

Post event report



3rd Annual Securing Online Gaming

3rd October 2017 | London, UK

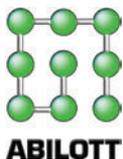
Strategic Sponsors



Education Seminar Sponsors



Networking Sponsors



Branding Sponsor



“ A really insightful day into the challenges facing the industry. Some really good speakers that shared some useful insights into how they are dealing with these challenges. 20 minute sessions are just right to keep the attention span and focus on the area. Again another superbly organised event that kept all to time and schedule. ”

Lead IT Auditor, Camelot Group

“ I thought the day was well run and the speakers very insightful. The presentation from Paddy Power Betfair was excellent and helped me to understand how major operators are now approaching cybersecurity. ”

Commercial Director, GBG Plc

“ Thanks very much for yesterday; it was an enjoyable and valuable day. I felt that the speakers were very good covering a wide range of important topics within security in our industry. GDPR of course is very topical, but the agenda also covered fraud, cyber threat management, compliance and cloud management. There were also relevant vendors available with solutions that can support information security professionals in the gaming industry. ”

Head of Governance, Risk and Compliance, Boylesports

Inside this report:

Sponsors

Key themes

Who attended?

Speakers

Agenda

Education Seminars



Speakers

- James Barrett,
Senior Director – EMEA
Endace
- Simon Brady,
Managing Editor
AKJ Associates
- Stephen Breen,
Head of Security Application
and Infrastructure
Paddy Power Betfair
- Richard Cassidy,
Consultant, Solutions
Architecture – EMEA
Synack
- Simon Crocker,
Director, Systems Engineering for
Western Region
Palo Alto Networks
- Sam De Silva,
Partner, CMS Cameron McKenna
Nabarro Olswang LLP
- Miles Dixon,
Senior VIP Manager
Betable
- Dermot Gannon,
Cyber & Threat Management Lead
Paddy Power Betfair
- Pascal Geenens,
EMEA Security Evangelist
Radware
- Richard Helliar,
eCommerce Sales Director EMEA
ThreatMetrix
- Matt Little,
CTO
ZoneFox
- Paul Norris (PJ),
Senior Systems Engineer
Tripwire
- Daniel O’Neill,
Payment & Risk Manager
Betable
- Alastair Parr,
EMEA Operations Director
InteliSecure
- Chris Sullivan,
Remote Investigations Manager
Gambling Commission
- Necla Vardal,
Information Security Manager
Smartgames Technologies

Key themes

- Defending against the core threats
- Compliance and regulation
- Optimise your incident response plan
- Secure application development
- Resilience: Maintaining availability despite attacks

Who attended?



Agenda	
08:00	Registration
08:50	Opening remarks
09:00	<p>Playing the compliance game: Balancing security and compliance in the gaming industry</p> <p>Necla Vardal, Information Security Manager, Smartgames Technologies</p> <ul style="list-style-type: none"> • Intersection area for compliance: UKGC regulation, ISO27001, PCI, DPA, GDPR • How to balance compliance and security • How to manage digitalisation • Compliance and regulatory advice for SMEs
09:20	<p>Battle of the IoT bots</p> <p>Pascal Geenens, EMEA Security Evangelist, Radware</p> <ul style="list-style-type: none"> • IoT – ‘S’ is for security <ul style="list-style-type: none"> – Common exploits by IoT malware • The battle of the bots: <ul style="list-style-type: none"> – Mirai, the Bad – Hajime, the Good (at least for now?!) – BrickerBot, the Vigilante • How to protect against the IoT threat • What to do when infected
09:40	<p>Network recording: Preparing for the worst</p> <p>James Barrett, Senior Director – EMEA, Endace</p> <ul style="list-style-type: none"> • How do you minimise brand damage when a breach occurs? • How do you ensure compliance with GDPR Article 25? • How can you maintain security on elastic gaming platforms?
10:00	<p>Operation gambling: Insights into cyber threat management in the gambling industry</p> <p>Stephen Breen, Head of Security Application and Infrastructure; and Dermot Gannon, Cyber & Threat Management Lead, Paddy Power Betfair</p> <ul style="list-style-type: none"> • Cyber and threat management in the gambling industry • Where software is being developed at such high technical levels and speed, how does one align threat management with product development and business efficiency? • Balancing security with business agility/resilience: How does security operations and infrastructure fit into this?
10:20	<p>Education Seminar Session 1</p> <p>Palo Alto Networks</p> <p>Don't forget to secure the cloud because clouds aren't made equal!</p> <p>Simon Crocker, Director, Systems Engineering for Western Region, Palo Alto Networks</p>
11:00	Refreshments and networking break
11:30	<p>So you want to be a DPO?</p> <p>Sam De Silva, Partner, CMS Cameron McKenna Nabarro Olswang LLP</p> <ul style="list-style-type: none"> • Practical advice to manage the oncoming regulatory changes. Managing sensitive customer data • DPO is one of the mandatory conditions for GDPR for certain companies. But what does that mean? What are the risks/responsibilities/accountabilities? • Working with the regulator: What are the legal implications?
11:50	<p>Data context in effective information security management</p> <p>Alastair Parr, EMEA Operations Director, IntelISecure</p> <p>Controls around sensitive data protection are under more scrutiny than ever and existing, perimeter-only programmes are no longer satisfactory. Data needs to be adequately protected from creation, through its transmission, storage and destruction. This session will highlight best practices for today's environment, including:</p> <ul style="list-style-type: none"> • Challenges with legacy security programmes • Data maturity assessments • Data-centric infosecurity programmes • Common data-centric pitfalls • Data profiling

Agenda	
12:10	<p>The currency of trust – how identifying trusted users can help increase business and eliminate fraud</p> <p>Richard Helliar, eCommerce Sales Director EMEA, ThreatMetrix</p> <ul style="list-style-type: none"> • Cybercrime threats in the gambling industry: Insights from the ThreatMetrix Digital Identity Network • Digital identity: Using associations between anonymised attributes across the network to build digital identities • Reducing friction: How to accelerate trusted users through the customer journey while still catching bad ones • Helping with compliance: Assessing trust and risk, allowing you to present evidence that responsible operator behaviour has been observed • Use cases and examples from ThreatMetrix: Dealing with key challenges such as self-exclusion, regulation and promotional abuse
12:30	<p>Education Seminar Session 2</p> <p>Tripwire</p> <p>Place your bets: How much would you bet on the security of your systems?</p> <p>Paul Norris (PJ), Senior Systems Engineer, Tripwire</p>
13:10	Lunch and networking
14:10	<p>VIP: Very Important Protection. How to analyse and protect client data and user analytics</p> <p>Miles Dixon, Senior VIP Manager, Betable</p> <ul style="list-style-type: none"> • What makes a VIP? How two potential VIP clients can look exactly the same when it comes to 'data', and how to differentiate • Customer data. How do you keep this data secure? • Why automation won't eat the gambling industry. How algorithms can detect anomalies in user analytics, but it takes experience and 'human instinct' to analyse these anomalies
14:30	<p>Fraud and threats</p> <p>Daniel O'Neill, Payment & Risk Manager, Betable</p> <ul style="list-style-type: none"> • Fresh perspectives from the gaming industry. Are there threats that are unique to the gaming industry? • Nuances of igaming. Digitalisation of the industry • Fraud, risk and payments • What does the arrival of AI/automation mean for fraud analytics and the gaming industry?
14:50	<p>Playing the insiders at their own game...</p> <p>Matt Little, CTO, ZoneFox</p> <ul style="list-style-type: none"> • What online gaming organisations should be thinking about when considering a machine Learning solution • Identify the connection between machine learning, behavioural analytics and why the 'human element' is essential in driving the accuracy and power of threat detection • Find out more about the threat investigation pipeline – from conception right through to presenting accurate real-time forensic reports
15:10	<p>Education Seminar Session 3</p> <p>Synack</p> <p>Securing gaming against hackers</p> <p>Richard Cassidy, Consultant, Solutions Architecture – EMEA, Synack</p>
15:50	Refreshments and networking break
16:10	<p>Lessons from the Gambling Commission</p> <p>Chris Sullivan, Remote Investigations Manager, Gambling Commission</p> <ul style="list-style-type: none"> • Perspectives from major UK regulator • Working with the Gambling Commission • Practical takeaways for regulatory changes: GDPR
16:30	<p>Small medium expertise, what SMEs in the gaming and gambling industries need to know</p> <p>Simon Brady, Managing Editor, AKJ Associates</p> <ul style="list-style-type: none"> • Cybersecurity for SMEs is impossible: What's the next big thing? • Industry collaboration is the only way to counter the hacker community • Fail and your stakeholders will increasingly abandon you
16:50	Conference close

Education Seminars	
<p>Palo Alto Networks</p> <p>Don't forget to secure the cloud because clouds aren't made equal!</p> <p>Simon Crocker, Director, Systems Engineering for Western Region, Palo Alto Networks</p>	<p>What attendees will learn:</p> <ul style="list-style-type: none"> • The advent of cloud adoption (IaaS, PaaS, SaaS): both sanctioned and unsanctioned applications are being accessed and utilised by organisations and their employees • The impending GDPR, which aims to ensure that personal data is protected, wherever it resides, and the security implications of these deployments and workloads. Clouds are not made equal, and organisations shouldn't make any assumptions when it comes to security. Your vendor may take care of securing the infrastructure, but what about the data? • Gaining visibility and control, reducing the attack surface and the preventing of both known and unknown threats in the cloud and how this will significantly help when it comes to compliance and the GDPR.
<p>Synack</p> <p>Securing gaming against hackers</p> <p>Richard Cassidy, Consultant, Solutions Architecture – EMEA, Synack</p>	<p>Inside the heart of every hacker is a gamer. Finding exploits combines the thrill of the chase with the exultation of the kill. So it's no surprise that the gaming industry is seeing increased attention from attackers, from slot machines to fish tanks.</p> <p>Traditional methods, such as scanning and penetration testing only go so far. They don't simulate offensive techniques the same way properly motivated and prepared hackers can. Modern attackers are persistent, data-driven, and relentless and face defenders that are usually understaffed due to a perpetual worldwide cybersecurity skill shortage.</p> <p>What attendees will learn:</p> <ul style="list-style-type: none"> • What's wrong with current best practices • What early results from crowdsourced penetration testing are showing • How to partner with hackers effectively and discreetly • A model for integrating DevOps and security into gaming software development
<p>Tripwire</p> <p>Place your bets: How much would you bet on the security of your systems?</p> <p>Paul Norris (PJ), Senior Systems Engineer, Tripwire</p>	<p>Security experts agree hardening your server and endpoint configurations can be the smartest security investments you can make. Why? Continually monitoring and hardening systems help keep your data safe, repel exploits, ensure regulatory compliance and provide measurable confidence in your security posture.</p> <p>Security experts also acknowledge that keeping your network devices hardened is hard to do. How do you get started? What capabilities do you need to look for in an effective solution?</p> <p>What attendees will learn:</p> <ul style="list-style-type: none"> • How to adopt and implement a security hardening policy that will effectively harden your systems against attacks, without breaking your budget • Understand true FIM and discover what else can be monitored beyond file systems plus learn about the common misconceptions of adopting a FIM solution • How to rapidly repair configuration drift so you can continuously comply with industry or government regulations and produce automated documentation that proves it