Post event report

Strategic Sponsors

DARKTRACE

KnowBe4
Human error. Conquered.

SentinelOne™

SOCRadar®

Education Seminar Sponsors

DEVO

RELIAQUEST

Reveal security

Synack

Networking Sponsors

eset
ENJOY SAFER TECHNOLOGY™

FORESCOUT

MEND
You Code. We Cure.

Branding Sponsors

MENLO SECURITY

stratesys

"I wanted to convey my congratulations for the event. Both the organisation, the management of the talks and the selection of contents were excellent. I thank you for your invitation and I hope we will see each other at the next event."

Jefe del Departamento de Asesoramiento Técnico TIC, Congreso de Diputados

"Congratulations. Great event and organisation. The exhibitions had some luxury speakers, very instructive. The roundtables are also very good, both moderated and the choice of content to be discussed."

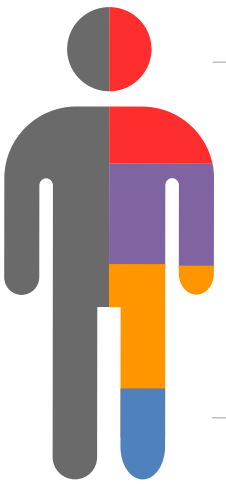
Dpto IT Corporativo, El Corte Ingles

Inside this report:

Key themes

- Can zero trust be done?
- Here comes real cybersecurity regulation
- Cloud native next
- Securing the citizen
- Ransomware – dealing with the new normal
- From smart machines to smart cities – securing the IoT
- Developing the next generation of security leaders
- Securing digital currencies
- The pros and cons of managed services
- Closing the cybersecurity skills gap
- Building better Cloud security
- Are AI/ML solutions the answer?

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

Speakers

José Badía Lopéz,
Country Manager Spain & Portugal
Darktrace

Raúl Benito,
Regional Sales Manager Iberia
SentinelOne

Moshe Benoliel,
VP of Business Development
Reveal Security

Enrique Cervantes Mora, CISO
Fintonic

Stefano De Blasi, Cyber Threat Intelligence Analyst, **ReliaQuest**, Digital Shadows, a ReliaQuest Company

Ramon De La Iglesia Vidal, Head of Cybersecurity & Emerging Risks
Santander Consumer Finance

Alejandro Espejo-Saavedra López,
Head of Information Security & Compliance/CTO
Telefonica

Nacho García Egea, CTO, A3SEC, on behalf of **SOCRadar**

David González, CISO
Coren

Paco Huerta,
Vice President Product Management
Devo

Udo Llorens, CTO & CISO
Dune Technology

Juan Carlos López Ruggiero, CISO
Bouygues Energies & Services

Jesús Mérida Sanabria, CISO
Iberia

Eusebio Moya López, Head of Data Protection & Cyber Security
Diputación Provincial de Valencia

Alejandro Novo, Country Manager, Spain
Synack

Jorge Pardeiro Sánchez,
Global IT Security Architecture
Banco Sabadell

Laura Parra,
Global Director of IT Strategic Projects
Cellnex Telecom

Javier Sánchez Salas, CISO
ENGIE

Jesús Valverde Romero, Head of Information Technology & Cybersecurity
ISEMAREN

Jelle Wieringa,
Security Awareness Advocate
KnowBe4

Agenda

08:30 Registration & networking

09:30 Chairman's welcome

09:40 **The vulnerability vector: An opportunity for the hacker and a challenge for the CISO**

Juan Carlos López Ruggiero, CISO, Bouygues Energies & Services

- Malicious actors are so much better organised (and financed) than company CISOs
- How do we survive the threats and stay one step ahead?
- What works and what doesn't when facing the challenges in an ever changing scenario?

10:00 **How an AI thinks like an attacker**

José Badía Lopéz, Country Manager Spain & Portugal, Darktrace

- In the face of increasing cyber-risk, it is no longer enough to detect and respond to attacks. Organisations must take proactive steps to prevent threats before they occur, and to recover if they are compromised
- In this session, Darktrace unveils an ambitious new approach to security, with core engines that power AI technologies to prevent, detect, respond to, and ultimately heal from attacks
- Together, these engines combine to strengthen the security posture of organisations in a virtuous AI feedback 'loop', providing powerful, bespoke, self-learning, end-to-end solutions unique to each organisation

10:20 **Education Seminars | Session 1**

Devo	Synack
The autonomous SOC: richer data, guided analytics and the power of the community	**A better way to pentest**
Paco Huerta, Vice President Product Management, Devo	**Alejandro Novo,** Country Manager, Spain, Synack

11:00 Networking break

11:30 **No cybersecurity, no digital transformation**

Jesús Mérida Sanabria, CISO, Iberia

- What are the most significant security risks of business and process digitalisation?
- Which new digital technologies introduce the most risk and how can they be secured? [As organisations transform, they will use more cloud services, AI products, big data analytics, Internet of Things (IoT) devices etc.]
- How can cybersecurity be incorporated into transformation projects and by whom?

11:50 **Psychology of a social engineering attack**

Jelle Wieringa, Security Awareness Advocate, KnowBe4

In this talk, you will better understand how cybercriminals leverage the power of your own mind to make you do their bidding. And how a better understanding of yourself can help to better protect against this.
Get actionable insights on:

- The tricks cybercriminals use to manipulate you
- How psychology plays a vital role in social engineering
- How to better protect yourself

12:10 **SentinelOne security platform, new era needs autonomous and interconnectable platforms**

Raúl Benito, Regional Sales Manager Iberia, SentinelOne

- Contextualisation of incidents
- Fast and efficient response
- Interconnection of all security elements in response

12:30 **Independent cyber-risk management function in banking**

Ramon De La Iglesia Vidal, Head of Cybersecurity & Emerging Risks, Santander Consumer Finance

- Principles of the second line of defence and its evolution in cyber/IT
- Who, how and why?
- Risk models: then and now
- Summary & tips

Agenda

12:50 — **Education Seminars | Session 2**

Reveal Security

Monitoring authenticated users in business applications to detect external attackers and rogue insiders

Moshe Benoliel, VP of Business Development, Reveal Security

ReliaQuest

Maximise your threat intelligence: Four proven steps to integrating threat intelligence for higher-fidelity detection and response

Stefano De Blasi, Cyber Threat Intelligence Analyst, ReliaQuest, Digital Shadows, a ReliaQuest Company

13:30 — Lunch break

14:30 — **EXECUTIVE PANEL DISCUSSION** | **CISO security challenges**

Juan Carlos López Ruggiero, CISO, Bouygues Energies & Services (Moderator); **David González,** CISO, Coren; **Udo Llorens,** CTO & CISO, Dune Technology; **Jesús Valverde Romero,** Head of Information Technology & Cybersecurity, ISEMAREN; **Alejandro Espejo-Saavedra López,** Head of Information Security & Compliance/CTO, Telefonica

Stepping back from the day-to-day necessities, what challenges in firms' digital environments cause greatest problems for the information security programme; how does the information security function mitigate and alleviate the burden on their IT and business colleagues to solve them? This panel will look at the challenges posed by:

- asset inventories (devices, applications, identity, network, data)
- overall technology landscape complexity,
- 'digital' transformations of the business/products
- testing and measuring the effectiveness of the cybersecurity control environment
- incident response and problem management
- ensuring the same coverage/visibility over cloud environments as on-prem
- managing supply chain risk in a world less tolerant to long delays around supplier assurance (post covid)
- Web 3.0 and the next generation of the internet: securing new technologies and services which are inherently decentralised?

15:00 — **SOCRadar's Spain Threat Landscape Report: Threat actors and attack types**

Nacho García Egea, CTO, A3SEC, on behalf of SOCRadar

- Which threat actors targeted Spanish organisations?
- What kind of TTPs were used in the attacks?
- Learned lessons and mitigation recommendations

15:20 — Networking break

15:40 — **Cybersecurity in local administration: the achilles heel of the public sector?**

Eusebio Moya López, Head of Data Protection & Cyber Security, Diputación Provincial de Valencia

- The challenge of securing citizens' data within local councils and other bodies
- Security on a budget: the role of cybersecurity vendors
- Case study: a real-world example of how local entities can get security right

16:00 — **EXECUTIVE PANEL DISCUSSION** | **CISOs and security technology**

Laura Parra, Global Director of IT Strategic Projects, Cellnex Telecom (Moderator); **Jorge Pardeiro Sánchez,** Global IT Security Architecture, Banco Sabadell; **Javier Sánchez Salas,** CISO, ENGIE; **Enrique Cervantes Mora,** CISO, Fintonic

As cybersecurity matures, CISOs have a better idea of the key digital risks to their businesses and the types of security solutions they require. At the same time, vendors are consolidating and providers of enterprise application suites and cloud services are strengthening the security capabilities of their offerings or buying security vendors (as Google has with Mandiant). So, this panel will look at:

- Different approaches to selecting and consolidating security technologies
- Budget and investment questions as more vendors broaden their capabilities
- Replacing legacy cybersecurity technology
- One-stop shop versus security stack
- Building a continuous control environment for cybersecurity

16:30 — Conference close

Education Seminars	
Devo **The Autonomous SOC: richer data, guided analytics and the power of the community** **Paco Huerta,** Vice President, Product Management, Devo	How effective is your security operations and your ability to gather evidence, investigate and find source data? If unsure, you're not alone. Combating today's threats requires new approaches to how your SOC manages its data, analytics, and expertise. Join Devo as we explore innovative ways your security team can thrive in the era of massive data growth, talent shortage, and constantly evolving threats. Top 3 takeaways: • Cloud-based solutions scale to achieve the critical full visibility into threats, giving you a single source of truth • Analytics that use automation and machine learning uplift analysts' performance, saving your security team valuable time • Community expertise augments your tribal knowledge to quickly resolve threats, helping you bridge the industry talent gap
ReliaQuest **Maximise your threat intelligence: Four proven steps to integrating threat intelligence for higher-fidelity detection and response** **Stefano De Blasi,** Cyber Threat Intelligence Analyst, ReliaQuest, Digital Shadows, a ReliaQuest Company	Accurate, trustworthy threat intelligence is a boon if you have it – but too much of it becomes a management headache. Analyst group 451 Research, surveying security leaders for its report Tackling the Visibility Gap in Information Security, found that 49% of enterprises using SIEM, EDR, and other security tools were overwhelmed by the day-to-day operation of managing and ingesting threat feeds into their growing technology stack. The problem is one of balance: Too little intel, and your organisation runs the risk of failing to notice (or be prepared for) a major threat. Too many intel feeds, and the risk is that your team becomes overwhelmed by data. Just because you have a large quantity of intel doesn't mean your security teams and technologies can process it and use it effectively. During this session, you will be able to learn: • How to integrate threat intelligence with security programmes • What processes are needed to create high-fidelity threat detection • Why examining both indicators of compromise and behaviour patterns are key to improving security
Reveal Security **Monitoring authenticated users in business applications to detect external attackers and rogue insiders** **Moshe Benoliel,** VP of Business Development, Reveal Security	This session demonstrates the detection of malicious activities in and across applications by contextualising entire journeys of users. • This session explores the growing need for user journey analytics within and across business applications to accurately detect malicious activities performed by authenticated users • Current detection solutions are application-specific and in most cases ineffective, due to many false positives • Analysing and contextualising entire journeys of users through and across application enables the detection of fraud, malicious activities and application misuse by both external attackers and rogue insiders • Examples: an attacker's takeover of a checking account via social engineering; a customer service agent modifying an insurance policy to add themselves as a beneficiary; a salesperson downloading a report of all customers before switching to work at a competitor
Synack **A better way to pentest** **Alejandro Novo,** Country Manager, Spain, Synack	Antiquated legacy penetration testing methods fail to catch all the critical vulnerabilities that exist within a company's environment, which puts organisations at risk. Learn more about the challenges and deficiencies of traditional pentesting, and how Synack's innovative and continuous solutions can help organisations protect critical software, platforms, and APIs more effectively while meeting increased security requirements. In this session, you will learn: • Why the current model of compliance-based penetration testing is increasingly ineffective and obsolete • Which exploitable vulnerabilities are missed the most and cause the greatest concerns for organisations and CISOs • How an adversarial model with teams of international top class security researchers (with a hacker mindset) provides the necessary critical mass