

## MESSAGE FROM THE UK CHAPTER PRESIDENT



Dear Members,

Advanced Persistent Threats is the topic for our next meeting on June 9th, kindly hosted by PWC (please note new venue and see <http://londonjune9.eventbrite.com/> for more details)

The following month (July 14th) we have our annual security event on the River Thames, this time a CISO's Den where we get to hear from vendors, 10 minutes apiece, as to new technology and services that will make a world of difference to our information security lives! An expert judging panel will be on hand to deliver the final verdict and award prizes to the best product and best presenter.

We are also hosting an educational workshop in Bristol on June 16th - Security on the Brain - Using Human Psychology to Achieve Compliance, where delegates will find out how to mould the elusive human brain to compliment one's security efforts.

Registration details for all events appear below.

You should have received an email from ISSA on June 1st, entitled "ISSA International Election Polls Now Open". Our very own Geoff Harris is standing so please do take a keen interest.

On a final note, a thank you to IO Active for helping fund the drinks at our Infosec 2011 networking evening in April - your assistance was much appreciated.

With very best wishes,

Tim Holman  
ISSA-UK President



## IN THIS MONTH'S ISSUE

### 1. UK CHAPTER MEETINGS IN 2011:

Our next Chapter Meeting will be in March and our scheduled dates for 2011 are as follows. Please do place in your diaries and look out for further information.

Chapter Meeting	9th June, 2011
Security on the Brain - Using Human Psychology to Achieve Compliance, Bristol Workshop	16th June, 2011
Security Innovations - CISO's Den HMS President (River Thames)	14th July, 2011
Chapter Meeting	8th September, 2011
Glasgow Regional Meeting	1st November, 2011
Chapter Meeting	8th December, 2011

You may register these in advance and add them to your calendar via the following link:  
<http://www.eventbrite.com/org/379120395?s=3292759>

### 2. SPEAK!

We welcome presentations from our members at our events and in particular are looking to fill a speaking slot on July 14th (our CISO's Den event). Is there a particular challenge you have faced over past years and how did you solve it? Contact [administration@issa-uk.org](mailto:administration@issa-uk.org)

### 3. GET PUBLISHED

We welcome <800 word submissions from our members on a topical theme or emerging threat related to our profession. We will look to publish these in the monthly newsletter



and website and ask that articles are kept independent with no sales plugs or vendor promotion. Please email [administration@issa-uk.org](mailto:administration@issa-uk.org)

#### 4. PARTNER NEWS

##### **This month, try Qualys Free Services:**

###### **BrowserCheck**

Test to See if Your Browser is Secure

<http://browsercheck.qualys.com>

###### **Malware Detection**

Scan Your Web Site for Malware Infections & Threats

<http://www.qualys.com/stopmalware>

###### **SSL Server Audit**

Audit Your SSL Web Site Implementation

<http://www.qualys.com/ssllabs>

##### **LogRhythm Webinar - PCI 2.0 Compliance - Are you ready for an Audit?**

If you are subject to PCI DSS compliance, we would like to invite you to a complimentary webinar titled "PCI 2.0 Compliance - Are you ready for an Audit?" on 14 June 2011 at 4:00 PM GMT.

The 45 minute webinar features PCI experts from Coalfire Systems, an independent IT audit and compliance firm, who will present a PCI Audit Checklist to help you prepare for an audit.

To view the details and to register, click on the link below.

<https://www1.gotomeeting.com/register/533504585>

##### **Palo Alto**

The Palo Alto Networks' Application Usage and Risk Report summarizes application traffic assessments performed between October 2010 and May 2011 on more than 1,253 networks worldwide. With a sample size of 1,253 participating organizations, a number that is nearly double that of the previous report, and a view into more than 28 exabytes worth of data, the latest edition of the Application Usage and Risk Report (May 2011) is, arguably, the largest application analysis of its kind.

<http://www.paloaltonetworks.com/literature/forms/aur-report.php>

##### **Qosmos**

Qosmos CEO Thibaut Bechetoille explains the value of communications metadata to build an intelligent Second Line of Cyber Defense:

Tasked with protecting highly sensitive data assets, government cyber security teams must defend against a growing mix of known and unknown threats on a daily basis.

Budget pressures force governments to increasingly rely on Commercial Off-The-Shelf (COTS) products to ensure cyber security. While these solutions (firewalls, anti-virus, etc.) are necessary, experience shows that they are not enough for comprehensive protection of government networks.

In most cases, the role of COTS is to ensure a first line of cyber defense and filter out known threats, which allows a government's uniquely qualified cyber security specialists to focus on the abnormal and potentially most serious threats with custom solutions for situational awareness, confidentiality, and rapid mitigation of advanced threats.

Behind COTS products used to filter out known threats, software that facilitates the extraction and decoding of communication metadata provide unique capabilities for building a Second Line of Defense to rapidly detect and mitigate the more advanced threats of zero-day attacks and weaponized malware, such as the Operation Aurora Trojan and Stuxnet-class malware.



Communication metadata describe information extracted or computed from network data flows for more accurate protocol decoding and deep, real-time visibility into applications traffic. Technology that leverages metadata goes beyond Deep Packet Inspection (DPI) and treats the network as a real-time, dynamic database, from which information can be fed to cyber security solutions. Traffic information can be extracted at the flow, session and application levels for rapid analysis of abnormal traffic behaviour and communication patterns.

The network and application visibility made possible by metadata extraction and analysis improves situational awareness and cyber defense. In much the same way Business Intelligence provides context around enterprise data to improve decision making and business agility, traffic metadata can provide the intelligence to put context around network usage and events, increasing the insight and agility of cyber security teams to be effective.

Where COTS products can take weeks to detect and mitigate new threats, custom second-line solutions based on metadata extraction enable government agencies and their major contractors, critical infrastructure industries, and centralized Security Operations Centers to protect sensitive networks in near real time.

Metadata decoding enables rapid correlation and analysis of information. It can not only complement data logs, but is often more valuable than looking at full packet payloads to identify traffic patterns. Metadata require less storage than full packet capture, which means historical data can be retained for longer periods of time, improving investigative capabilities. The use of metadata enables much faster forensic searches, for example, the ability to search two terabytes of data in less than two minutes. Metadata can also be used to quickly index traffic flows and packet contents.

By leveraging metadata, security solution developers can quickly and affordably build a custom barrier, based on their specific knowledge about their network environment and what constitutes normal network behavior. Applications can be built to identify threats that evade COTS products, such as the detection of ICMP, DNS and Tor tunneling, abnormal email, malware transfer through IM files and Botnets.

Such custom solutions created specifically as an intelligent Second Line of Defense give security specialists complete control over these applications and rules based on their knowledge and experience in their environment. Any anomaly in network behavior can be detected and mitigated in minutes. The custom barrier based on metadata extraction also improves the confidentiality of cyber defense.

Thibaut Bechetoille is the CEO of Paris-based Network Intelligence technology vendor Qosmos.

#### 5. ISSA-UK/EMEA PROMOTED "SECURITY DAYS"

(either run by ISSA UK or in cooperation with associates & affiliates)  
(6 CPEs - no admittance charge for ISSA members)

Check <http://www.issa-uk.org> for upcoming Security Days

#### 6. ISSA-UK & 'MEDIA PARTNER / ASSOCIATE' - CALENDAR OF EVENTS:

<http://www.issa-uk.org/events.htm>

In all cases please contact [administration@issa-uk.org](mailto:administration@issa-uk.org) to obtain discount codes

#### JUNE

**MISi Europe: 8th Annual CISO Executive Summit & Roundtable** - Rome, Italy 8th - 10th June  
- established as Europe's premier event for directors and thought-leaders in information security and technology risk management and a new 1-day pre CISO Cloud Security Think Tank (Tuesday 7th



## SPONSORS

### PLATINUM



### GOLD



### SILVER



### BRONZE



### Association Partner



### Partner Organisations



### Training, event, media & association sponsors:

MISTi (Europe)  
Gartner "IT Security Summit"  
SANS  
RSA europe  
Virus Bulletin  
BlackHat Europe  
Search Security UK

June) that will be dedicated to tackling security best practices & challenges around

the Cloud. Please see website for further information at <http://www.mistieurope.com/ciso>  
\*ISSA members will get a 10% discount off all registrations

### SC Magazine - 3rd Annual Data On The Move Conference: Mobile Device Management - London - 23rd June

SC magazine's 3rd Annual Data On The Move conference; Mobile Device Management on 23 June 2011 in London and think that the event will be relevant to the members of your organisation. The conference is designed for IT Security professionals and will provide expert insight into overcoming the security challenges of increasing IT consumerisation.

To obtain your exclusive £100 discount simply quote the code 'SCISSA' in the section 'How did you hear about this conference?' when booking online at: <http://www.scmobiledevicemanagement.com>.  
\*end-users only

### SASIG: "Social Networking - Friend or Foe?" - The Gherkin, London - 10th June 2011

Join leading professionals from a range of organisations who will share their experience and best practice advice on integrating social networking into your business:

For more information, email [sasig@thesecurityco.com](mailto:sasig@thesecurityco.com) or call +44 1234 708456.

## JULY

### CIR Summit: The Cyber Threat 2011 - IoD Hub, London - 7th July 2011

Is your organisation prepared to deal with organised and high level digital attacks? The Government's recent National Security Strategy cites cyber risk as top of the list of concerns for today's organisations. The CIR one day summits will provide effective information and solutions for organisations seeking to protect themselves against cyber threats; with acknowledged industry experts sharing their knowledge and skills. The Right Hon David Blunkett MP will present this year's keynote address.

20% discount for ISSA members (if booked before 10th June 2011) discounted price £475 +vat (regular rate £595)

To book your place, contact: [Hayley.kempen@cirmagazine.com](mailto:Hayley.kempen@cirmagazine.com) + 44 (0)207 562 2414 please quote booking code: ISSA\_11

Find out more: [http://www.cirmagazine.com/conferences/cyber\\_threat](http://www.cirmagazine.com/conferences/cyber_threat)

## NOVEMBER

ISSA-UK are pleased to announce their partnership with Info-Crime 2011 as an Associate Partner we would like to offer our members the opportunity to Sponsor the event with an ISSA corporate discount. For further information on preferred discounts please do not hesitate to contact [robert@gbs-events.co.uk](mailto:robert@gbs-events.co.uk) quoting ISSA corporate discount.

## 7. ISSA INTERNATIONAL ELECTIONS

Just as a reminder, the ISSA International Board elections will be taking place soon. Please ensure that your membership details are correct at <http://www.issa.org>, otherwise you may not be eligible to vote.