Post event report

Principal Sponsor

CyberKnight

Strategic Sponsors

BITSIGHT The Standard in SECURITY RATINGS
CEQUENCE SECURITY
DARKTRACE
ExtraHop
Green Method
Pulse Secure
SHAPE Part of F5
VECTRA Security that thinks
Education Seminar Sponsors
APPGATE
RISKIQ
shufa
Si
SIRP
Synack
Networking Sponsors
Arcon
BeyondTrust
BULWARK Technologies
COFENSE
corelight
emt TECHNOLOGY DISTRIBUTION
ipswitch
ManageEngine
mimecast
PGI
Securden
ThreatConnect
Branding Sponsors
Cyberinc
FIREEYE
FLASHPOINT
PhishRod
SECLORE
STEALTHbits TECHNOLOGIES
ZIMPERIUM MOBILE THREAT DEFENSE

“Overall it was an insightful event with access to a lot of information on current issues faced by the industry, both through the presentations and through the partners showcasing their products/technology.”

Senior Manager Internal Audit, Internal Audit Business, Majid Al Futtaim Properties LLC

“Congress was really helpful and I got a lot of perceptive related to different products. I like a few of the presentations and discussions which helps me to decide workaround for my IT security department. Security is always less concern domain in the companies and such events can highlight the issues to the stakeholders to take efforts correctly and measurably.”

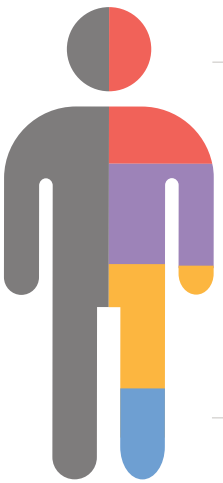
Sr Officer IT Security, Etisalat Group

Inside this report:

Key themes

- Dealing with nation-state actors and exploits
- Compliance with new regulations
- Adapting to the changing threatscape
- Slow train coming: the wait for intelligent cybersecurity
- One-stop shop security?
- Securing digital transformation

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

Ashraf Aboukass, Global Head of Information Security Architecture, Ops & Eng

Bilal Ahmad, Head – Information Security, Union Coop

Syed Abid Ali, Co-Founder & CCO, PhishRod

David Anumudu, Solutions Architect, Flashpoint

Gita Butzlaff, Head of Compliance & MLRO, Beehive P2P

Chris Cheyne, SOC Director and CTO, Si Consult

Christos Christou, Chief Compliance Officer, Lulu International Exchange

Owen Cole, VP Emerging Territories, EMEA, ExtraHop

James Connolly, Expert in application of AI, Darktrace

Ammar Enaya, Regional Director Middle East/Turkey, Vectra AI

Ismail Jani, Information Security and Compliance Manager, Engineering Office

Rizwan Khan, Head of Compliance, Al Dahab Exchange

Martin Leo, Head of Technology Business Controls, State Street Bank

Fabian Libeau, VP EMEA, RiskIQ

Nicola Lishak, Head of Information Assurance, Royal Mail Group

Mohamad Mahjoub, CISO, Veolia Middle East

Goher Mohammad, Head of Information Security, L&Q Group

Dr. Erdal Ozkaya, Head of Information Security, Standard Chartered Bank

Marco Pereira, Regional Head of Commercial Sales EMEA, BitSight

Ron Peeters, Managing Director EMEA, Synack

Matthew Platten, TFP Presales Manager EMEA, AppGate

Sumit Puri, Chief Technology Officer, Evercare Group

Rajiv Raghunarayan, Senior Vice President of Products and Marketing, Cyberinc

Faiz Shuja, CEO & Co-Founder, SIRP

Rohit Sinha, Cyber Security Specialist, Zimperium

Islam Soliman, Presales Manager Middle East, Pulse Secure

Ameya Talwalkar, Chief Product Officer, Cequence Security

Dan Woods, VP Shape Intelligence Center, Shape Security

Aizaz Zaidi, Head of Transformation and Operational Risk, Al Masraf Bank

Agenda

08:00 Registration and breakfast networking

08:50 Chairman's welcome

09:00 **Protecting data and achieving privacy: lessons from Royal Mail's GDPR journey**

Nicola Lishak, Head of Information Assurance, Royal Mail Group
- Data protection regulation: see it coming and why preparation is vital
- Engaging your stakeholders: whether the Board, the Business, or the Regulator, collaboration is key to achieving success
- Having a vision and mapping your journey: implementing the systems and controls to enable you to answer the big questions and demonstrate your path to compliance to your customers, shareholders and regulator(s)
- Achieving privacy in an online world: future-proof your privacy programme
- Practical takeaways from Royal Mail's GDPR journey: how regulation can help you to realise business benefits and achieve the buy-in you need

09:20 **Securing mobile workplaces**

Mohamad Mahjoub, CISO, Veolia Middle East
- Deploying secure yet easy to use collaborative tools
- Bringing agility to operations
- Redesigning the way of working
- Being cost effective, environmentally friendly, and secure

09:40 **How to succeed at threat hunting & IR: think differently about data**

Owen Cole, VP Emerging Territories, EMEA, ExtraHop
- How a data-first approach to security architectures can illuminate natural consolidation points
- How collaboration with other parts of the IT organisation can improve security posture and reduce tool sprawl
- How this collaborative approach also creates opportunity to improve security posture through smarter processes and practices

10:00 **APIs – the next frontier in cybercrime**

Ameya Talwalkar, Chief Product Officer, Cequence Security
- Explosive growth in API usage exposes organisations to significant cybersecurity risks
- Visibility – the first step in understanding and cataloguing the API security risk
- Exposure – what types of attacks are each of the APIs susceptible to
- Protection – which of the many API security products is best suited for your needs

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

RiskIQ	SIRP	Synack	Zimperium
Defending your organisation and your customers against JavaScript injection attacks **Fabian Libeau,** VP EMEA, RiskIQ	**Risk-based approach to security operations** **Faiz Shuja,** CEO & Co-Founder SIRP	**Next generation: offensive security testing** **Ron Peeters,** Managing Director EMEA, Synack	**Mobile devices are the 'new endpoint' today** **Rohit Sinha,** Cyber Security Specialist, Zimperium

11:00 Networking and refreshments

11:30 **'Will' vs. 'Skill': are we using the wrong tactics to recruit for our information security team?**

Goher Mohammad, Head of Information Security, L&Q Group
- There is a cybersecurity skills shortage that is still not shrinking; as hiring managers and leaders, we need to tackle the gap between demand and supply of cybersecurity professionals
- Traditional methods of hiring need challenging, how to adopt an agile and flexible approach
- Get yourself noticed! What are cybersecurity hiring managers looking for in a new recruit?
- Positive results: lessons learnt from L&Q Group on building and retaining talent within your security team

11:50 **Hacked! Security beyond the hype**

Rajiv Raghunarayan, Senior Vice President of Products and Marketing, Cyberinc
- The worldwide spending on information security products and services exceeds more than $100bn annually, growing at ~10%. Complexity is growing even faster. And breaches feel like a daily affair
- As we continue our digitalisation journey and as more 'things' start getting connected, securing businesses and individuals becomes increasingly paramount
- Drawing insights from past breaches, we will explore key learnings and our path forward in getting ahead of the attackers and the attacks
- This presentation will identify solutions that can transform security defences, making it nimbler and simpler

12:10 **The shifting front line of fraud**

Dan Woods, VP Shape Intelligence Center, Shape Security
- Attack evolution – navigate the attack-roadmap as it has progressed from the commodification of credential stuffing and ATO schemes to some of the most complex and cutting-edge examples of manual fraud and dark web marketplaces
- Countermeasure efficacy – discover how cybercriminals retool to easily circumvent traditional countermeasures such as WAFs, CAPTCHA, and even fraud tools – and what can be done to stop them
- Inverting friction – understand how organisations can protect their customers and brand without compromising user experience or collecting PII

Agenda

12:30 — **AI in security operations: what we have learnt so far…**

Ammar Enaya, Regional Director Middle East/Turkey, Vectra AI

Time and talent are key factors in preventing a data breach. Learn from peers how AI enabled them to:

- Detect hidden threats in cloud and enterprise networks
- Perform conclusive incident investigations
- Respond at previously unattainable speed and efficacy

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

AppGate	Flashpoint	PhishRod	Si Consult
Risk-based authentication: how to minimise user friction	**Secrets of illicit forums: actionable insights from cybercrime communities**	**Framework for automated phishing defence and orchestrated response**	**Building an effective operating centre SOC – the central nervous system of your security**
Matthew Platten, TFP Presales Manager EMEA, AppGate	**David Anumudu,** Solutions Architect, Flashpoint	**Syed Abid Ali,** Co-Founder & CCO, PhishRod	**Chris Cheyne,** SOC Director and CTO, Si Consult

13:30 — Lunch and networking

14:30 — **EXECUTIVE PANEL DISCUSSION** — **Digital transformation: delivering the best, securely**

Sumit Puri, Chief Technology Officer, Evercare Group
Bilal Ahmad, Head – Information Security, Union Coop
Ismail Jani, Information Security and Compliance Manager, Engineering Office
Aizaz Zaidi, Head of Transformation and Operational Risk, Al Masraf Bank

14:50 — **Attacks are moving at computer-speed – how will your teams respond fast enough?**

James Connolly, Expert in application of AI, Darktrace

- The rise of machine-speed and worm-able attacks
- Autonomous response: how cyber AI responds surgically to fast attacks across the entire digital infrastructure
- Using AI to ensure your network security works in tandem with your email security
- Real-world case studies where zero-days and insider threats were interrupted within seconds
- How to prepare for offensive AI attacks

15:10 — **How do you implement a 'zero trust' security policy throughout your organisation?**

Islam Soliman, Presales Manager Middle East, Pulse Secure

- How can you improve managing and governing user access?
- How to implement a single access policy to your data, regardless of where it is located, from wherever the person is accessing it from on whatever device
- How to achieve total user and endpoint visibility, and up-scaling device security
- How you can enable IoT identification in a secure way and set relevant profile

15:30 — **Cybersecurity – regulation, resiliency, risk**

Martin Leo, Head of Technology Business Controls, State Street Bank

- Regulatory landscape and change in the years
- How resiliency is becoming the dominant theme with regulator
- What role does risk (management) play in the midst of regulation and compliance?

15:50 — **Transforming cybersecurity risk management, monitoring & reporting**

Marco Pereira, Regional Head of Commercial Sales EMEA, BitSight

It is now much easier to determine what's important, dangerous and a real risk to your cybersecurity posture. Using a common framework leads to more effective conversations on risk with your security teams, board members, business partners, insurers and regulators.

Join the BitSight session to explore:

- Prioritisation, justification and validation of IT security investments to underpin business digital transformation
- Managing your security performance, and that of your subsidiaries, and third- and fourth-party suppliers in today's hyper-connected environment
- Monitoring and reporting on cyber-risk to non IT stakeholders

16:10 — Networking and refreshments

16:30 — **EXECUTIVE PANEL DISCUSSION** — **Compliance and risk mitigation in the changing regulatory landscape: financial services perspective**

Aizaz Zaidi, Head of Operational Risk and Transformation, Al Masraf Bank
Christos Christou, Chief Compliance Officer, Lulu International Exchange
Gita Butzlaff, Head of Compliance & MLRO, Beehive P2P
Rizwan Khan, Head of Compliance, Al Dahab Exchange

16:50 — **How to get the most out of your security investment**

Dr. Erdal Ozkaya, Head of Information Security, Standard Chartered Bank

- Ensuring your organisation's sensitive data remains secure within company walls goes far beyond simply buying and implementing a security solution
- Build a long-term plan for your security investment. The IT department should be aware of its role in the organisation and its importance for business continuity
- Threats come from every connected channel – do your tools cover all vulnerabilities?
- Responding to a security breach: plan, do, check, act

17:10 — **The new wave of AI/ML cyber-attacks**

Ashraf Aboukass, Global Head of Information Security Architecture, Ops & Eng

- What can emerging technologies such as artificial intelligence do to help security initiatives – and what new challenges do they introduce?
- Developing strategy and oversight of hyperconnectivity
- How are the cybercriminals using ML and AI techniques. What do information security leaders need to know to stay ahead of the game?

17:30 — Conference close

Education Seminars

AppGate

Risk-based authentication: how to minimise user friction

Matthew Platten, TFP Presales Manager EMEA, AppGate

Too much security kills security. We are all familiar with this concept, yet in today's escalating banking fraud environment, how can one master the challenge of customer retention along with the need for strong user authentication and stringent security procedures?

In this presentation, we will see how risk-based authentication provides necessary user authentication while lowering friction, by basing authentication requests on context, not a systematic approach. This can be determined by profiles factors such as origin, destination, time of day, velocity, IP, user platform and location, allowing expert systems to determine if risk-based authentication is needed.

This presentation will cover:

- RBA context
- User authentication acceptance
- Technology participating in RBA
- RBA chain of event
- Necessary steps for implementation

Flashpoint

Secrets of illicit forums: actionable insights from cybercrime communities

David Anumudu, Solutions Architect, Flashpoint

- Understanding of, and procedures that can be gleaned from online illicit communities
- What does risk intelligence actually mean?
- How do illicit communities operate?
- What can I learn from these about threat actor motivations, tactics and techniques?
- Is my organisation mature enough to gain value from intelligence products?

PhishRod

Framework for automated phishing defence and orchestrated response

Syed Abid Ali, Co-Founder & CCO, PhishRod

Traditional security controls such as IPS & email gateways are only effective to a certain level, that is why phishing remains the most potent threat vector to date. Once a phishing email lands into the mailbox, it only takes a click to trigger a cyber-attack. The longer the phishing email resides in the mailbox, the higher the probability of the threat propagation.

The IT Security teams receive too many incidents with little time to respond. Even after identification of phishing emails, the deletion from all end-user mailboxes remains a challenge largely due to involvement of different stakeholders.

In this session, you will learn

- How phishing attacks bypass the traditional email security layer
- Need for an orchestrated response that involve people, process and technology
- Framework for automated phishing defence & orchestrated response
- Using internal & external threat intelligence for phishing defence
- Defending against phishing threats through orchestrated response from reporting, investigation, quarantine to deletion
- Correlating phishing readiness, security awareness, policy compliance & actionable threat intelligence

RiskIQ

Defending your organisation and your customers against JavaScript injection attacks

Fabian Libeau, VP EMEA, RiskIQ

Browser-based attacks – web skimming, cryptocurrency miners, fingerprinters, and waterholing encounters – are responsible for some of the most high-profile breaches in recent history, such as the hacks of British Airways and Ticketmaster. Given the frequency by which RiskIQ researchers now encounter these attacks, we believe that they should be taken as seriously as threat mainstays such as phishing and ransomware. Browser-based attacks have one thing in common: malicious injects. These can be notoriously difficult to detect as their actions take place in the user's browser. The result is weeks or months of compromise on average.

In this session we'll break down the most common and interesting injection techniques RiskIQ researchers have observed in our telemetry. We'll also look at ways organisations can defend themselves against this growing class of attack.

- JavaScript injection attacks – what are they?
- A brief history
- The current landscape – attackers acting with impunity
- Steps to defend against JavaScript injection attacks
- How RiskIQ can help

Education Seminars	
Si Consult **Building an effective operating centre SOC – the central nervous system of your security** **Chris Cheyne,** SOC Director and CTO, Si Consult	Parallels between cybersecurity and the human body are nothing new. In fact, cybersecurity has often been referred to as the immune system, or skin, of an organisation. When you think that our skin is the initial layer that blocks harmful bacteria/pathogens from entering and attacking our delicate and important internal organs, you can draw similarities between the harmful bacteria and cybercriminals/bad actors trying to gain access to the precious organs, these being a parties inner systems, technology and people. But if we take this analogy further, you will observe key resemblances between how our human senses, namely how sight, hearing, touch and smell, mirror key components of a well-run SOC. 1. Learn how EDR tooling is the eyes of your operation centre; how event logs are your ears; how behaviour analytics guide your sense of smell. And how context acts as the touch that guides and propels your organisation forward. 2. In any living organism, the right balance of chemicals/water/light/food is crucial. Equally, within a well-run SOC the right balance of people, skills, technology and processes are fundamental. Find out how to get that balance right. 3. Most do not consider how reflex and automation affect cybersecurity. Learn how to successfully receive and react to data in rapid time, just as the human body reacts to and reflects oncoming threats. 4. We aren't all made of money. Obtain tips and tricks on how to get the best from your Security Operation Centre on a budget.
SIRP **Risk-based approach to security operations** **Faiz Shuja,** CEO & Co-Founder, SIRP	On average, every organisation has 25+ security controls generating a ton of alerts and vulnerabilities. On top of that, if the organisation is diligent enough, they'll be getting threat advisories from different external sources as well. Since it is not humanly possible to investigate and take action upon so much data coming in so fast, how can you prioritise your response? Presentation will cover: • Drawbacks and limitations of focussing on traditional bucket based (High, Medium, Low) severity approach • The fundamental gap between what technical guys are doing and what senior management understands • The requirements for effective risk-based security operations • How to use the Security Score to maximise efficiency and focus your limited resources on the threats that matter the most
Synack **Next generation: offensive security testing** **Ron Peeters,** Managing Director EMEA, Synack	Malicious hackers and state-sponsored cyber-attacks CAN easily breach any of your mission critical web and mobile applications and networks. Vulnerability scanners and traditional pen testing are not good enough to find many of these exploitable vulnerabilities in your live systems. In this session you'll learn: • About a next generation security testing platform incorporating advanced, offensive and adversarial security testing with artificial Intelligence • How one of the world's most elite hacking teams with 1200+ international top-class security researchers can be virtually deployed with short notice • Of a number of use cases and POCs performed at customers in the UAE and Saudi Arabia

Education Seminars	
Zimperium **Mobile devices are the 'new endpoint' today** **Rohit Sinha,** Cyber Security Specialist, Zimperium	Traditionally, endpoints (laptops, desktops) have always been the weakest link and an easy target for attackers. Ensuring that these endpoints in their organisation are secure has been the most dispersed and difficult security challenge for CISOs and their security teams. And just as security professionals solved that problem, a 'new endpoint' arrived vulnerable to some threats that were similar, but others that were entirely new, different and which exponentially increased organisational risk. Today, mobile devices are used for all your corporate needs: financial and digital commerce, social engineering, information and entertainment. There is very little one can think of that smartphones cannot now do. In addition, with the advent of mobile devices, the way we accessed applications also changed completely. Applications, which earlier were web-based and accessible over a browser, are all now available as apps – always and anywhere available on your smartphone. Even through mobile devices and apps have become such an integral part of our professional and personal life, there is little in the way of in-built security to eliminate their vulnerability to advanced cyber-attacks. In this session: • You will learn: about the various attack vectors applicable for mobile devices and how vulnerable our smartphones are • You will see: a live demonstration of a targeted attack compromising the entire device and the apps on it • You will experience: the impact of this compromise on your corporate data, personal data and your corporate/consumer business apps