guardia Civil's Cyberterrorism Group do in order to analyse, combat and investigate crime to ensure national security and ensure public safety? What is the latest thinking on emerging threats and the potential use for cyber space by terrorists? 		
09:50	<p>The myth of phishing awareness</p> <p>Aaron Higbee, Chief Technology Officer & Co-founder, PhishMe</p> <ul style="list-style-type: none"> People click phishing emails because they are unaware of the threat. So the answer is to make them aware right? Early on we believed this too, until the data proved it completely wrong In 2008 this was partly true, in 2016, we need to bury this fairy-tale 		
10:10	<p>Education Seminars</p> <table border="1"> <tr> <td> <p>ESET Mandatory security rules for trading in/with the European Union Josep Albers, Chief Communications Officer, ESET</p> </td> <td> <p>Vormetric, a Thales company Addressing the challenges of protecting data Ignacio Berrozpe, Sales Engineer South EMEA, Vormetric, A Thales Company</p> </td> </tr> </table>	<p>ESET Mandatory security rules for trading in/with the European Union Josep Albers, Chief Communications Officer, ESET</p>	<p>Vormetric, a Thales company Addressing the challenges of protecting data Ignacio Berrozpe, Sales Engineer South EMEA, Vormetric, A Thales Company</p>
<p>ESET Mandatory security rules for trading in/with the European Union Josep Albers, Chief Communications Officer, ESET</p>	<p>Vormetric, a Thales company Addressing the challenges of protecting data Ignacio Berrozpe, Sales Engineer South EMEA, Vormetric, A Thales Company</p>		
10:50	Refreshments & networking break		
11:20	<p>EXECUTIVE PANEL DISCUSSION The challenges facing today's CISO</p> <p>Fernando Vegas, CIO, Grupo OHL Israel Diaz Dominguez, CISO, Paginas Amarillas Juan Ramón Caravaca Sánchez, CCO, CISO Juan Quintanilla, SOC Service Delivery Manager, Airbus España Moderator: Santiago Gómez Sancha, Director of Information Systems, Uría Menéndez</p>		
11:40	<p>Balancing risk – tackling security challenges with AI</p> <p>Anton Grashion, Senior Director of Product Marketing, EMEA, Cylance</p> <ul style="list-style-type: none"> The need for endpoint protection is nothing new and organisations don't spend a lot of time thinking about it, even though traditional security suites can only protect against threats that have been previously identified Artificial intelligence can secure a system against previously unknown threats, in addition to threats that may hide their malicious behaviour while under scrutiny Legacy solutions that sort through signatures stored in their database to determine whether an application meets their profile of a threat depend on the threat already existing within the database How to stop the millions of new threats that are released each month, many of which are able to hide their presence and mimic other types of file Modern enterprises inevitably increase their attack surface area as they adopt new and different work practices in order to better compete 		
12:00	<p>Stay smart: How cyber intelligence, compliance, and recruitment can add business value</p> <p>Enrique Ávila, Director, Centro Nacional de Excelencia en Ciberseguridad</p> <ul style="list-style-type: none"> Overcoming the concept of cyber security. This business is a game of cyber intelligence The question is not whether we have a security incident, but when and how we will face it The need to generate future scenarios of digital evidence as a measure of cyber resilience and compliance NIS Directive. Directive 2013/40 / UE: Criminal liability in case of regulatory compliance Talent as a scarce resource. The loss of talent, an unavoidable risk The urgent need to recruit talent. The first visibility of it as value to a business Dual-use technologies: Reputation and report vs command and control systems 		
12:20	<p>The Enterprise Immune System: Using machine learning for next-generation cyber defence</p> <p>Emmanuel Meriot, Country Manager France and Spain, Darktrace</p> <ul style="list-style-type: none"> How new machine learning and mathematics are automating advanced cyber defence Why 100% network visibility allows you to detect threats as they happen, or before they happen How smart prioritisation and visualisation of threats allows for better resource allocation and lower risk Real-world examples of unknown threats detected by 'immune system' technology 		

Agenda	
12:40	<p>A SOC today, changing the paradigm</p> <p>David Conde, SOC/CERT Manager, S21sec</p> <ul style="list-style-type: none"> • From SOC to Cyber Intelligence Centre • How the model needs to be evolved in order to meet the current environment • Solutions to face new advanced threats, from reactive to preventive
13:00	Lunch and networking break
14:00	<p>The Directive on security of network and information systems</p> <p>Alejandra Frías López, Senior Judge. Advisor at the Ministry of Justice. Member of the National Cybersecurity Council</p> <ul style="list-style-type: none"> • The effect of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union • The interrelation of the Directive with other standards: Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure • New challenges: the fight against hybrid threats
14:20	<p>Everyday information theft, and what it's costing your business</p> <p>Manuel Barrios Paredes, CISO, Informática El Corte Inglés</p> <ul style="list-style-type: none"> • Everyday information theft and its economic and reputational costs to private and public organisations • 'Everyone's a hacker': The developing sophistication and accessibility of hacking today • The most popular practical techniques that threaten information security in corporate environments
14:40	Refreshments and networking break
15:00	<p>Implementing cyber security strategy throughout the global organisation</p> <p>Juan Carlos Sanchez, CISO, CESCE</p> <ul style="list-style-type: none"> • Challenges faced during the process • Solutions to implementing a global cyber security strategy • Case study from CESCE
15:20	<p>The last line of defence: People</p> <p>Santiago Gómez Sancha, Director of Information Systems, Uría Menéndez</p> <ul style="list-style-type: none"> • They're not users, they're people • How to convince the board • How to improve employee awareness • How to create new habits of 'cyber caution' • What about tomorrow?
15:45	Conference close

Education Seminars	
<p>ESET</p> <p>Mandatory security rules for trading in/with the European Union</p> <p>Presenter: Josep Albors, Chief Communications Officer, ESET</p>	<p>Europe has decided to enforce mandatory security measures to all companies that, by any commercial or business activity, deal with European citizens' personal data. The most important rule that regulates these obligations is called 'General regulation of data protection'.</p> <p>This regulation forces to implement measures such as encryption systems, two-factor authentication systems, key management systems, etc. Likewise, all the foreign companies that wish to deal with European citizens' data such as names, surnames or e-mails, are obliged to sign specific contracts about data privacy.</p> <p>Failing to meet any of these rules entails a penalty in the form of a fine up to 20 million Euros or up to 4% of the global turnover of the company in the previous financial year.</p> <p>What attendees will learn:</p> <ul style="list-style-type: none"> • Know European IT security laws that affect European and foreign companies • Knowing to avoid illegal activities that could happen • Know which are the cases in which it is mandatory to encrypt or set up two-factor authentication, backup and DLP systems • Know which are the IT security systems that allow the companies to fulfill all these requirements
<p>Vormetric, a Thales company</p> <p>Addressing the challenges of protecting data</p> <p>Presenter: Ignacio Berrozpe, Sales Engineer South EMEA, Vormetric, A Thales Company</p>	<p>Cyber threats are not diminishing. Protecting an organisation's data is critical to the daily workings, reputation and future growth of every business. Within European enterprises action is being taken with a focus to protect 'data at rest'.</p> <p>This session will discuss how organisations are making that move. Using real life examples, it will illustrate how security professionals within global brands are adopting a strategy of encrypt everything to address the onslaught of cyber threat and compliance mandates such as PCI DSS and GDPR. Ultimately a strategy that enables them to create a best practice approach to protecting their data and their reputation.</p> <p>What attendees will learn:</p> <ul style="list-style-type: none"> • The growth of cyber threats facing the enterprises • Forthcoming compliance considerations including GDPR • Why organisations are shifting their data protection strategy to focus on data at rest • Why organisations are now adopting a strategy of 'encrypt everything' • A best practice approach to protecting data