Post event report

Strategic Sponsors

DeepRecce

esentire

NSFOCUS

satisnet
streamlining security management

ThreatMetrix
The Digital Identity Company

TREND MICRO

Education Seminar Sponsors

COMSEC Group
Cyber & Information Security

SIRIUM
SECURE · SCALE · SIMPLIFY

Pervade Software

RISKIQ

TeleSign

Networking Sponsors

EMERSON
Network Power

Pay360 by Capita

ZENEDGE
MAKING CYBERSECURITY SMARTER

Branding Sponsor

Experian

"The quality of attendees was great. Attendees were happy to engage and the right people to talk to."
NuData Security

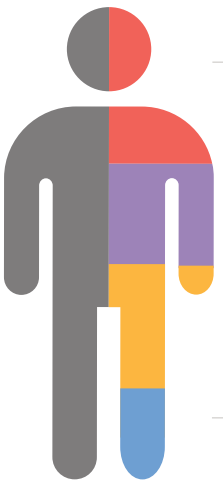
"I enjoyed the event indeed. I had the chance to network with nice people all relevant to the subject of the event. All the vendors having their desk there were related to prevention, detection and response and they were all helpful. Presentations were short and to the point. Presenters were easy to approach."
Cyber Security Manager, SKY

Inside this report:

Key themes

- Open source and cloud solutions
- Automating security
- Secure application development
- Continuous security delivery

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

Aftab Afzal,
SVP & GM EMEA,
NSFOCUS

Giacomo Collini,
Director of Information Security,
King

Jonathan Davies, CTO,
Pervade Software Ltd

Gabriel Dezon, Lead IT Auditor,
Camelot Group

Simon Edwards CISSP,
Cyber Security Architect EMEA,
Trend Micro

Dr. Grigorios Fragkos,
Head of Offensive CyberSecurity,
DeepRecce

Dan Gurfinkel,
Head of Offensive Security &
Response Unit,
Comsec Consulting

Andy Harris,
Engineering Director, Osirium

Richard Jones,
Operations Manager,
National Cyber Crime Unit (NCCU),
National Crime Agency (NCA)

Caroline Kean,
Litigation Partner,
Wiggin LLP

Jeff Lenton,
Solution Architect, RiskIQ EMEA,
RiskIQ

John McCann,
Director of Honeycomb Technologies and
Security Integrator,
Satisnet

Milorad Mitrović,
EMEA Sales Engineer,
TeleSign

Lluis Mora,
Head of Information Security and
Technology Governance,
bwin.party digital entertainment

Joe Nelson,
Senior Solutions Engineer – EMEA,
eSentire

Jon O'Keefe,
Network and Security Engineer,
Codemasters

Ian Spanswick,
Director, Customer Engagement –
EMEA,
ThreatMetrix

Agenda

08:00 Registration

08:50 Chairman's welcome

09:00 **Preventing involvement in cybercrime: The NCA Prevent response**

Richard Jones, Operations Manager, National Cyber Crime Unit (NCCU), National Crime Agency (NCA)

- Introduction to Cyber Prevent
- Pathways into cybercrime and offender behaviour
- The NCCU's Prevent Gaming project
- Positive interventions to divert from the cybercrime pathway

09:20 **Intelligent hybrid security**

Aftab Afzal, SVP & GM EMEA, NSFOCUS

Move toward an intelligent hybrid security model by taking the following steps:

- Take an intelligent look across the network: Execute on a vision of an intelligent ecosystem of threat-aware solutions combined into a single entity that dramatically increases the visibility of the entire network and application landscape in the enterprise
- Eliminate silos with integrated defences: Deploy defences that interoperate with and are fully aware of the other defences in place, communicating vertically with the cloud and laterally across the entire enterprise, helping eliminate security silos and fragmented approaches.
- Identify security blind spots: Implement closed-loop threat intelligence feedback for both cloud and on-premises defences that removes blind spots and significantly reduce the time from measure to counter-measure, infection to detection
- Automate threat intelligence: Consume real-time global threat intelligence and put it into action across all of the security technologies deployed within the enterprise, in an automated fashion that requires no human interaction

09:40 **Is threat intelligence enough? Tips and tricks for day-to-day operations**

Joe Nelson, Senior Solutions Engineer – EMEA, eSentire

- Methods to identify where the addition of a threat intelligence source might save time and money in a security process
- Know your enemy: Using threat intelligence against malware, ransomware and phishing
- Best practices to defend your network from the evolving cyber threat

10:00 **Education Seminars | Session 1**

Osirium	TeleSign
Really useful security: Maintaining privileged access management in a multi-dependency environment **Andy Harris,** Engineering Director, Osirium	Top security threats in online gaming and how to protect your user ecosystem **Milorad Mitrović,** EMEA Sales Engineer, TeleSign

10:40 Refreshments and networking break

11:10 **Playing a new game: When a traditional gaming company goes digital**

Gabriel Dezon, Lead IT Auditor, Camelot Group

- Changes/developments in the gaming industry landscape
- What does this mean from an information security perspective?
- Threats and risks from an internal audit viewpoint: What do you need to know?

11:30 **Digital identity intelligence: The ace up your sleeve**

Ian Spanswick, Director, Customer Engagement – EMEA, ThreatMetrix

- Latest insights into gaming fraud trends – across payments, account creations and logins
- Identifying valued customers versus fraudsters in real-time
- Reducing abandonment and fraud losses with digital identity intelligence
- Minimising bonus abuse and improving regulatory compliance

11:50 **Information security in an agile environment**

Giacomo Collini, Director of Information Security, King

- How to leverage agile principles and risk driven approach
- Listen to the business, prepare for the worst
- Put people at the centre of the picture, focus on awareness and ownership

Agenda

12:10 — Orchestrating and automating cyber security in the gaming industry

John McCann, Director of Honeycomb Technologies and Security Integrator, Satisnet

- Cybercriminals often use big sporting and social media events to lure users with phishing emails and fake websites, exposing fans to intensified and new potential cyber risks
- Discover how to respond to these new attacks and maximise use out of the security technologies you have invested in

12:30 — Education Seminars | Session 2

Comsec Consulting	TeleSign
New generation DDoS attacks – is the online gaming industry secured? **Dan Gurfinkel,** Head of Offensive Security & Response Unit, Comsec Consulting	Top security threats in online gaming and how to protect your user ecosystem **Milorad Mitrović,** EMEA Sales Engineer, TeleSign

13:10 — Lunch and networking break

14:10 — Compliant by design: Meeting security requirements across gaming jurisdictions

Lluis Mora, Head of Information Security and Technology Governance, bwin.party digital entertainment

- Tracking and communicating gaming regulations' security requirements
- Implementing effective gaming security controls
- Reducing the cost of compliance across multiple jurisdictions
- Using new market launches as a business advantage

14:30 — Ransomware and the risks for online gaming and gambling industry

Simon Edwards CISSP, Cyber Security Architect EMEA, Trend Micro

- Why ransomware has become the number 1 threat facing organisations in 2016
- Why ransomware is now targeting network shares, database clusters and backup servers
- Why email is still the number 1 attack vector and why most existing email gateways cannot detect 'unknown new malware'
- How using sandbox technology on the email gateway can identify advanced malware
- How threat intelligence can be actively shared between security devices to stop the spread of malware
- How to protect your organisation from the 'unknown, unknown' threats

14:50 — Online gaming towards cyber resilience

Dr. Grigorios Fragkos, Head of Offensive CyberSecurity, DeepRecce

- Today's challenges and requirements towards security online gaming
- How attacks are evolving, and what should we expect
- Taking steps for an effective cyber resilience strategy

15:10 — Education Seminars | Session 3

Pervade Software	RiskIQ
Evasive attacks – attack vectors that are invisible to SIEM systems **Jonathan Davies,** CTO, Pervade Software Ltd	Security in the age of social media **Jeff Lenton,** Solution Architect, RiskIQ EMEA, RiskIQ

15:50 — Refreshments and networking break

16:10 — What do you do when you have been hacked – the legal aspects of dealing with data breaches

Caroline Kean, Litigation Partner, Wiggin LLP

- Possible claims and sanctions resulting from a breach
- Factors likely to aggravate/mitigate any fines issued
- Storing data with third-party providers
- European Data Protection Regulation (2016/679)
- Brexit and the regulation

16:30 — In an ideal world: Ideal system security and steps to get there

Jon O'Keefe, Network and Security Engineer, Codemasters

- The ideal security system for small- and medium-sized gaming companies
- Experiences of key threats, restraints and solutions in building network security in the gaming industry
- The ideal system versus reality. And a few ideas on how to get closer to 'ideal security'

16:50 — Closing remarks

17:00 — Conference close

Education Seminars	
Comsec Consulting **New generation DDoS attacks – is the online gaming industry secured?** Presenter: Dan Gurfinkel, Head of Offensive Security & Response Unit, Comsec Consulting	What attendees will learn: • DDoS attacks trends • New generation attacks, DDoS solutions and technology and why you are not protected • Fighting DDoS • DDoS Case study
Osirium **Really useful security: Maintaining privileged access management in a multi-dependency environment** Presenter: Andy Harris, Engineering Director, Osirium	What attendees will learn: • What the attacker's kill chain looks like, where it can be blocked or disrupted • Techniques for dealing with multiple versions of management applications that can clash at the workstation • How to avoid sharing credentials for jump boxes and administrator/root accounts • How to speed up DevOps and SysAdmins whilst increasing security and removing the repetitive drudge work • How to speed up deployments of new versions and not worry so much about older legacy systems
Pervade Software **Evasive attacks – attack vectors that are invisible to SIEM systems** Presenter: Jonathan Davies, CTO, Pervade Software Ltd	There is a new generation of DoS attacks emerging out of the Tor Network that are proving to be completely invisible to Security Information and Event Management (SIEM) monitoring systems. These attacks have even slipped through Akamai and Cloudflare protection and a wide range of organisations have been hit including defence, government, TV and large enterprises, which is causing chaos in SOCs all over the world. Jonathan Davies, CTO of Pervade Software who have been recognised as one of 'The Most Innovative Cyber Security Companies in the UK' in a recent competition run by techUK & UK Govt's Department of Business innovation & Skills and sponsored by HP, Atkins and InfoSecurity Europe Magazine, provides a crucial insight into the anatomy of these new threats and how identifying them means bringing the SOC and NOC closer together. What attendees will learn: • Why expectations of SOC results do not match the reality of their capabilities • How SOCs are handicapped by having to deploy & manage multiple technologies • An example of an external attack that is invisible to SIEM systems – DoS • An example of an internal attack that is invisible to SIEM systems – WMI • Why bringing SOC and NOC together is critical for the next generation SOC

Education Seminars	
RiskIQ **Security in the age of social media** **Presenter:** Jeff Lenton, Solution Architect, RiskIQ EMEA	According to research published earlier this year by Demos (http://www.demos.co.uk/wp-content/uploads/2016/02/Gambling-Social-Media-Demos-and-RGT.pdf), over 900,000 people in the UK regularly engage with social media to discuss or interact with the gambling community and an additional 6 million people outside the UK regularly engage with these same social accounts. In the age of social media, the importance of having an advanced social media strategy is more critical than ever. In this session, we'll discuss the diverse attack methods hackers use on social media and give you the latest techniques to protect your organisation on the most popular social platforms. What attendees will learn: • The attack methods hackers use to exploit social media platforms and profiles • Which weaknesses cybercriminals look for so you can protect your company's social media reputation • How to strengthen your security approach to combat social media threats • The defence techniques an organisation must employ to prevent social phishing attacks, brand impersonation, recruiting scams, customer service impersonations, malware attempts, RDC, and more
TeleSign **Top security threats in online gaming and how to protect your user ecosystem** **Presenter:** Milorad Mitrović, EMEA Sales Engineer, TeleSign	By 2018, it is estimated that total international gaming revenue will reach a staggering $113.3 billion. The explosive growth of this industry – which includes massively multiplayer online role-playing games (MMORPG), free-to-play (FTP), and other online video and mobile-app based games – has made it a leading target for hackers. Gaming companies are exposed to great risk of end-user account compromise. Fraudsters are wreaking havoc on gaming communities by creating hundreds of fake accounts to perform a host of malicious activities. These activities lead to revenue loss, security distrust within the user base and brand damage. In this session, we will discuss why protecting gamers' identities and account access is now more critical than ever, the many types of fraud facing online gaming communities, and how to identify, challenge and block suspicious users while protecting a legitimate user base. What will attendees learn: • Fraudulent activity to watch out for (i.e. fake accounts, account takeover, social engineering, game bots, phishing and more) • Ways to protect user accounts and stop fraudulent accounts from being created • How to add incremental security such as automatic two-factor authentication to games to prevent fraud, while improving user experience, reducing friction and managing costs