

CYBER INTELLIGENCE ASIA 2013

12-15 March 2013, Royale Chulan Hotel, Kuala Lumpur, Malaysia

Organised by: **INTELLIGENCE-SEC**

Supporting Partner:



Endorsed By:



SPEAKERS:

- Honourable Howard Schmidt, Former Special Assistant to the President, Cyber Security Coordinator, Executive Office of the President Obama
- Ir. Md Shah Nuri Bin Md Zain, Under Secretary Cyber & Space Security Division, National Security Council, Prime Minister's Department, Malaysia
- Zahri Yunos, Chief Operating Officer, CyberSecurity Malaysia
- Dr. Mingu Jumaan, Director, Sabah State Computer Services Department, Malaysia
- Chief Inspector (Dr.) Frank Law, President, The High Technology Crime Investigation Association (HTCIA)
- Phannarith Ou, Head, Cambodia Computer Emergency Response Team (CamCERT)
- Leo Dofiles, Computer Crime Investigator/Computer & Cellphone Forensics Planner, Philippine National Police
- Budi Rahardjo, Chairman, Indonesia Computer Emergency Response Team (ID-CERT)
- Jack YS Lin, Information Security Analyst, Japan Computer Emergency Response Team (JPCERT)



WHY ATTEND?

- Listen to the key players in the cyberspace industry
- Opportunity to network with 200+ delegates from across the globe
- Discuss the latest cyber trends and threats
- Analyse the latest solutions to stop cyber terrorism with esteemed government personnel
- Take the time to visit the vibrant exhibition to learn the industry solutions to cyber security
- Don't miss the chance to be networking with senior cyber experts for a full 4 day event

SPONSORS:



EXHIBITORS:



ASSOCIATED WORKSHOPS

Pre-event Workshops on the 12th March 2013

08.30 – 12.30 **WEB APPLICATIONS & SECURITY**

In Association with:  **INDIAN CYBER ARMY™**
Securing Digital India

13.30 – 17.30 **CYBER DEFENCE OR DEFENDING THE BUSINESS**

In Association with:



Post-event Workshops on the 15th March 2013

08.30 – 13.00 **NETWORK HACKING & VULNERABILITY MANAGEMENT**

Hosted by:



KNOWLEDGE PARTNER:



SUPPORTED BY:



For more information visit – www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com

Tel: +44(0)1582 346706 | Fax: +44 (0)1582 346718

Event Schedule

DAY 1 – TUESDAY 12TH MARCH 2013

08.30 – 12.30 | WEB APPLICATION AND SECURITY

Workshop Leader: KISLAY CHAUDHARY, Director of Indian Cyber Army, and Cyber Crime Investigation Bureau

The training will focus on hacking three distinct parts of any web application:

- Web Server Security / Infrastructure Security
- Web Application Security / Code Security
- Web Data Security / Database Security

In Association with:



13.30 – 17.30 | CYBER DEFENCE OR DEFENDING THE BUSINESS

Workshop Leader: AIR COMMODORE (Ret'd) BRUCE WYNN OBE FBSC CITP, Owner, Business Information Solutions UK

This workshop will stimulate and expand your thinking on how to address the Cyber issues confronting you

- Defending the UK Cyber Domains
- Proactive Cyber Defence
- An alternative way of thinking

In Association with:



18.00 – 19.30 | PRE-CONFERENCE DRINKS RECEPTION

- Join (sponsor) for Icebreaker Drinks in the conservatory of the Hotel.

DAY 2 – WEDNESDAY 13TH MARCH 2013

08.30 – 18.00 | CONFERENCE AND EXHIBITION

- Day one of conference and exhibition. Listen to high level military, government and industry presentations from across Asia

Topics Include:

- Malaysian Cyber Security Update
- Investigation against extortion via DDoS Attack
- Cyber Crime in the Philippines
- Indonesian Internet Security Status

DAY 3 – THURSDAY 14TH MARCH 2013

08.30 – 18.00 | CONFERENCE AND EXHIBITION

- Day two of conference and exhibition. Listen to high level military, government and industry presentations from across the Middle East and the US. Gain an insight into the future of Cyber Security.

Topics Include:

- US Government perspective on Cyber Security
- Fighting Cyber Crime in Cambodia in the absence of law
- Japan CERT Activity
- ICS Computer Forensics – Threat Intelligence and Cyber Terrorism Investigations

DAY 4 – FRIDAY 15TH MARCH 2013

08.30 – 13.00 | NETWORK HACKING & VULNERABILITY MANAGEMENT

Workshop Leader: CLEMENT ARUL, Certified EC-Council Instructor (CEI)

What will you learn from the training session

- Gain a wider understanding on how perimeter defences work
- Gain practical experience in analysing internal and external security threats against a network
- Gain valuable insight to expose network vulnerabilities and defend against them
- Be able to implement more effective security policies and firewall strategies

Hosted at EC-Council Academy's Headquarters in Kuala Lumpur:



For more information visit - www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com

Tel: +44(0)1582 346706 | Fax: +44 (0)1582 346718

INTELLIGENCE-SEC

Day 1 - Wednesday 13th March 2013

08.30 Registration & Coffee

09.00 CHAIRMAN'S OPENING ADDRESS

Lieutenant Colonel (Ret'd) Sazali bin Sukardi, Head of Strategic Policy Research, CyberSecurity Malaysia

HOST NATION (MALAYSIA) – OPENING SESSION

09.10 OPENING ADDRESS – MALAYSIAN CYBER SECURITY THREATS AND CHALLENGES

- Overview of cyber security issues in Malaysia
- Where the threats are coming from
- What challenges are the Malaysian Government dealt with when trying to resolve a cyber-attack
- What procedures are in place in to investigate cyber-attacks
- Future needs

Ir. Md Shah Nuri Bin Md Zain, Under Secretary Cyber & Space Security Division, National Security Council, Prime Minister's Department, Malaysia

09.40 CYBER SECURITY CHALLENGES IN SABAH MALAYSIA

- Current computer security status in Sabah
- Cyber Security challenges faced in the state
- Protecting Critical Infrastructure
- Cooperation with neighbouring islands and countries

Dr. Mingu Jumaan, Director, Sabah State Computer Services Department, Malaysia

10.10 RESERVED FOR EC-COUNCIL ACADEMY

Wilson Wong, Managing Director, EC-Council Academy

10.40 Morning Coffee

11.10 SPECIAL ADDRESS - MALAYSIAN CYBER TERRORISM

- Overview of CyberSecurity Malaysia
- What cyber threats Malaysia deals with
- What procedures are in place in to investigate cyber-terrorism
- Future needs

Zahri Yunos, Chief Operating Officer, CyberSecurity Malaysia

PROTECTING CRITICAL INFRASTRUCTURE IN ASEAN REGION

11.40 INVESTIGATION AGAINST EXTORTION VIA DDoS ATTACK

- Analysis of the crime trend against Distributed Denial-of-Service (DDoS)
- Understanding the problem
- Scenarios showing prevalent M.O.s of DDoS extortion in Asia
- Demonstration of the challenges faced in investigations

Chief Inspector (Dr.) Frank Law, President, The High Technology Crime Investigation Association (HTCIA)

12.10 Networking Lunch Break

14.00 JAPANESE CYBER SECURITY UPDATE

- Cyber threats in Japan
- Major Cyber Attacks in the past years
- Findings from massive Cyber attacks
- Analysis on Digital Forensics
- Activities on Digital Forensics

Akira Yamada, Senior Security Analyst, Information Analysis Department, Cyber Defence Institute, Japan

14.30 CYBER CRIME IN THE PHILIPPINES

- Current situation
- Overview of the Digital Forensic Laboratory
- Accomplishments to date
- Cooperation
- Recommendations

Leo Dofiles, Computer Crime Investigator/Computer & Cellphone Forensics Planner, Philippine National Police

14.30 CHINESE CYBER UPDATE

- Overview of CNCERT
- Cooperation between China and international allies to protect critical infrastructure
- Dealing with the black market of hackers

Invited: *Dr. Yuejin Du, Deputy Chief Technology Officer, CNCERT, and Director, National Institute of Network and Information Security, China*

15.00 Afternoon Tea

15.30 FIGHTING CYBER THREATS IN THAILAND

- Overview: Internet situation in Thailand
- Interesting cases in Thailand
- Next steps for protecting government's network
- IT Security Awareness activities

Kitisak Jirawannakool, Senior Engineer, Wireless Information Security and Eco-Electronics Research Unit (WISRU), Thai National Electronics and Computer Technology Center (NECTEC)

MIDDLE EAST CYBER UPDATE

16.00 UAE CYBER UPDATE

- Overview of aeCERT
- Cyber related crime in the UAE
- Current procedure in place to investigate cyber attacks
- Current trends in cyber crimes and threats
- Future solutions for the Middle East

Tariq Al Hawi, Director, aeCERT, United Arab Emirates

16.30 CHAIRMAN'S CLOSING REMARKS

Lieutenant Colonel (Ret'd) Sazali bin Sukardi, Head of Strategic Policy Research, CyberSecurity Malaysia

16.45 Close of Conference Day 1

17.30 Close of Exhibition Hall Day 1

For more information visit - www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com

Tel: +44(0)1582 346706 | Fax: +44 (0)1582 346718

INTELLIGENCE-SEC

Day 2 - Thursday 14th March 2013

08.30 Registration & Coffee

09.00 CHAIRMAN'S OPENING ADDRESS

Anwer Yusoff *Head of Innovation and Commercialisation, CyberSecurity Malaysia*

US CYBER SECURITY UPDATE

09.10 KEYNOTE ADDRESS – US GOVERNMENT PERSPECTIVE ON CYBER SECURITY

- Current procedures in place within the Obama Administration on cyber threats
- How the US Government protects its critical infrastructure
- What new procedures have been implemented in the last few years to protect sensitive information
- Has social networking increased the threat of cyber attacks in the US?
- New strategies in place to improve Government infrastructure

Honourable Howard Schmidt, *Former Special Assistant to the President, Cyber Security Coordinator, Executive Office of President Obama*

ASEAN CERT UPDATE

09.40 FIGHTING CYBERCRIME IN CAMBODIA IN THE ABSENCE OF LAW

- Current threats in Cambodia
- Challenges faced
- Response to the threats
- Case study examples

Phannarith Ou, *Head, CamCERT, Cambodia*

10.10 INDONESIA INTERNET SECURITY STATUS 2012/2013

- Current cyber trends in Indonesia
- Different incidents ID-CERT are receiving
- Social media impact
- Procedures in place to prepare for a cyber attack
- IT Forensic investigations

Budi Rahardjo, *Chairman, ID-CERT, Indonesia*

10.40 Morning Coffee

11.10 JAPAN CERT ACTIVITY

- Security incident trends
- CERT countermeasures
- Security alliances
- Challenge for the changing threats

Jack YS Lin, *Information Security Analyst, JPCERT, Japan*

CYBER FORENSIC INVESTIGATIONS

11.40 RESERVED FOR ELCOMSOFT PRESENTATION

Senior Representative, ElcomSoft

12.10 Networking Lunch

14.00 ICS COMPUTER FORENSICS – THREAT INTELLIGENCE AND CYBERTERRORISM INVESTIGATIONS

- Comparative analysis of security incidents in ICS sphere for last years
- Threats description and attack vectors – practical view on ICS security
- Counter forensics measures for cyber terrorism and cyber warfare
- Computer forensics in RTOS, RTU's, ICS network infrastructure
- Malware intelligence of ICS malware

Andrey Komarov, *Chief Technology Officer for CERT-GIB, Russian Law Enforcement & Representative at the European Union*

14.30 RESERVED FOR EMERGING THREATS PRESENTATION

Matt Jonkman, *Chief Technology Officer, Emerging Threats*

15.00 Afternoon Tea

15.30 FORENSIC OPERATIONS IN THE TELECOMMUNICATIONS INDUSTRY

- Overview of the International Telecommunications Union (ITU)
- Threats faced to telecommunication infrastructure
- Forensic investigations
- Common challenges faced

Marco Obiso, *Cyber Security Coordinator, International Telecommunications Union (ITU)*

16.00 CYBER FORENSICS IN INDIA

- Overview of Indian Cyber Security
- Case studies of hacking attempts to Indian Critical Infrastructure
- Computer Forensic update
- Future solutions to consider

Kislay Chaudhary, *Director and Senior Information Security Analyst, Indian Cyber Army*

16.30 CHAIRMAN'S CLOSING REMARKS

Anwer Yusoff *Head of Innovation and Commercialisation, CyberSecurity Malaysia*

16.45 Close of Conference Day 2

17.30 Close of Exhibition Hall Day 2

For more information visit - www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com

Tel: +44(0)1582 346706 | Fax: +44 (0)1582 346718

INTELLIGENCE-SEC

SPONSOR SYNOPSIS

SPONSORS



ElcomSoft Co.Ltd. is a global industry-acknowledged expert in computer and mobile forensics providing tools, training, and consulting services to law enforcement, forensics, financial and intelligence agencies. ElcomSoft pioneered and patented numerous cryptography techniques, setting and exceeding expectations by consistently breaking the industry's performance records. ElcomSoft is Microsoft Gold Independent Software Vendor, Intel Software Premier Elite Partner, member of Russian Cryptology Association (RCA) and Computer Security Institute. More info at <http://elcomsoft.com/>.



Emerging Threats is a world-leading provider of open source and commercial threat and malware intelligence. Founded in 2003 as a cyber security research community, Emerging Threats has become the de facto standard in network-based malware threat detection.

EXHIBITORS



Codenomicon is a market leader in proactive security testing and real-time situation awareness solutions. Codenomicon's fully automated solutions enable you to improve your defenses against Advanced Persistent Threats (APTs). Experience cyber security beyond traditional signature-based defenses: discover zero-day vulnerabilities proactively and detect suspicious traffic at the earliest possible moment. www.codenomicon.com



Established in 2005 and headquartered in Hong Kong, DataExpert is one of the leading companies in IT security industry. We provide a full suite of products and services in the areas of data recovery, computer crime investigation, and data disposal, to help governments, corporations and individuals better manage their data assets and comply with regulations.



HackingTeam provides the premier Cyber Intelligence solution: Remote Control System (RCS).

Proven by years of worldwide adoption and designed to fulfill LEAs and Security Agencies higher expectations, RCS gives you total control over endpoint devices. Offering the widest selection of infection vectors and showing total invisibility to protection systems, RCS guarantees easy installation on target devices. An integrated, easy to use Console allows you to manage all of your tasks, from evidence collection to infrastructure management. Newly released RCS version 8, codenamed Da Vinci, introduces a new dimension of cyber investigations: data intelligence. Find out more at www.hackingteam.com



EC-Council Academy was established in 2000 and is now recognized as one of the leading providers for global training programs and services, designed to enable advancement through information security training.

EC-Council Academy is a specialized and boutique information security training provider. Top courses include Certified Ethical Hacker (CEH), EC-Council Certified Security Analyst (ECSA), and Computer Hacking Forensic Investigator (CHFI).

EC-Council Academy is the winner for "Information Security Education & Training Provider of the Year" awarded by CyberSecurity Malaysia for 3 consecutive years including 2012. For more information, please visit www.eccouncilacademy.org

For more information visit - www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com

Tel: +44(0)1582 346706 | Fax: +44 (0)1582 346718

INTELLIGENCE-SEC

12th March 2013

08:30-12:30

WEB APPLICATION & SECURITY

In association with:



OBJECTIVE

The objective of this training is to provide an in-depth approach to Web Application hacking and is meant to create an environment for participants to create, test and verify exploits for various web application vulnerabilities in multiple simulated application settings. This course is meant for people who have a basic web programming background and are keen to get started on hacking, testing, defending and building web applications. The training is meant to be fast paced, intensive and result oriented mixture of a lot of practical hands-on and a little bit of theory thrown in for good measure.

The training will focus on hacking three distinct parts of any web application:

- Web Server Security / Infrastructure Security
- Web Application Security / Code Security
- Web Data Security / Database Security

COURSE CONTENT

- Web Application Security Basics
- Hacking and Protecting Web Application Servers
- Web Server common misconfigurations
- Port scanning, service discovery
- Vulnerability Assessment, reducing the attack surface
- Auditing users, file permissions
- Sandboxing, securing processes from running wild
- Application Security
- Clickjacking and UI Redressing
- HTTP Parameter Pollution
- HTTP Response Splitting
- Side Channel Attacks in SSL
- Attacking User Data
- Common Database mis-configurations
- Secure hashing and encryption

WHY ATTEND?

- How to test for and compromise web servers
- How to detect vulnerabilities and compromise web applications
- How hackers steal user data for profit
- All of the above to create, maintain, secure web servers and web applications

WHO SHOULD ATTEND?

- Web Application Developers
- Web Application Security Consultants
- Penetration Testers
- QA Professionals
- Security Experts
- System Administrators with basic scripting knowledge

ABOUT HOST



- KISLAY CHAUDHARY the current Director of Indian Cyber Army and Cyber Crime Investigation Bureau, is a technocrat par excellence a dynamic and result-oriented Manager with very fine personal and inter-personal qualities an astute Institution-builder with a strategic vision an able Administrator with a positive attitude and an inspiring Leader credited with nurturing leadership skills in the younger generation. He has had a distinguished career adorned with accomplishments that spans beyond 8 years in Information Security, Ethical Hacking and InfoSec Researches.
- He is a graduate in Information Technology, completed his CEH from EC Council, CCNA from Cisco and was awarded MCSE from Microsoft.
- As the founder Director of Indian Cyber Army [ICA], he is credited with setting up a world class and model scientific Research Centre in Information Security and Detective Agency for Cyber Crimes right from concept to fruition in a record time of two years. His relentless efforts in the aftermath of the Cyber Wars of November 2010 resulted in the formulation of a Cyber Security Lab for the Indian Cyber Army at New Delhi, India, which was later successfully established.
- He has definitive experience in the field of Internet Security. He has authored several International bestsellers on numerous topics related to computer security, which have been widely appreciated by both professionals and industry leaders.
- He has also conducted more than 200 different training sessions on various topics related to cyber security to an audience comprising corporate executives, law n enforcement personnel, entrepreneurs and technical specialists. He possesses an in-depth knowledge and insight into today's security risks and tomorrow's potential threats.
- He has been interviewed by several print and online media where he has shared his experiences relating to latest happenings in Cyber War and Cyber Crimes. He is regularly invited by Dainik Jagran and Dainik Bhaskar to share the latest updates on virus outbreaks, loopholes and cyber crime trends

PREREQUISITES

- Basic knowledge of HTTP.
- Understand terms like GET, POST, HEAD
- Understand what is a cookie, interception proxy, web server document root, port number
- Basic knowledge of at least in PHP/.net/JSP/Java Servlets
- Basic comfort level in using the command line on Windows and Linux
- Basic idea of SQL and working knowledge of databases like MySQL and MSSQL

WHAT TO BRING

- Bring your own Laptop
- The laptop should have 20 GB of HDD space free
- The laptop should have a working wireless connection
- Install Windows/Linux capable of running VirtualBox/VMware as Host OS

For more information visit - www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com

Tel: +44(0)1582 346706 | Fax: +44 (0)1582 346718

INTELLIGENCE-SEC

12th March 2013

13.30-17.30

CYBER DEFENCE OR DEFENDING THE BUSINESS

In association with:



OBJECTIVE

The workshop will stimulate and expand your thinking on how to address the Cyber issues confronting you.

Using as a starting point the UK MOD's Cyber Defence Taxonomy (which was authored by the presenter under specific tasking from the UK MOD), the workshop will explore the competing pressures on CIOs, CISOs, CTOs, COOs and CEOs across their respective areas of responsibilities, and present some guidance on how to make more appropriate balance of investment decisions in 'Cyber'

In defending in the Cyber domain, it will address what should be the balance between:

- Technology versus Tactics?
- People versus Procedures?
- Defending versus Detecting?

It will analyse the trend towards Intelligence-based Cyber Defence, and some of the consequent legal implications.

Business is about managing risk - cyber is no different

- Risk = (Threat x Vulnerability x Impact) / Probability
- How should this affect the way in which we protect ourselves and our systems?
- Advanced Persistent Threat or Conventional Malware Attacks - what should we REALLY be worried about?
- And how do you address the solution?

WORKSHOP PROGRAMME

1330-1430 - Defending the UK Cyber Domains

- UK Cyber Strategy and The UK CND Taxonomy
- Military operations v Intelligence Collection v Law Enforcement
- Immediate Self-Defence versus Forensics and Evidence-Chain preservation

1430-1530 - Proactive Cyber Defence

- The Cyber Kill Chain
- Intelligence-based Cyber Defence

1530-1600 - Refreshments break

1600-1645 - An alternative way of thinking

- Deter - Deny - Defend - Detect - Diagnose - Delineate - Display - Demarcate - Decontaminate - Dissect - Disseminate - Destroy

1645-1730 - Bringing it all together

- Where should you spend the money?
- Why do you need more money?
- What are the consequences of your selected course of action?

ABOUT HOST



- Air Cdre Bruce Wynn (O-7, OF6, Brig Gen, RADM (lower half)) spent 34 years in the UK's Royal Air Force Information Systems arena, across the Operations, Technical and Intelligence business, including being the Service's Chief Information Technology Officer (CTO for 'Cyber'), Chief Information Security Officer, Chief Security Accreditation Officer, and Deputy Chief Information Officer. He is now an independent consultant.
- Since his retirement from active duty in 2004, he has developed a portfolio of engagements in the informatics and cyber domains, including special advisor to the CIO/CTO of one of the UK's intelligence agencies, support to large companies such as IBM, Gartner, Lockheed Martin, Raytheon, EADS, Dell/Secureworks, Global Crossing and L3 in the UK, and IBM, Guidance Software, Endgame Systems, Integrity Global Security, VIR-SEC, @Sentinel and ResilientCom/Tier-V Corp in the USA.
- His portfolio also includes active participation as CTO in small niche companies at the heart of the high-security aspects of government, and as a Visiting Scientist with the US Navy's Office Of Naval Research Global, covering Cyber! He has been appointed as a Serious Cyber Incident Response Coordinator for a Fortune 50 cyber security services company for their interaction with affected CIOs, CEOs and COOs
- He has spoken widely on Cyber, as well as facilitated discussions and workshops, at conferences and seminars in the US, and UK as well as across Europe for the defence, intelligence and national security communities, and has been a regular at conferences such as BlackHat and Defcon since 2004
- He is a Senior Fellow of the British Computer Society, a Chartered Information Technology Professional, and has been appointed by Her Majesty the Queen as an Office of the Most Excellent Order of the British Empire

WHO SHOULD ATTEND?

- CIO/COO/CTO senior staff who need an appreciation of cyber challenges outside their immediate responsibility areas, and a set of tools to help them think through their challenges
- Technical Cyber staff who need to update their business credentials, and position themselves within the wider business space rather than just the Cyber Domains
- Government officials who want better insight into commercial Cyber Defence thinking
- Anyone faced with balance of investment decisions (ranging from multimillion dollar projects down to simple domestic options) in 'Cyber'

For more information visit - www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com

Tel: +44(0)1582 346706 | Fax: +44 (0)1582 346718

INTELLIGENCE-SEC

15th March 2013

08.30-13.00

NETWORK HACKING & VULNERABILITY MANAGEMENT

Hosted By:



OBJECTIVE

This is a comprehensive technical workshop providing a clear understanding of network from an offensive and defensive point of view. You will learn how to analyze risk and deploy the appropriate countermeasures to reduce your exposure to network threats.

The workshop consists of demonstrations of “ethical hacking”, featuring the most common but effective hacking tools used, such as Backtrack 5 R3, Subterfuge, Cain & Abel, Yamas, Metasploit, NeXpose, SQLMap, Social Engineering Toolkit, Keyloggers and many more.

Besides that, components and requirements of a robust vulnerability management program will be covered, and students will practice these components in hands-on labs. Additionally, the workshop will focus on top mitigation techniques and strategies to implement and reduce the chance of a compromise.

ABOUT HOST



EC-Council | Academy

IT Security Training or Nothing Else.

EC-Council Academy was established in 2000 and is now recognized as one of the leading providers for global training programs and services, designed to enable advancement through information security training.

EC-Council Academy is a specialized and boutique information security training provider. Top courses include Certified Ethical Hacker (CEH), EC-Council Certified Security Analyst (ECSA), and Computer Hacking Forensic Investigator (CHFI).

EC-Council Academy is the winner for “Information Security Education & Training Provider of the Year” awarded by CyberSecurity Malaysia for 3 consecutive years including 2012.

For more information, please visit www.eccouncilacademy.org

WORKSHOP PROGRAMME

8:30 – 10:30 **Network Hacking: Concepts, Techniques, Tools, Hacks and Defenses**

10.30 – 11.00 **Networking Break**

11:00 – 13.00 **Vulnerability Assessment and Pentesting : Manual and Automated Approaches with FREE and Enterprise tools**

WHAT ARE THE LEARNING OUTCOMES?

- Have wider understanding on how perimeter defenses work
- Gain practical experience in analyzing internal and external security threats against a network
- Gain valuable insight to expose network vulnerabilities and defend against them
- Be able to implement more effective security policies and firewall strategies

WHO SHOULD ATTEND?

- Information Security Professionals
- System Administrators
- Network Administrators
- Penetration Testers
- Security Architects
- Security Analysts
- Security Engineers
- Anyone who is concerned about network security

For more information visit - www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com

Tel: +44(0)1582 346706 | Fax: +44 (0)1582 346718

INTELLIGENCE-SEC

EVENT PARTNERS



CyberSecurity Malaysia (www.cybersecurity.my) is the national cyber security specialist agency under the Ministry of Science, Technology and Innovation (MOSTI), Malaysia (www.mosti.gov.my). Previously known as the National ICT Security and Emergency Response Centre (NISER), CyberSecurity Malaysia became an agency under the purview of MOSTI in 2005 as a national body to monitor aspects of National e-Security. In essence, the role of CyberSecurity Malaysia is to provide specialised cyber security services in the following areas:

1. Cyber security emergency response, incident handling, and digital forensics.
2. Cyber security quality management.
3. Cyber security capability and capacity development.
4. Cyber security outreach and acculturation.
5. Cyber security research and risk assessment.
6. Cyber security evaluation and certification

For more information, please visit www.cybersecurity.my



www.indiancyberarmy.org/security/index.php



MyCEB was established in 2009 by Ministry of Tourism, Malaysia to further strengthen Malaysia's business tourism brand and position for the international meetings, incentives, conventions and exhibitions (MICE) market. A non-profit organisation, MyCEB serves as a one-stop centre to assist meeting and event planners to bid for and stage regional and international business tourism events in Malaysia and act as a conduit for national product development. We trust with this information, your good office has a better understanding of MyCEB's role and objectives which is in line with the Government's aim of promotion Malaysia as the preferred MICE destination in the international market. www.myceb.com.my



ASDNews.com—"Bethe first to know" ASDNews brings the latest aerospace, defence and security news from government, industry and major news agencies around the world. Our service has over 60,000 active subscribers and 2 million article readers per year. ASDNews content is categorised in over 25 main news groups - for example: "Training & Simulation News", or "Unmanned Systems News" - making recent and related articles easy to find. Subscribe to our free daily newsletter or weekly group newsletters on www.asdnews.com/subscription



The Asia Pacific Security Magazine is the Asia Pacific's leading government and corporate security magazine. Distributed to many of the biggest decision makers in the security industry, the Asia Pacific Security Magazine is a highly respected and sought after publication. Since acquiring what was the Australian Security magazine in 2011, My Security Media has expanded the scope of the magazine to the Asia Pacific region incorporating hard hitting investigative journalism, provoking editorial and up-to-date news, trends and events for all security professionals. Covering topics within frontline security to Asia Pacific security to training, equipment and technology to name a few, the Asia Pacific Security is a must read for all those in the security industry. <http://www.asiapacificsecuritymagazine.com/>



Asian e-Marketing is a pioneer in the region, covering the digital age and zooming in on the increasingly valuable and indispensable tools of today's marketers? The Internet and mobile devices. Circulated twice every month to more than 22,000 top management and marketing decision-makers in Asia Pacific, the informative guide supports and advises e-marketers in finding a sound marketing strategy, which is vital for further business success. <http://www.mediabuzz.com.sg/asian-emarketing-latest-issue/latest-issue>



ContingencyToday.com is dedicated to the challenges and opportunities of Critical National Infrastructure protection. Its readership includes policy-makers, decision-influencers and middle management implementers engaged in emergency planning, disaster recovery and infrastructure protection including electronic attack and the sophisticated misuse of computer systems; physical attacks by terrorist organisations and other criminals; the effects of climate change; and other natural disasters, including pandemics, fire and flood.



Digital Forensics Magazine. Dedicated to all aspects of Digital Forensics with the quality and feel of a peer-reviewed journal yet the layout and features of a magazine. Packed full of feature articles plus sections on Legal, From the Lab, All things Apple, Interviews, Expert Comment, Competitions and much more. www.digitalforensicsmagazine.com



Global Security Mag is a quarterly magazine & website in French & English. Global Security Magazine is a Logical & Physical IT Security Magazine circulated to 5,000 decision makers, typically CSO. We have daily online information in English & French at: www.globalsecuritymag.com & www.globalsecuritymag.fr and in newsletters. On the 4th April 2013, we have organised the 4th annual GS DAYS, the francophone Security days conference in French on Ethical hacking. www.gsdays.fr Contact: SIMP, 17, av. Marcelin Berthelot, 92320 Châtillon, Tél. : 01 40 92 05 55 – Fax : 01 46 56 20 91 – email: ipsimp@free.fr or marc.jacob@globalsecuritymag.com

For more information visit - www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com

Tel: +44(0)1582 346706 | Fax: +44 (0)1582 346718

INTELLIGENCE-SEC

EVENT PARTNERS



Hakin9 is an online weekly issued magazine devoted to IT Security in all its aspects. Delivering practice-focused information provided by IT Security specialists world-wide is our mission which we have been successfully completing over the past decade. The yearly subscription gives you the access to over 50+ new issues, 200 archive issues, e-books, video tutorials, guides as well as attractive discounts and free passes to conferences, trainings, other related events, software licenses and sometimes even hard copies of the soft/hardware or books http://hakin9.org?a_aid=agatawierzchowiak&a_bid=8f6377e8



The ICT Community Portal is the Middle East and Africa leading online Portal providing in-depth coverage and features to serve the needs of the dynamic ICT Community. Users can access the latest news, events and trends shaping the IT world, stay abreast of upcoming products, events and services, and utilize interactive features to discuss favorite topics. For more information please visit <http://www.ictcommunityportal.com>



Information Security Today, www.infosectoday.com, provides essential information for managing the security of a modern, evolving enterprise. It is written for information security managers and other technical managers and staff who are the first-line support responsible for the daily, efficient operation of security policies, procedures, standards, and practices. Information Security Today informs its readers of best practices, as well as of research into current and upcoming issues in information security. Articles take a how-to approach to their topics. They help readers solve problems and be applicable to on-the-job situations faced everyday by IT, information security, and networking and system administration professionals. Information Security Today covers Access control systems and methodologies; Computer operations security; Application and systems development; Business continuity and disaster recovery planning; Telecommunications and network security; Security architecture and models; Physical security; Cryptography; Security management practices; Law, investigations, and ethics.



MediaBUZZ aims to make an impact in the Asia Pacific region through its online publication Asian e-Marketing, which is designed to empower marketers in the vibrant, ever-changing, electronic marketing environment. www.mediabuzz.com.sg/



My Security.com.au - The My Security website provides a multi faceted medium for security companies to engage with the Australian market and also with one another. MySecurity.com.au is a comprehensive resource for all those in the industry to stay informed on current events, news, jobs as well as serving as a platform for Australian Security companies to promote and advertise their products and services. Since its inception in 2006, My Security.com.au has grown rapidly from an online security portal, to the creation of the My Security Media Group which publishes the Asia Pacific Security Magazine. In 2011, My Security TV launched its very own security channel that has seen it broadcast from many security related events around the world. <http://www.mysecurity.com.au/>



PenTest Magazine is a weekly downloadable IT security magazine, devoted exclusively to penetration testing. It features articles by penetration testing specialists and enthusiasts, experts in vulnerability assessment and management. We cover all aspects of pen testing, from theory to practice, from methodologies and standards to tools and real-life solutions. Each magazine features a cover focus, and articles from our regular contributors, covering IT security news and up-to-date topics. The magazine is available by paid subscription. It is devoted to the best penetration testing services providers, who will show you the pen testing world from their perspective. It's an excellent opportunity to observe security trends on the market for the readers, and for companies – to share their invaluable knowledge. www.pentestmag.com



SecurityXploded is a popular Infosec Research & Development group delivering the latest information in various areas of security including Anti-Spyware, Reverse Engineering, Cryptography, Password Recovery, Network security, Forensics etc. It has published 50+ research articles and 90+ FREE security software's. Most of these software's have been listed and received top awards from leading download sites including Softpedia, BrotherSoft, CNet Download etc. Founded 4 years ago, it has grown to become one of the most popular security portals on the net serving the community through its knowledge sharing work. <http://securityxploded.com>



Vigilance is the undisputed leading voice of the global security industry. The depth of our reportage, the brilliance of our analysis of the global security issues and the global influence of our editorials are incomparable. The intellectual and marketing bent of Vigilance are the results of many years of research. Our writers and contributors are key players of the global security industry; no wonder Vigilance is not only the magazine for decision makers and those who are in charge of purchasing budgets in their various organizations across the globe, but the world's leading security magazine. Because our focus is international, our news has the farthest reach, so also is every advert placed on Vigilance. Vigilance therefore, is your definitive guide to the global security market.



Virus Bulletin has a formidable reputation as the leading specialist publication on computer malware and spam. Each issue contains news and opinions from the anti-malware and anti-spam community, analyses of the latest threats and comparative product reviews featuring the unique VB100 and VBSpam award schemes. The comparative reviews are also available separately. VB2013, the 23rd Virus Bulletin International Conference, will take place 2-4 October 2013 in Berlin, Germany. Split into two streams, the conference program caters for both technical and corporate audiences, covering a wide range of anti-malware and spam-related subjects. www.virusbtn.com

For more information visit - www.intelligence-sec.com

Book your place by:

Web: www.intelligence-sec.com | Email: events@intelligence-sec.com

Tel: +44(0)1582 346706 | Fax: +44 (0)1582 346718

INTELLIGENCE-SEC

HOW TO REGISTER
Telephone: +44 (0)1582 346 706 | Fax: +44 (0) 1582 346 718 | Online: www.intelligence-sec.com
Email: events@intelligence-sec.com

DELEGATE DETAILS:
Please complete your details below.

Title/Rank:	
First Name:	
Surname:	
Job Title:	
Company:	
Tel:	
Fax:	
Email:	
Address:	
Signature:	
Date:	

Please Tick	Military/Government, Public Sector Rate	Standard Price
	Two Day Conference & Exhibition	£500
	Workshop A	£200
	Workshop B	£200
	Workshop C	£200
	All of the above	£1,100
Please Tick	Commercial Organisations	Standard Price
	Two Day Conference & Exhibition	£1,000
	Workshop A	£400
	Workshop B	£400
	Workshop C	£400
	All of the above	£2,200

VENUE & ACCOMMODATION

Hotel Name: Royale Chulan Hotel,
5 Jalan Conlay, 50450, Kuala Lumpur, Malaysia

Please tick here if you would us to contact you to book your accommodation

PAYMENT DETAILS:
Please complete your details below.

Wire Transfer:
Barclays, 16 High Street North, Dunstable, Bedfordshire, LU6 1JZ, United Kingdom
Sort Code: 20 55 33 Account Number: 53554104

Payment by Credit Card:
All card payments need to be made via our website
<http://www.intelligence-sec.com/login/>

ADDITIONAL NOTES

TERMS AND CONDITIONS

Payments - All bookings made prior to the conference must be paid in full to guarantee registration. Once payment has been received, an email confirmation and a receipted invoice will be sent. If payment is not made at the time of booking, registration will be provisional. Bookings received less than two weeks before the conference date can only be paid by credit card.

Early Bird Rate - In order to qualify for any 'early bird' rates, booking must be received before the deadline date listed in the conference marketing material.

Substitutions & Cancellations - Delegates may nominate an alternative person from their organisation to attend up to 24 hours prior to the start of the event, at no extra charge. Should substitution not be possible, cancellation charges apply as follows: 8 weeks or more prior to start of event: 10% of the delegate fee, 4 to 8 weeks prior to start of event: 50% of the delegate fee, 4 weeks or less prior to start of event: 100% of the delegate fee. All substitutions and cancellations must be received in writing

Access Requirements - Delegates should advise of any special access requirements at the time of registration.

Registration Information - Registration information will be sent to registered delegates by email at least seven days prior to the event. Any delegate not receiving the registration information should contact us by email to events@intelligence-sec.com

Alterations to Programme - Cancellation/Postponement of Event - Intelligence-Sec reserves the right to make alterations to the conference programme, venue and timings. In the unlikely event of the programme being cancelled by Intelligence-Sec, a full refund will be made. Liability will be limited to the amount of the fee paid by the delegate. In the event of it being found necessary, for whatever reason, that the conference is being postponed or the dates being changed, the organisers shall not be liable for any expenditure, damage or loss incurred by the delegate. If by re-arrangement or postponement the event can take place, the booking between the delegate and the organisers shall remain in force and will be subject to the cancellation schedule in paragraph 3

Speakers - Views expressed by speakers are their own. Intelligence-Sec cannot accept liability for advice given, or views expressed, by any speaker at the conference or in any material provided to delegates.

Photography & Filming - For promotional purposes, there may be a professional photographer and video production taking place during the conference. Delegates who do not wish to be filmed or recorded should advise the organisers by email to events@intelligence-sec.com prior to the event.

Data Protection - By submitting registration details, delegates agree to allow Intelligence-Sec and companies associated with the conference to contact them regarding their services. Delegates who do not wish to receive such communications please email events@intelligence-sec.com. The contact details of registered delegates will be placed on the attendee list which will be passed to sponsoring companies and to all attendees for them to see who is at the conference for the purpose of networking and meetings. Delegates who do not wish to be included on this list should advise at the time of booking.

Websites & Links - The conference and associated Intelligence-Sec websites may link to other websites and networking tools provided for the convenience of the users. The contents of these websites are maintained by their owners, for which Intelligence-Sec takes no responsibility. Neither can responsibility be taken for contents of any website linking to this website.

Insurance - It is the responsibility of the delegate to arrange appropriate insurance cover in connection with their attendance at the conference. Intelligence-Sec cannot be held liable for any loss, liability or damage to personal property. If you have any questions about these Terms & Conditions, please contact – events@intelligence-sec.com