Post event report

Strategic Sponsors

DARKTRACE · exabeam · InteliSecure · NTT Security · PHISHME · thycotic · ZoneFox

Education Seminar Sponsors

Carbon Black. · CROWDSTRIKE · Cynet (Advanced Threat Detection & Response) · EASYSOLUTIONS (A CYXTERA BUSINESS) · egress · eset (ENJOY SAFER TECHNOLOGY) · GUIDANCE SOFTWARE is now opentext · logpoint · mimecast · NYOTRON (SECURING THE WORLD) · paloalto NETWORKS · portnox · THALES · tripwire · VERISIGN

Networking Sponsors

ANOMALI · F-Secure · Post-Quantum · Threatscape (SECURING THE DIGITAL LANDSCAPE) · VECTRA (Security that thinks) · XQ CYBER

“My key takeaway from the day was that many organisations are still struggling to get the message through to their top management about security risks in ways that top management and boards can understand. i.e. how can we as IT professionals describe the risks and quantify in terms that top management and boards can make balanced security investment decisions?”

Director, IT Infrastructure & Service Management, Poyry

“This event was great for networking with suppliers and peers focusing on the same issues and concerns and insightful to future trends and developments.”

Senior Techincal Services Development manager, Vue Cinema

“The event lived up to its reputation – being clear, concise with thought provoking insight to topical issues with no waffle and an opportunity to network with likeminded peers. Needless to say, speakers were outstanding, knowledgeable and overall was well organised. The e-Crime & Cybersecurity Congress has become a regular not to be missed event in my diary.”

Internal Audit Manager, ARM Holding

“As usual, the presentation and the topics covered in the e-Crime & Cybersecurity Mid-Year Summit were very good. In addition, I find that the event provides an excellent opportunity for networking and sharing information with peers. I wish to express my thanks to you and AKJ for organising and hosting such great event.”

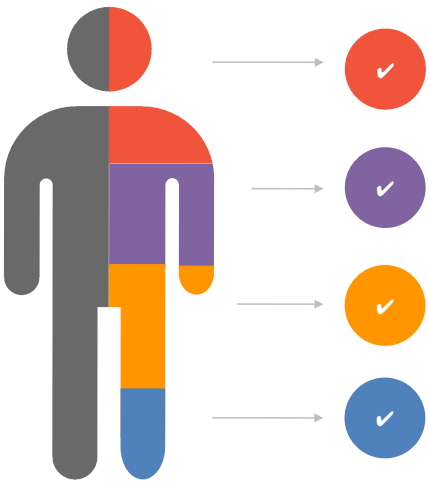
IT Security & Risk Officer, UBS

Inside this report:

Key themes

- Reporting structures of successful security teams
- Regulatory update: What do you need to know?
- Optimising enterprise architectures
- Beating ransomware: It can be done
- Closing the door on email-delivered malware
- Intelligent IDAM: Driving business value
- Cognitive analytics: Making ground against the enemy

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

Ofer Amitai, CEO, Portnox

Dan Bridges, Technical Director EMEA Channels, Exabeam

Tim Carolan, Sales Engineer, Thycotic

Jan Coulson, Presales Lead UK, Nyotron

Gill Fenney, Senior Information Security Consultant, ASDA

Andy Deacon, Security Consultant, LogPoint UK & Ireland

Anthony DiBello, Senior Director of Products, Guidance Software/OpenText

Jamie Graves, Founder and CEO, ZoneFox

Ian Greenwood, Regional Sales Manager, UK&I, Thales eSecurity

Caroline Howard, Account Manager, Egress Software Technologies

Mark James, IT Security Specialist, ESET UK

David Janson, VP Sales, UK & Europe, PhishMe

Sebastian Kinnaird, Director of Cyber Security, Willis Towers Watson

Michael Kolotov, Sales Engineer, Cynet

Amit Lakhani, Head of Information Security, Hermes Investment Management

Michael Lazer, Head of Security (E-Commerce), Office Depot

James Martin, Senior Cyber Security Manager, Darktrace

David McKissick, Senior Systems Engineer, Tripwire

Naqui Mirza, Enterprise Account Manager, Mimecast

Elisabetta Osta, Head of CSO Analytics, CSO, Barclays

Kevin Piper, Senior Product Manager, Verisign

Mike Pitman, BISO, John Lewis

Matthew Platten, Anti-Fraud Solutions Consultant, Easy Solutions

Helen Rabe, Head of Cyber Defence EMEA, CBRE

Deepak Rajgor, Systems Engineer WEUR, Palo Alto Networks

Stuart Reed, Senior Director – Market Strategy, NTT Security

Claire Rushton, Senior Director – Crimes Against the Business, Walmart

Mandeep Sandhu, EMEA Cyber Security Strategist, Carbon Black

Ian Snelling, Infrastructure/Cyber Resilience Manager, Pentland Brands

John Titmus, Director, EMEA, CrowdStrike

Dane Warren, Global CISO, Intertek

Ben Wheeler, Country Manager, UK, Nyotron

Jeremy Wittkop, Chief Technology Officer, InteliSecure

Agenda

08:00 Registration

08:50 Opening remarks

09:00 **The digital revolution: Cybercrime and cyber solutions**

Elisabetta Osta, Head of CSO Analytics, CSO, Barclays

- Digital revolution has brought lots of opportunities ... and opened the door to cybercrime
- The profound impact of cybercrime on the business
- Lots can be done: Collaboration, changing the culture in the ecosystem, measuring success

09:20 **Effectively integrate the human element into your security posture**

Jamie Graves, Founder and CEO, ZoneFox

- 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
- Discover what the new GDPR legislation will mean for organisations, and gain an understanding of how machine learning can support businesses to meet new regulation

09:40 **A new age of behavioural analytics**

Dan Bridges, Technical Director EMEA Channels, Exabeam

- Can Artificial Intelligence match the expertise of the Security Analyst?
- User behaviours – the difference between too much data and the right data
- Pinpointing the real attacker and reducing false positives
- Automating incident investigation and response to increase productivity and minimise human errors

10:00 **Case studies on cybercrime**

Claire Rushton, Senior Director – Crimes Against the Business, Walmart

- Structure of crimes against the business: Walmart. How to investigate a breach
- Case study: Social engineering and dot.com sites
- Case study: EMV and chip authorisation

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

CrowdStrike	Cynet	Easy Solutions	Guidance/OpenText	Portnox	Verisign
Hacking exposed: Regional trends, predictions and real-world tradecraft **John Titmus,** Director, EMEA, CrowdStrike	**The evolution of cybercrime – what's next** **Michael Kolotov,** Sales Engineer, Cynet	**Authentication Simple as a Selfie: How biometrics are reducing customer friction and improving security** **Matthew Platten,** Anti-Fraud Solutions Consultant, Easy Solutions	**Insider? Hacker? Accident? How forensic security reveals all** **Anthony DiBello,** Senior Director of Products, Guidance Software/ OpenText	**IoT and DDoS: Partners in crime** **Ofer Amitai,** CEO, Portnox	**Using DNS to help combat the threat of malware** **Kevin Piper,** Senior Product Manager, Verisign

11:00 Networking and refreshments

11:30 **There is no such thing as cyber risk – bringing cyber risk to the boardroom**

Dane Warren, Global CISO, Intertek

- Starting a greenfield strategy for cybersecurity
- Building organisational momentum for successful delivery
- Aligning cyber risk with business risk, and driving a business led cybersecurity programme

11:50 **Cybersecurity: The key to unlocking the value of digital transformation projects**

Stuart Reed, Senior Director – Market Strategy, NTT Security

- What is driving digital transformation and how does cybersecurity play a role in its success?
- Making the business case for resilient cybersecurity as a core component of value for your digital project
- Do organisations' implementation deadlines allow for integrated cybersecurity?

12:10 **A new era of cyber threats: The shift to self-learning, self-defending networks**

James Martin, Senior Cyber Security Manager, Darktrace

- The new age of silent, stealthy attacks that lie low in networks for weeks and months
- Why legacy approaches, like rules and signatures, are proving inadequate on their own
- How new 'immune system' technologies based on advanced mathematics and machine learning are being deployed today
- Real-world examples of subtle, unknown threats that routinely bypass traditional controls

12:30 **Protecting and securing privileged accounts and passwords as the security perimeter evolves**

Tim Carolan, Sales Engineer, Thycotic

- Privileged accounts and what threats do they pose?
- How to protect and secure privileged accounts
- Key hacker takeaways

Agenda

12:50 Education Seminar | Session 2

Egress Software Technologies	ESET	LogPoint	Mimecast	Palo Alo Networks	Tripwire
Time to face up to reality – the biggest data security risk to your business isn't a hacker, it's your staff!	**Hidden information within easy reach – threat intelligence**	**It's your data – do something useful with it**	**Facing the cybercrime threat with cyber resilience**	**Implementing a comprehensive cybersecurity strategy to address modern threats**	**How to better protect your organisation against high-profile breaches with foundational security controls**
Caroline Howard, Account Manager, Egress Software Technologies	**Mark James,** IT Security Specialist, ESET UK	**Andy Deacon,** Security Consultant, LogPoint UK & Ireland	**Naqui Mirza,** Enterprise Account Manager, Mimecast	**Deepak Rajgor,** Systems Engineer WEUR, Palo Alto Networks	**David McKissick,** Senior Systems Engineer, Tripwire

13:30 Lunch and networking

14:30 The 'B' stands for business: The true business risk and value of cybersecurity

Mike Pitman, BISO, John Lewis

- Cyber-metrics and how the information is measured at John Lewis
- How do you justify 'ROI' on information and cybersecurity?
- Communicating the business risk to the board

14:50 Protecting critical data assets in the cloud

Jeremy Wittkop, Chief Technology Officer, InteliSecure

- How organisations can safely store and process critical information assets in the cloud
- Understanding options for CASB implementations
- The impact of cloud-based DLP solutions on security programmes
- How encryption factors into a holistic cloud security solution

15:10 The 2017 phishing threat landscape

David Janson, VP Sales, UK & Europe, PhishMe

- High-profile leaks and mature malware tools in phishing emails and how this has led to the resurgence and emergence of ransomware and botnet malware.
- What is meant by the 'phishing threat landscape', how attackers have evolved this and the risks that poses to the enterprise
- What your enterprise can do in the face of all this, and goals for a holistic, comprehensive and agile defence

15:30 Education Seminar | Session 3

Carbon Black	Cynet	Nyotron	Thales eSecurity
Are you flying blind? The power of complete visibility with endpoint threat detection and response (ETDR)	**The evolution of cybercrime – what's next**	**Threat-agnostic defence – a new security paradigm**	**GDPR – regulation, myths and encryption**
Mandeep Sandhu, EMEA Cyber Security Strategist, Carbon Black	**Michael Kolotov,** Sales Engineer, Cynet	**Ben Wheeler,** Country Manager, UK, Nyotron; and **Jan Coulson,** Presales Lead UK, Nyotron	**Ian Greenwood,** Regional Sales Manager, UK&I, Thales eSecurity

16:10 Networking and refreshments

16:30 EXECUTIVE PANEL DISCUSSION — So, do you really need a CISO?

Sebastian Kinnaird, Director of Cyber Security, Willis Towers Watson

Amit Lakhani, Head of Information Security, Hermes Investment Management

Michael Lazer, Head of Security (E-Commerce), Office Depot

Gill Fenney, Senior Information Security Consultant, ASDA

Helen Rabe, Head of Cyber Defence EMEA, CBRE

16:50 Sponsor presentation

Please see details on handout

17:10 Taking steps towards cyber-maturity: How to get the board's attention. And what to do with it

Ian Snelling, Infrastructure/Cyber Resilience Manager, Pentland Brands

- Managing the relationship with the board. Why they are not asking the right questions
- A true understanding of the business value of cyber: What do you perceive to be the biggest risks?
- How to align business efficiency and security

17:30 Drinks reception and networking

18:30 Conference close

Education Seminars	
Carbon Black **Are you flying blind? The power of complete visibility with endpoint threat detection and response (ETDR)** **Mandeep Sandhu,** EMEA Cyber Security Strategist, Carbon Black	Many organisations are flying blind, with no idea of what is going on in their environment and with no visibility of the activity – and thus the threats and attacks – on their endpoints. A sophisticated endpoint threat detection and response (ETDR) approach can empower you to move beyond reactive tactics such as re-imaging devices, to a more proactive incident response and threat hunting model. By continuously recording and centralising all activity on the endpoint, you can get the complete, real-time data needed to continuously monitor, hunt, detect and isolate threats before they propagate. What attendees will learn: • The power of ETDR • How you can move to a model of pro-actively threat hunting • How visibility on the endpoint can enable you to address wider business issues such as compliance and user behaviour analytics
CrowdStrike **Hacking exposed: Regional trends, predictions and real-world tradecraft** **John Titmus,** Director, EMEA, CrowdStrike	Nation-state hacking continues to dominate the media. These attacks are the most challenging that any organisation can face because a nation-state actor can invest a significant amount of R&D to target an organisation and isn't driven by a profit motive. Yet techniques adopted by these actors invariably find their way into the mainstream criminal world and are a leading indicator of what organisations should prepare for. Using real-world examples to illustrate the extraordinary tradecraft that is routinely employed to steal state secrets, gain access to critical infrastructure or poach valuable intellectual property, we will expose how the UK threat landscape has changed in recent months. Hosted by the company that uncovered the highest profile attack in 2016, don't miss this opportunity to hear the latest threat intelligence and discuss with your peers how best to respond. What you will see: Witness new attack techniques that have been uncovered by CrowdStrike's threat hunting and incident response teams including: initial attack vectors, persistence, lateral movement and data exfiltration techniques. See new techniques for dealing with malware, ransomware, spearphishing, exploits and malware-free intrusions and leave knowing how to identify and stop advanced threat activity in your environment. What attendees will learn: • How nation-state threats are crafted and how their Tactics, Techniques, and Procedures (TTPs) help identify them from more routine advanced attacks • Who are the most notable adversaries in 2017 and the key security themes based on the latest intelligence compiled across CrowdStrike's global intelligence gathering operation • What are the indicators of attack and how you can apply them to defeat the adversary?
Cynet **The evolution of cybercrime – what's next** **Michael Kolotov,** Sales Engineer, Cynet	In order to understand the future, we must understand the past. Since the introduction of cybercrime, attackers have been evolving their methods to avoid detection, spawning new threats that leave nothing off-limits. Cybercrime has reached new heights and understanding its evolution is integral to protecting the organisation. What attendees will learn: • The present-day landscape of cybercrime • The evolution of cybercrime • Cybercrime – what's next • Case study: Review of an attack on a large government organisation

Education Seminars	
Easy Solutions **Authentication Simple as a Selfie: How biometrics are reducing customer friction and improving security** **Matthew Platten,** Anti-Fraud Solutions Consultant, Easy Solutions	Biometric authentication adoption is booming because it helps balance security and convenience by reducing customer friction. Our fingerprints, voice, face and more can all be used to validate our identity online. But where do biometrics fit in an authentication framework and how can these factors best be deployed? What attendees will learn: • New biometric options and how they reduce customer friction • Channels other than mobile to consider when launching biometrics • The need to integrate biometrics with legacy authentication systems • Why biometrics need to be part of an authentication framework in a layered fraud protection strategy
Egress Software Technologies **Time to face up to reality – the biggest data security risk to your business isn't a hacker, it's your staff!** **Caroline Howard,** Account Manager, Egress Software Technologies	All too often a business will focus its cybersecurity strategy on the protection of its corporate network, its staff and its customer data from sophisticated external threats. They are right to worry, the threats come in many forms, from socially engineered malware to password phishing attacks and the consequences of a breach can be grave. Yet this preoccupation with an 'unknown' external threat can distract from the biggest data security risk in any business today – its staff! As Gartner reports, the 'insider threat' now contributes to approximately 50% of all data breaches globally. These can be malicious to intentional, but just as often they are simply the result of human error. In this session, Egress will explore the role technology needs to play in engaging with and supporting users in a business to protect them and the data they manage and share. What attendees will learn: • A simple three-step approach to tackling the insider threat • How organisations can prevent the 'accidental' (fat finger) email send • That it is time to dispel the myth of 'Man vs Machine' and replace it with 'Man and Machine' if they are to effectively prevent future data breaches
ESET **Hidden information within easy reach – threat intelligence** **Mark James,** IT Security Specialist, ESET UK	Detailed knowledge of security threats provides companies with valuable insights about the present-day risks they are exposed to. By knowing more about these security risks, it makes it possible to actively prevent potential damages, comply to legal requirements, or at least to implement the necessary measures to mitigate them. The Intelligence Reports help in recognising the security threats and provide information about malware and its configurations, which is actually used or would be utilised in attacks against specific organisations or their customers (e.g., targeted threats). At the presentation you will hear more about the intelligence and information on targeted malware within your reach. What attendees will learn: • The kind of threat intelligence information that organisations can access • How this information can be analysed • How these insights can help to secure your organisation

Education Seminars	
Guidance Software/ OpenText **Insider? Hacker? Accident? How forensic security reveals all** **Anthony DiBello,** Senior Director of Products, Guidance Software/ OpenText	Insider threats account for more than 60% of intrusions, making them a top challenge for today's busy infosec teams. Whether it's from vindictive acts, carelessness or a simple mishap, the result is the same… you've got a problem that needs to be rectified ASAP. But finding, prioritising and acting on the multitude of potential risks your organisation faces every day is not easy. With so many alerts coming in, it is critical you find a way to waste less time chasing the unimportant and focus on what matters. This is where forensic security can help – by gaining visibility into all the points on your network you can better understand where the sensitive data is housed, identify the source of critical breaches and stop the damage before it starts. What attendees will learn: • How to find hidden risks lurking beneath the surface that can be the most dangerous to your organisation • How understanding where your data is helps you comply with new regulations • Methods for uncovering forensic residue across every stage of the attack lifecycle so you can get to the heart of the issue and solve it faster
LogPoint **It's your data – do something useful with it** **Andy Deacon,** Security Consultant, LogPoint UK & Ireland	Referencing the latest developments in security technology, Andy will explain how to use intelligence analytics in ways you probably never even considered possible. This session will be an informative and light-hearted look at what data you already have in your organisation and how best to use it to get some positive benefits. What attendees will learn: • Innovative ways to use the data you have to actually enhance your security position • How data analytics can deliver tangible ROI to your organisation
Mimecast **Facing the cybercrime threat with cyber resilience** **Naqui Mirza,** Enterprise Account Manager, Mimecast	Navigating a turbulent cybersecurity climate can be hard – especially as threats like Petya and WannaCry continue to cripple organisations. Business disruption, downtime, technical failure and data loss are all real risk factors that can't be ignored. The power of preparedness is in your hands. It's time to start thinking holistically about safeguarding against email-borne threats and mitigating risk – it's time to implement a cyber resilience strategy.' What attendees will learn: • Assessing the impact of disruption, downtime and technical failure • Mitigating risk with a cyber-resilience strategy • Preparing with Mimecast
Nyotron **Threat-agnostic defence – a new security paradigm** **Ben Wheeler,** Country Manager, UK, Nyotron; and **Jan Coulson**, Presales Lead UK, Nyotron	What does every cyber attack since Stuxnet have in common? Regardless of the method of the attack, the attacker bypassed the multiple layers of security technologies, penetrated the network and wreaked havoc to the organisation. Once inside, the intention of the hacker is always to steal, delete, manipulate, encrypt or exfiltrate data. Threat-agnostic defence turns the security paradigm upside down. Instead of worrying about stopping intruders from getting into your network, the focus is on stopping the damage that the attacker intends to inflict upon your data. This new security approach doesn't care what kind of threat is trying to get in. It doesn't care about the method or technique of the attack. It doesn't even care if the threat is already inside your network. It simply stops the damage that hackers intend to cause. What attendees will learn: • A fundamentally differentiated approach to protecting against cyber attacks • Protecting against the unknown unknown possible for the first time • A compensating control that will simply not allow damage to data

Education Seminars

Palo Alto Networks

Implementing a comprehensive cybersecurity strategy to address modern threats

Deepak Rajgor, Systems Engineer WEUR, Palo Alto Networks

The cloud (SaaS, IaaS, PaaS) is enabling an unprecedented wave of innovation that not only help reduce costs, but also enable increased collaboration, productivity and customer experience. Consequently, existing and emerging threats have become more sophisticated and challenging to prevent.

IT and Security teams have historically been overwhelmed by reactive alerts from a variety of disparate security products, a problem that will continue to increase as yet more point products are deployed to resolve developing point problems. Such complexity only serves to weaken the overall security posture due to yet higher volumes of alerts from unintegrated systems that lack the ability to automatically prevent these threats as they emerge

With the EU GDPR and NIS Directive coming into effect in May 2018, added pressure is being put on organisations to adopt 'state of the art' cybersecurity to ensure adherence.

What attendees will learn:

- How antiquated 'defence in depth' thinking has actually reduced security levels and given way to a modern, automated and more effective platform approach that secures the cloud, the network and the endpoint
- How to meet legislative obligations and prevent successful breaches by cybercriminals and other adversaries
- How to implement an integrated platform approach that reduces the attack surface and automatically reprograms the environment in a proactive fashion

Portnox

IoT and DDoS: Partners in crime

Ofer Amitai, CEO, Portnox

The Internet of Things (IoT) is one of the hottest technologies on the market, yet there is growing concern around the security risks that these connected devices present. While they are helping businesses of all sizes increase efficiency by mining data on processes and operations, a lack of regulation requiring security standards puts the businesses that choose to implement this technology at imminent risk.

One of the greatest risks that IoT presents is the ability to be hacked and used as botnets for carrying out Distributed Denial of Service (DDoS) attacks. 'Thingbots', or a collection of IoT devices hacked and used to carry out a DDoS attack, present a real risk to enterprises that depend on IoT technology for their daily operations. There are a number of examples – the most famous being the Mirai botnet – but the real concern here is that neither governments nor device manufacturers are taking responsibility to ensure that IoT cannot be used for malicious activities.

This session will examine some of the underlying risks inherent in the deployment of IoT technology in enterprise, as well as highlighting some lesser-known examples of thingbot attacks carried out across the globe in recent years. Finally, the presenter will suggest a number of steps that can be taken to secure networks from potential thingbot breaches, as well as who is responsible for ensuring that IoT devices are secure enough for the enterprise environment.

What attendees will learn:

- What are the benefits of IoT in enterprise, i.e. why so many businesses are deploying them
- What are the security risks inherent in IoT
- How IoT can be used as botnets in DDoS attacks
- Steps for securing IoT in enterprise
- Who is responsible for IoT security and preventing their use as a gateway for malicious activity

Education Seminars	
Thales eSecurity **GDPR – regulation, myths and encryption** **Ian Greenwood,** Regional Sales Manager, UK&I, Thales eSecurity	The GDPR comes into force on 25th May 2018. A maelstrom of information is available from a variety of sources, explaining the Regulation and its many facets. But how do you sort the real news from the fake news? Some of the available information on GDPR from certain sources is, to put it kindly, somewhat inaccurate. What attendees will learn: • What the Regulation does and does not say • What's new in terms of data protection and GDPR and what is not • An exploration to explode some myths and counter some of the #gdprubbish • Review of some specific areas of GDPR where Thales might be able to help as part of an overall approach
Tripwire **How to better protect your organisation against high-profile breaches with foundational security controls** **David McKissick,** Senior Systems Engineer, Tripwire	Cybersecurity is a chaotic and complex field. From new threats to evolving compliance requirements, cyber defenders must navigate countless options to get the job done. For its complexity, however, many of the essentials have remained remarkably consistent. Yet organisations struggle to effectively implement these essentials, and are often distracted or unable to overcome internal hurdles. The first task of a cybersecurity leader is to sift through an ever-increasing amount of things to know, do and deliver, in order to focus on the things that matter most. What attendees will learn: • Ways to manage this complexity, drawing on real-life examples • Best practices in implementing foundational controls effectively • How security at scale can help to reduce cyber risk in a complex environment • How critical controls can support with key compliance requirements such as the upcoming GDPR
Verisign **Using DNS to help combat the threat of malware** **Kevin Piper,** Senior Product Manager, Verisign	Malware can be a nightmare for network security teams. Infection resulting in encryption, deletion or even exfiltration of data or sensitive content can be devastating for companies – effectively halting productivity and sending network security teams scrambling to fix the vulnerability and clean their systems. Join and learn how DNS can be used to block certain malware and other malicious content. What attendees will learn: • Overview of the growing malware issues organisations face and how they relate to DNS • DNS resolution process • Discussion of DNSSEC, recursive DNS and DNS filtering • Overview of Verisign DNS Firewall (including live demo)