FIRST™

Improving Security Together

security is not an island

CONFERENCEPROGRAM

24th Annual **FIRST** Conference

MALTA

17 - 22 June 2012

welcome to malta.

It is my pleasure to welcome you to the 24th Annual FIRST Conference here in Malta. I'm sure that the combination of the location, the program and the people I know are attending is going to make this an unforgettable week for us all.

The tagline for this week (*security is not an island*) speaks volumes about what we do and why FIRST exists. On one hand it serves to remind us that security is not an end in itself - but part of the larger picture.

The tagline also fits on a different level—in what FIRST exists to do; to ensure that teams are part of a greater grouping and to reinforce that an incident that affects one team almost always affects others and can be more easily resolved using relationships started at conferences such as this. This has been reinforced many times over the years I have been attending FIRST conferences as people I have met have proved to be exceptionally helpful to me in my work in incident response.

Malta has an amazing history, stretching back thousands of years. It stands between Europe and Africa. It has been known as a meeting point between cultures, countries and people over the centuries. I am sure, looking at the program that we can live up to that history—I can only be impressed at the calibre and quality of the speakers and the program that Jose has put together.

As we face our challenges—old as well as new—in technologies such as cloud computing and mobile through to compliance and cybercrime, the need to come together and talk, discuss, challenge and create solutions becomes more important. FIRST has been helping its members do this for over 20 years and it is as crucial now as it was when we started.

I'd like to thank all the people who've worked to bring this conference together, Dr. Jose Nazario (2012 Program Chair) and his program committee, Steve Adegbite (Conference Liaison), CAPS LLC (Phoebe Boelter, Kristen Jacobucci and Traci Wei). All of these people have put in enormous amounts of time and effort over the last year, making this yet another great conference.

I'd like to thank the Steering Committee and their employers for the time and effort they put in year round to keep FIRST improving and moving forward all the time.

I'd like to especially thank the keynotes and speakers who are sharing their knowledge and experience with us.

Most of all, I'd like to thank you for attending. I encourage you all to take advantage of the program, the breaks and the social events to introduce yourselves to people you've not met before, to reinvigorate old friendships with people you've not seen for a while and talk about your successes and challenges (and have some fun). You are what makes this a great and successful conference and we should celebrate that above everything else.

FIRST is what we make of it. Opportunities abound to volunteer to support worthwhile efforts: SIGs, hosting TCs. and so on. I hope you'll be sufficiently inspired by what you see this week to want to participate in—and perhaps, join FIRST and its efforts. We'd love to have you aboard with us.

Chris Gibson

Chris Gibson
Chairman, FIRST.Org
Director, Citi ,UK

2011-2012 Steering Committee

Kenneth van Wyk
Vice Chairman
KRvW Associates LLC, US

Peter Allor
CFO
IBM, US

Steve Adegbite
Conference Liaison
Lockheed Martin, US

Cristine Hoepers
CERT.br/NIC.br, BR

Margrete Raaum
UiO-CERT, NO

Reneaué Railton
Cisco Systems, US

Robert Schischka
CERT.at, AT

Maarten Van Horenbeeck
Microsoft, US

Suguru Yamaguchi
JPCERT/CC, JP

FINAL ONLINE COPY
July 7, 2012

FIRST Secretariat

FIRST.Org, Inc.
PO Box 1187
Morrisville, North Carolina
27560-1187
United States of America

first-sec@first.org

Conference Office

FIRST.Org, Inc.
Conference Coordination Office
c/o CAPS, LLC
219 W. Chicago, Suite 300
Chicago, Illinois 60654
United States of America

first-2012@first.org
+1 312 646 1013

Venue Information

Hilton Malta
Portomaso, St. Julian's
Malta PTM01

+356 (0) 2138 3383

FIRST Websites

http://www.first.org
http://conference.first.org

Lost & Found

Registration Desk

Please bring all tems to the registration desk. The conference staff will hold all lost items until the conference close on Friday. Items that have not been claimed will be discarded or donated.

@firstdotorg
#FIRSTCON

http://www.facebook.com/firstcon

table of contents.

conference information.

Registration Information

Spinola Lobby - Conference Center Level 5

Sunday	14:00-18:00
Sunday - *Poolside Gazebo*	18:30-21:00
Monday-Tuesday	08:00-16:00
Wednesday-Friday	08:30-16:00

Breakfast Hours

Hilton Hotel - Oceana Restaurant

Monday-Friday	07:00-09:00

Only attendees staying in the Hilton property will be allowed in to the Ocean Restaurant for breakfast. Hilton staff will check for room numbers and your name badges.

An early morning coffee break will be provided in the Spinola Lobby located in the Conference Center for attendees staying at other properties in the main lobby area of the Conference Center.

Accessing Conference Presentations

To access public presentations, please visit:
You must have attended the conference to access this URL

If there is no presentation available, the presenter has either no slides, not yet made their presentation available, or has not granted permission to publish. Final versions of presentations will be collected following conference completion and will be available for one month to download at the URL above.

Final & full presentations will be moved to the presentation archive on the FIRST Member side at https://members.first.org. If you are unable to locate a presentation, please send email to first-2012@first.org.

Internet Access

Conference Meeting Rooms

Free wireless internet will be available to attendees throughout the conference meeting rooms for the duration of the conference. For access, please use the following:

SSID: **FIRST2012**
WPA & WPA2: **FIRST24Malta**

If you have trouble connecting, please ask for assistance at the registration desk.

Attendees are responsible for internet access in their sleeping rooms.

Network Monitoring Privacy Statement

Cisco's Computer Security Incident Response Team (CSIRT) has developed a mobile monitoring and networking solution for providing on-site network and computer security monitoring during conferences and events. The first use of the solution at FIRST 2007 was showcased in a Cisco-on-Cisco article. This year Cisco CSIRT has a similar deployment at the Cisco House of the London Olympics. The CSIRT team monitors 2-3 events per year with this kit, and usually sends 1-2 people to each event to provide security monitoring and a follow-up report.

For more information, please visit http://www.first.org/conference/monitoring.

You may direct questions about this setup, such as the network, security, or privacy assurances, to the Cisco team by emailing first-2012-malta@cisco.com.

CISCO™

Download the Mobile Agenda via EventBoard!

EventBoard

conference policies.

About Conference Policies

Please note the following policies will be in effect during the conference. We ask for your compliance in respecting the privacy of your fellow attendees and limiting distraction and interruptions of the speakers and presenters.

Attendee List

Unless the Conference Office has received an explicit request from a registrant disallowing to share their contact information (through the Registration Form), a list of all attendees, job titles and their affiliation institutions will be included in the delegate packs. Please note this delegate list is for personal use only and may not be used for marketing purposes or shared with other individuals or sources. Violation of this information sharing policy may result in suspension from FIRST and future events.

Mobile Devices

A kind reminder to please turn off or silence all mobile devices during conference sessions.

Photography, Videography & Voice Recording

Photography, videography or voice recording of any FIRST Conference sessions is strictly prohibited. If the policy is violated, the offender will be issued a warning. Any second offense may result in removal (non-refundable) from the conference.

Photography is permitted at the following FIRST Conference events: Ice Breaker Reception, Vendor Showcase and Wednesday Banquet.

Use of Social Media

Please use common sense and respect during conference week. Any individual caught disclosing information from a closed session or a members-only meeting will be issued a warning. Any second offense may result in removal (non-refundable) from the conference.

Use of any social media medium is strictly prohibited during the Annual General Meeting (AGM), this includes, but is not limited to: Twitter, Facebook, IRC, blogging, etc. Any communications are for those in physical attendance at the AGM. Exceptions can only be granted by the FIRST Steering Committee for a limited purpose.

Press Policy

All press must pre-registered with the FIRST Secretariat (first-sec@first.org) and have been granted approval to attend sessions by the FIRST Conference Liaison. Please read the full Press Policy at http://www.first.org/newsroom/policy.

Any opinions expressed are that of the individual and not of FIRST.Org.

about the challenge.

Geek Lounge Hours

Vilhena & Wignacourt Lobby - CC6

Monday-Thursday 10:00-17:00

Visit the Geek Lounge to speak to DRG Challenge staff; to recharge your workstations & mobile devices; and to get away from the crowds.

About the Challenge

The DRG Challenge is a series of technical problems designed to provide attendees a fun opportunity to compete using their creative technical problem solving skills.

Challenge registration starts Sunday evening at the Ice Breaker Reception. Please visit the DRG Challenge information table Sunday evening to get started!

This event is the inaugural kick-off for a series of in-person and online challenges the DRG intends to sponsor.

The Challenge is open to ALL attendees of the conference.

Players are encouraged to register as a team of up to four players. Solo players and smaller teams are also welcome to participate.

The winning team will receive iPad HDs - a representative from your team must be present on Friday during closing remarks in order to win!

Have fun, compete and win an iPad!

About the Dragon Research Group (DRG)

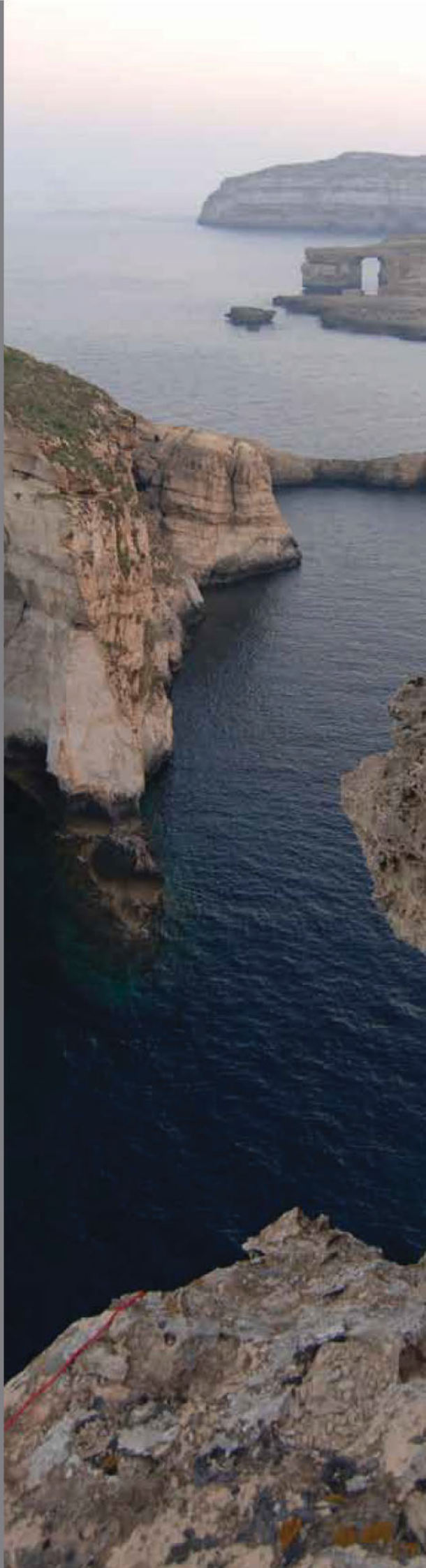
The DRG is a volunteer security research organization comprised of a geographically dispersed set of trusted volunteers who are passionate about making the Internet more secure. The DRG produces and supports open source security-related tools, analysis and free non-commercial insight for the Internet community. Join us and help make it all happen. Visit our website at http://www.dragonresearchgroup.org.

Follow us on Twitter @dragonresearch!

DRG

DragonResearchGroup.org

Here Be Dragons



DRG

DragonResearchGroup.org

The DRG Challenge

FIRST 24 CONFERENCE 2012

For more information, simply visit:

www.dragonresearchgroup.org/FIRST2012

schedule at-a-glance.

	Morning	Afternoon	Evening
Saturday 16 June 2012	**FIRST Education & Training Committee** — 09:00-16:30 (Perrellos - CC5)		
Sunday 17 June 2012	**FIRST Education & Training Committee** — 09:00-13:30 (Perrellos - CC5) **Becoming a Better Trainer** — 14:00-16:30 (Perrellos - CC5)		
		Registration — 14:00-18:00 (Spinola Lobby - CC5) *full* **Late Registration** — 18:30-21:00 (Outside Poolside Gazebo - Hilton) *just name badges* **Session Chairs Meeting** — 15:00-16:00 (Wignacourt - CC5) **Newbie Reception** — 18:30-19:00 (Outside Poolside Gazebo - Hilton) **Ice Breaker Reception** — 19:00-21:00 (Outside Poolside Gazebo - Hilton)	
Monday 18 June 2012	**Registration** — 08:00-16:00 (Spinola Lobby - CC5) **Challenge HQ & Geek Lounge** — 10:00-17:00 (Vilhena & Wignacourt Lobby - CC6)		
	Hilton Breakfast* 07:00-09:15 (Oceana Restaurant) **Morning Coffee Service*** 08:00-09:15 (Spinola Lobby - CC5) **Opening, Keynote & Plenary** 09:15-12:00 (Grandmaster Suite - CC6) **Networking Break** 10:45-11:15 (Lobbies - CC5 & CC6)	**Lunch** 12:00-13:30 (Spinola Suite - CC5) **Deep Technical Dives** 13:35-17:30 (Portomaso I+II - Hilton L3) **Technical Foundations** 13:35-17:30 (Grandmaster Suite - CC6) **Policy & Management** 13:35-17:30 (Portomaso III - Hilton L3)	**CVSS SIG** 15:00-17:00 (Vilhena - CC6) **Networking Break** 15:15-15:45 (Lobbies - CC5 & CC6)
Tuesday 19 June 2012	**Registration** — 08:00-16:00 (Spinola Lobby - CC5) **Challenge HQ & Geek Lounge** — 10:00-17:00 (Vilhena & Wignacourt Lobby - CC6)		
	Hilton Breakfast* 07:00-09:30 (Oceana Restaurant) **FIRST Business Plan, Budgeting & Compilations Reporting** 07:00-09:00 (Grandmaster Suite - CC6) **Morning Coffee Service*** 08:00-09:30 (Spinola Lobby - CC5) **Opening & Plenary** 09:30-12:00 (Grandmaster Suite - CC6) **Networking Break** 10:45-11:15 (Lobbies - CC5 & CC6)	**Lunch** 12:00-13:30 (Spinola Suite - CC5) **Deep Technical Dives** 13:35-17:35 (Portomaso I+II - Hilton L3) **Technical Foundations** 13:35-17:35 (Grandmaster Suite - CC6) **Policy & Management** 13:35-17:35 (Portomaso III - Hilton L3) **CVSS SIG** 15:00-17:00 (Vilhena - CC6) **Networking Break** 15:20-15:50 (Lobbies - CC5 & CC6)	**Metrics SIG** 17:30-19:30 (Vilhena - CC6) **Vendor Showcase & Networking Reception** 18:00-20:00 (Lobbies CC5 & CC6)
Wednesday 20 June 2012	**Registration** — 08:30-16:00 (Spinola Lobby - CC5) **Challenge HQ & Geek Lounge** — 10:00-17:00 (Vilhena & Wignacourt Lobby - CC6) **Exhibits** — 08:30-17:30		
	Hilton Breakfast* 07:00-09:30 (Oceana Restaurant) **Morning Coffee Service*** 08:30-09:30 (Spinola Lobby - CC5) **LECC SIG** 08:30-09:30 (Vilhena - CC6) **Opening, Keynote & Plenary** 09:30-12:00 (Grandmaster Suite - CC6) **Networking Break** 10:45-11:15 (Lobbies - CC5 & CC6)	**Lunch** 12:00-13:30 (Spinola Suite - CC5) **Vendor SIG** 13:00-15:00 (Vilhena - CC6) **Deep Technical Dives** 13:35-15:10 (Portomaso I+II - Hilton L3) **Technical Foundations** 13:35-15:10 (Grandmaster Suite - CC6) **Policy & Management** 13:35-15:10 (Portomaso III - Hilton L3) **CVSS SIG** 15:00-17:00 (Vilhena - CC6) **Networking Break** 15:15-15:45 (Lobbies - CC5 & CC6) **Lightning Talks** 15:50-17:30 (Grandmaster Suite - CC6)	**Conference Banquet** 18:15-18:30 Load Buses to Mdina 19:00-20:00 Tour of Mdina & Cocktail Reception 20:15-23:00 Banquet Dinner & Entertainment 22:00-23:15 Buses back to Hilton Malta
Thursday 21 June 2012	**Registration** — 08:30-16:00 (Spinola Lobby - CC5) **Challenge HQ & Geek Lounge** — 10:00-17:00 (Vilhena & Wignacourt Lobby - CC6) **Exhibits** — 08:30-17:30		
	Hilton Breakfast* 07:00-09:30 (Oceana Restaurant) **Morning Coffee Service*** 08:00-09:30 (Spinola Lobby - CC5) **Opening & Plenary** 09:30-12:00 (Grandmaster Suite - CC6) **Networking Break** 10:45-11:15 (Lobbies - CC5 & CC6)	**Lunch** 12:00-13:30 (Spinola Suite - CC5) **Deep Technical Dives** 13:35-15:10 (Portomaso I+II - Hilton L3) **Technical Foundations** 13:35-15:10 (Portomaso III - Hilton L3) **Policy & Management** 13:35-15:10 (Grandmaster Suite - CC6)	**CVSS SIG** 15:00-17:00 (Vilhena - CC6) **Networking Break Non-Members** 15:15-16:15 (Lobbies - CC5 & CC6) **AGM - Members Only** 15:30-17:30 (Grandmaster Suite - CC6)
Friday 22 June 2012	**Registration** — 08:30-16:00 (Spinola Lobby - CC5) **Exhibits** — 08:30-16:00		
	Hilton Breakfast* 07:00-09:30 (Oceana Restaurant) **Morning Coffee Service*** 08:00-09:30 (Spinola Lobby - CC5) **Opening & Plenary** 09:30-12:00 (Grandmaster Suite - CC6) **Networking Break** 10:45-11:15 (Lobbies - CC5 & CC6)	**Lunch** 12:00-13:30 (Spinola Suite - CC5) **Deep Technical Dives** 13:35-16:30 (Portomaso I+II - Hilton L3) **Technical Foundations** 13:35-16:30 (Portomaso III - Hilton L3) **Policy & Management** 13:35-16:30 (Grandmaster Suite - CC6)	**Networking Break Non-Members** 15:15-16:15 (Lobbies - CC5 & CC6) **Closing Remarks** 16:35-17:00 (Grandmaster Suite - CC6)

* See page 4 for attendee breakfast information.

security is not an island.

A Word From Jose, Program Chair 2012

"For this year's conference, I wanted to focus on networking organizations to address security challenges through talks, panels and sessions devoted to collaboration and data sharing, cooperating efforts and new models. As always, we also keep an eye on emerging threat areas including malware, SCADA, targeted attacks, and new attack vectors.

Our program is designed, just as in years past, to provide insights into the best practices your colleagues from around the world have to offer. We have a great line-up of speakers, including keynote presentations from Francisco Garcia-Moran from the European Commission, Suleyman Anil from NATO, and Lance Spitzner from Securing the Human and the Honeynet Project.

Malta's history can serve to highlight the role of security in modern networking: a bridge between organizations, a beachhead that must be defended, and, in our FIRST community, a global community. This is a fitting setting for our networking challenges in the 21st century.

I look forward to this week and to making those human connections that provide the most value in securing our networks."

Jose Nazario, Ph.D
2012 Program Chair, FIRST.Org, Inc.
Senior Manager of Security Research, Arbor Networks

About Jose...

Dr. Jose Nazario is a Senior Manager of Security Research with Arbor Networks. In this capacity, he is responsible for analyzing burgeoning Internet security threats, reverse engineering malicious code, software development, and developing security mechanisms that are then distributed to Arbor's Peakflow platforms via the Active Threat Feed (ATF) threat detection service.

Dr. Nazario's research interests include large-scale Internet trends such as reachability and topology measurement, Internet-scale events such as distributed denial of service (DDoS) attacks , botnets and worms, source code analysis tools, and data mining. He is the author of the books "Defense and Detection Strategies against Internet Worms" and "Secure Architectures with OpenBSD." He earned a Ph.D. in biochemistry from Case Western Reserve University in 2002. Prior to joining Arbor Networks, he was an independent security consultant. Dr. Nazario regularly speaks at conferences worldwide, with past presentations at CanSecWest, PacSec, Blackhat, and NANOG.

About the Theme...

The field of information security is a large mosaic of technical, procedural and physical controls that seeks to protect the confidentiality, integrity and availability of data. Security, however, is not an island unto itself. It must co-exist and collaborate with application developers, cloud computing environments and mobile platforms, not to mention regulatory compliance and law enforcement needs.

The 24th Annual FIRST Conference seeks to bridge this gap by focusing on the practical aspects of security and incident response in the face of a rush toward adoption of cloud computing and other distributed architectures. Considering the inroads that mobile devices are making in our daily workplaces, perhaps it is time for security to redefine itself in some fundamental ways.

About the Program...

Deep Technical Foundations

Presentations cover in depth, cutting edge information on threats, tools and practices.

Technical Foundations

Presentations cover technical information fundamentals and an overview of technical topics.

Policy & Management

Presentations cover incident response management and development, and issues regarding information sharing and legal boundaries.

Lightning Talks

Lightning Talks are open to all attendees. Talks are limited to five minutes each and participants must sign-up at the registration desk. First come, first served. This session is immensly popular—please don't wait to sign up! Slides are not mandatory; ***no sales presentations***.

floor plans–conference center.

LEVEL 5

LEVEL 6

floor plans–hilton malta.

*Please follow signs to get from the Hilton Portomaso Rooms to the Conference Center.

conference program.

SATURDAY, 16 JUNE 2012

09:00-16:30 Perrellos CC5	**Education & Training Committee Meeting** Open meeting

SUNDAY, 17 JUNE 2012

09:00-13:30 Perrellos CC5	**Education & Training Committee Meeting** Open meeting
14:00-16:30 Perrellos CC5	**Becoming a Better Trainer** Open meeting
14:00-18:00 Spinola Lobby CC5 **18:30-21:00** Hilton Poolside Gazebo	**Registration** Full registration will close promptly at 18:00 and "late" registration will open outside the entrance of the Hilton Poolside Gazebo for Sunday evening events. Attendees that come for "late" registration will receive their name badges and can pick up their conference bag & shirts Monday morning. ***Badges are required for entry to all events and sessions.***
18:30-19:00 Hilton Poolside Gazebo	**Newbie Welcome Reception w/ FIRST Steering Commitee** All first time attendees (members & non-member) are cordially invited to mix and mingle at this pre-event with the FIRST Steering Committee, Membership Commitee and Secretariat Staff. Beverages and appetizers will be served.
19:00-21:00 Hilton Poolside Gazebo	**Ice Breaker Reception** All conference attendees are welcome & invited to kick-off the 24th Annual FIRST Conference at a networking reception. Beverages and appetizers will be served.

MONDAY, 18 JUNE 2012

General Session	
09:15-09:45 Grandmaster Suite CC6	**Conference Opening & Welcome Remarks** ***Chris Gibson**, Chair, FIRST.Org, Inc. & Director, Citi, UK* **Special Guest Remarks** ***The Hon. Austin Gatt**, LL. D., M.P., Minister for Infrastructure, Transport and Communications, Malta*
09:45-10:45 Grandmaster Suite CC6	**Keynote Presentation | IT Security @ EC: Challenges & Experiences** ***Francisco García Morán**, Directorate General Informatics (DIGIT), European Commission* Trust and Security is one of the key areas of work in the Digital Agenda for Europe, one of the 7 flagship initiatives launched by the Commission in the framework of EU2020, the EU initiative for smart, sustainable and inclusive growth. It is in this framework that the European Commission proposes, develops and implements its IT security policies including the internal ones. This presentation will describe the framework in which the internal IT security initiatives are carried out and the challenges ahead. It will also describe how the policies are implemented internally, will present some of the tools used, and will describe some experiences in dealing with security incidents on the ground.
10:45-11:15 Main Lobbies CC5&6	**Networking Break**
11:15-12:00 Grandmaster Suite CC6	**Plenary | The DigiNotar Crisis: from incident response to crisis coordination** ***Aart Jochem**, Manager Security Team, NCSC-NL* Get behind the scene insights into handling the DigiNotar incident, from hack to national crisis. What happened, how did this impacted our operations and which lessons can be learned? DigiNotar was an important certificate service provider for the Dutch governmental PKIOverheid. The

MONDAY, 18 JUNE 2012 (continued)

	report of a fraudulent certificate issued by DigiNotar came as a bombshell to GOVCERT.NL. The seriousness of the situation was clear immediately, though the real impact on Dutch society became apparent later that week. Aart will present the chain of events which led from the report from CERT Bund to the management takeover of DigiNotar by the government.		
12:00-13:30 Spinola Suite CC5	**Lunch**		
Breakouts	**Deep Technical Dives** Portomaso I+II Hilton Level 3	**Technical Foundations** Grandmaster Suite CC Level 6	**Policy & Management** Portomaso III Hilton Level 3
13:35-14:20	**Poison Ivy for Incident Responders** ***Andreas Schuster*** *Senior Computer Forensic Examiner, Deutsche Telekom AG, DE*	**Who, What, Where and How: An Insider's View to Participating in the Security Community** ***John Kristoff*** *Researcher, Team Cymru, US*	**Leaving our island: a communication and business strategy for a National CSIRT** ***Christian Van Heurck*** *Team Leader - Coordinator, CERT.be, BE*
14:24-15:10	**DQ: a cyber missile** ***Vitaly Kamluk*** *Chief Malware Expert, Kaspersky Lab, RU* ***Costin Raiu*** *Director, Global Research & Analysis Team, Kaspersky Lab, RO*	**Team Cymru: Services for CERTs** ***Jacomo Piccolini*** *Security Evangelist, Team Cymru, BR*	**A study for CSIRTs strengthening: From a Viewpoint of Interactive Storytelling in an Organization** ***Ikuya Hayashi*** *Senior Researcher, NTT, JP*
15:00-17:00 Vilhena CC6	**Common Vulnerability Scoring System Special Interest Group (CVSS SIG)** *Open to all attendees; voting is restricted. Contributers must sign an IPR.		
15:15-15:45 Main Lobbies CC5&6	**Networking Break**		
15:50-16:20	**A forensic review of the TDSS bootkit** ***Tim Slaybaugh*** *Digital Analytics, General Dynamics, US-CERT, US*	**Securing the Internet Inter-Domain Routing System using Origin Validation and the RPKI** ***Carlos Martinez-Cagnazzo*** *R+D Engineer, LACNIC, UY*	**DNS-CERT: vision and reality for delivering a secure and healthy naming service** ***Igor Nai Fovino*** *Head of the Research Division, Global Cyber Security Center, IT*
16:25-16:55	**Stepping into the Carberp crimekit and reshipping business** ***Peter Kruse*** *Partner & Security Specialist, CSIS Security Group, DK*	**Phisherman's foes** ***Jean-Michel Doan*** *Cybercrime Analyst, LEXSI, FR* ***Vincent Hinderer*** *Cybercrime Analyst, LEXSI, FR*	**Putting Adobe on the MAPP with Microsoft** ***David Lenoe*** *Group Manager, PSIRT, Adobe Systems, US*
17:00-17:30	**Pinkslipbot: A deep look at how malicious code adapt and evolve** ***Guilherme Venere*** *Malware Researcher, McAfee, BR*	**Insight Into Russian Black Market** ***Almantas Kakareka*** *CTO, Demyo, Inc., US*	**CERT coaching in (own) practice—case studies and roads into the future** ***Przemek Jaroszewski*** *Senior Security Specialist, CERT Polska / NASK, PL*

conference program.

TUESDAY, 19 JUNE 2012

General Session			
07:00-09:00 Grandmaster Suite CC6	**FIRST Business Plan, Budgeting and Compilations Reporting** Open to all attendees. Members are encouraged to attend.		
09:30-09:45 Grandmaster Suite CC6	**Opening Remarks** ***Chris Gibson**, Chair, FIRST.Org, Inc. & Director, Citi, UK*		
09:45-10:45 Grandmaster Suite CC6	**Plenary | A CERT for the European Institutions** ***Freddy Dezeure**, DG INFSO, Head of CERT Pre-Configuration Team, CERT-EU* Cyberthreats are becoming ever more frequent and sophisticated. In the European Digital Agenda, the European Commission has proposed several initiatives to tackle these threats in a more effective manner. In particular the European Digital Agenda foresees two actions regarding the setting up of national CERTs and the improvement of the cooperation between national CERTs. The CERT-EU Pre-configuration Team is a key component to delivering these two actions. The presentation will cover the status and perspectives of CERT-EU.		
10:45-11:15 Main Lobbies CC5&6	**Networking Break**		
11:15-12:00 Grandmaster Suite CC6	**Plenary | Remediation of Malware at the Country Level: A Case Study** ***Jean-Christophe Le Toquin**, Director Digital Crimes Unit, Microsoft Europe Middle-East & Africa, FR* In my talk at FIRST 2011, I detailed remediation efforts associated with takedowns of the Waledac and Rustock botnets. I talked about the partnership with ISPs that enabled this and the tactics being utilized to share data and tools to better target infected machines. I also raised a challenge... for a CERT to work towards the eradication of malware in their country. I had several CERTs approach me to discuss this type of work. In this talk, I will detail the work we have undertaken, the protocol by which we propose such work to be effective, as well as challenges and progress to date.		
12:00-13:30 Spinola Suite CC5	**Lunch**		
Breakouts	**Deep Technical Dives** Portomaso I+II Hilton Level 3	**Technical Foundations** Grandmaster Suite CC Level 6	**Policy & Management** Portomaso III Hilton Level 3
13:35-14:05	**Advances in Passive DNS Replication** ***Eric Ziegast*** *SIE Programme Manager, Internet Systems Consortium (ISC), US*	**Injecting APT Response Into Your CSIRT Processes** ***Jeff Boerio*** *Sr. Information Security Specialist, Intel Corporation, US*	**Botnet Free Switzerland** ***Michael Hausding*** *Security Engineer, SWITCH-CERT, CH* ***Philippe Rütsche*** *Head of Abuse & Security Operations, Swisscom, CH*
14:10-14:40	**Anomaly Detection Through DNS Correlation** ***Michael H. Warfield*** *Senior Security Research & Threat Analyst, IBM Corporation, US*	**Combating APTS with NetFlow** ***Christopher Smithee*** *Network Security Manager, Lancope, Inc., US*	**Project MARS** ***Jean-Christophe Le Toquin*** *Director Digital Crimes Unit, Microsoft Europe Middle-East & Africa, FR*

TUESDAY, 19 JUNE 2012 (continued)

Breakouts	Deep Technical Dives Portomaso I+II Hilton Level 3	Technical Foundations Grandmaster Suite CC Level 6	Policy & Management Portomaso III Hilton Level 3
14:45-15:15	**Where automation ends and people begin—One CSIRT's journey replacing a SIEM with logging** ***Gavin Reid*** *Senior Manager, CSIRT, Cisco Systems, US* ***David Schwartzburg*** *Security Engineer/Incident Manager, Cisco Systems, US*	**Incident response in large complex business environments** ***Ramses Martinez*** *Director of Security, Yahoo!, US* ***Ismail Guneydas*** *Team Lead e-Crime Investigation, Yahoo!, US*	**DNS Filtering and Firewalls—Pancea for network protection or the cause of the Internet Balkanization?** ***Rod Rasmussen*** *President & CTO, Internet Identity, US*
15:00-17:00 Vilhena CC6	**Common Vulnerability Scoring System Special Interest Group (CVSS SIG)** *Open to all attendees; voting is restricted. Contributers must sign an IPR.		
15:20-15:50 Main Lobbies CC5&6	**Networking Break**		
15:55-16:25	**Cryptanalysis of malware encrypted output files** ***Nelson Uto*** *Information Security Consultant, CPqD, BR*	**Operation black tulip: Certificate authorities lose authority** ***Marnix Dekker*** *Application Security Officer, ENISA*	**CSIRTs are to Product Security as Ferries are to Islands** ***Erka Koivunen*** *Head of CERT-FI, Finnish Communications Regulatory Authority, FI* ***Anu Puhakainen*** *Head of PSIRT, Ericsson, FI*
16:30-17:00	**Further aspects of passive DNS: datamining, visualization and alterantive implementations** ***Alexandre Dulaunoy*** *Incident Management, CIRCL.lu* ***David Durvaux*** *Security Analyst, CERT.be / Belnet* ***L. Aaron Kaplan*** *Senior Security Analyst, CERT.at* ***Sebastian Tricaud*** *Chief Technology Officer, Picviz, FR*	**Engineering Solutions for Incident Investigations and Detection** ***Martin Nystrom*** *Manager, CSIRT Architecture, Cisco Systems, US*	**Cross-Organizational Incident Handling: An evolved process model for improved collaboration** ***Thomas Millar*** *Chief of Communications, US-CERT, US*
17:05-17:35	**CERT-GIB: Efficient mitigation of Phishing, Malware and Botnet activity within a ccltd** ***Alex Kuzmin*** *Head of CERT-GIB, RU*	**National Disinfection Case Study** ***Mounir Kamal*** *Incident Handling and Digital Forensics Section Manager, QCERT, QA*	**Sharing Crime Data Across International Frontiers** ***Patrick Cain*** *Resident Research Fellow, APWG, US*
17:30-19:30 Vilhena CC6	**Metrics Special Interest Group (Metrics SIG)**		
18:00-20:00 Main Lobbies CC5&6	**Vendor Showcase**		

conference program.

WEDNESDAY, 20 JUNE 2012

08:30-09:30 Vilhena CC6	**Law Enforcement/CSIRT Co-operation Special Interest Group (LECC SIG)**		
General Session			
09:30-09:45 Grandmaster Suite CC6	**Opening Remarks** ***Chris Gibson**, Chair, FIRST.Org, Inc. & Director, Citi, UK*		
09:45-10:45 Grandmaster Suite CC6	**Keynote Presentation | Defending Cyberspace—Global Challenges Require Global Responses** ***Suleyman Anil**, Head, Cyber Defence/Emerging Security Challenges Division, NATO* The Third Millennium started by witnessing Cyberspace being added, as a new global domain, to the natural domains of open seas, air and space. Mankind have always progressed by taking advantages of opportunities offered by the open seas, air or by space. Yet the opportunities offered by Cyberspace are unprecedented; both in scope and in speed. Third millennium will benefit those who knows how to utilize the cyberspace better. On the other hand, unprecedented opportunities offered by cyberspace require protection. Piracy in open seas took centuries to cease (well, almost). We need to move much faster in Cyberspace to respond to the cyber threats which are global in nature. Global threats can only be countered by global measures. In the multi-stake holder nature of Cyberspace, we all have shared responsibilities to make the cyberspace a safer global domain. Currently the most important shortcoming in defending against cyber threats is the lack of international cooperation. Through its 28 Member Nations and 40 Partner Nations, NATO has been raising awareness and assisting capacity building against global cyber threats at strategic levels. In this decade, international community needs to do better to make sure first that its own cyberspace is kept "hygiene" and secondly to assist others in defending their cyberspace.		
10:45-11:15 Main Lobbies CC5&6	**Networking Break with Exhibits**		
11:15-12:00 Grandmaster Suite CC6	**Plenary | Evolution of white-hat versus botnet takedown interaction** ***David Dagon**, Researcher, Georgia Tech Information Security Center, US* ***Eric Ziegest**, SIE Programme Manager, Internet Systems Consortium, US* Eric and David will present an evolution of white-hat versus botnet takedown interaction and how the working group model is forming to proactively work with law enforcement to go after criminal operators. They will discuss past failures, current failures, and recent successes.		
12:00-13:30 Spinola Suite CC5	**Lunch**		
13:00-15:00 Vilhena CC6	**Internet Infrastructure Vendors Special Interest Group (Vendor SIG)**		
Breakouts	**Deep Technical Dives** Portomaso I+II Hilton Level 3	**Technical Foundations** Grandmaster Suite CC Level 6	**Policy & Management** Portomaso III Hilton Level 3
13:35-14:20	**Cyber Crime & APT Hands On** ***Jeffrey Brown*** *Senior Principal, Cyber Clarity, US* ***Cory Mazzola*** *Operations Manager, General Dynamics, US-CERT, US*	**NorCERT incident handling of targeted attacks** ***Marie Moe*** *Senior Engineer, NorCERT, NO* ***Eldar Lillevik*** *Chief Engineer, NorCERT, NO*	**Legal challenges to information sharing of national/governmental CERTs in Europe** ***Silvia Portesi*** *Expert, ENISA* ***Neil Robinson*** *Research Leader, RAND Europe*

WEDNESDAY, 19 JUNE 2012 (continued)

Breakouts	Deep Technical Dives Portomaso I+II Hilton Level 3	Technical Foundations Grandmaster Suite CC Level 6	Policy & Management Portomaso III Hilton Level 3
14:25-15:10	**CANCELLED SESSION**	**Post-Intrusion Problems: Pivot, Persist and Property** ***Cory Altheide*** *Digital Archaeologist, Google, Inc.* ***Morgan Marquis-Boire*** *Console Cowboy, Google, Inc.*	**The Laws of Large Numbers and The Impact on IT Security** ***Peter Kuper*** *Partner, In-Q-Tel, US*
15:00-17:00 Vilhena CC6	**Common Vulnerability Scoring System Special Interest Group (CVSS SIG)** *Open to all attendees; voting is restricted. Contributers must sign an IPR.		
15:15-15:45 Main Lobbies CC5&6	**Networking Break with Exhibits**		
15:50-17:30 Grandmaster Suite CC6	**Lightning Talks** Lightning Talks are open to all attendees. Talks are limited to five minutes each and participants must sign-up at the registration desk. First come, first served. This session is immensly popular—please don't wait to sign up! Slides are unnecessary; ***no sales presentations***.		
Conference Banquet Schedule			
18:15-18:30 Hilton Lobby	**Conference Attendees Board Buses to Mdina** Please begin to gather in the Hilton Lobby starting at 18:15. We will start boarding attendees on to buses promptly at 18:15 with the final bus leaving at 18:30. *You MUST have your name badge and colored meal card.* *Guests MUST have their name badge and colored meal card.* Tickets will not be transferable the day of the dinner. All ticket transfers must be reported to the conference staff no later than Tuesday at 17:00. We will not be accepting additional guest reservations for dinner onsite. No exceptions. There will be a walking tour. If you foresee any health/physical issues with this, please be sure to talk to the conference staff no later than Tuesday to ensure proper arrangements.		
19:00-20:00 Medievel City of Mdina	**Tour of Mdina & Cocktail Reception** Attendees will be greeted by a master of ceremony and will continue on with a tour of Mdina. Attendees will be treated to a cocktail reception in Bastian Square prior to dinner.		
20:15-23:00 Bacchus Restaurant	**Banquet Dinner & Entertainment** Attendees will be welcomed and escorted to tables. Please have your meal card with you and place your card in front of you and on your plate. Outdoor and indoor seating arrangements will be available.		
23:00-23:15 Bacchus Restaurant	**Buses Back to Hilton Malta**		

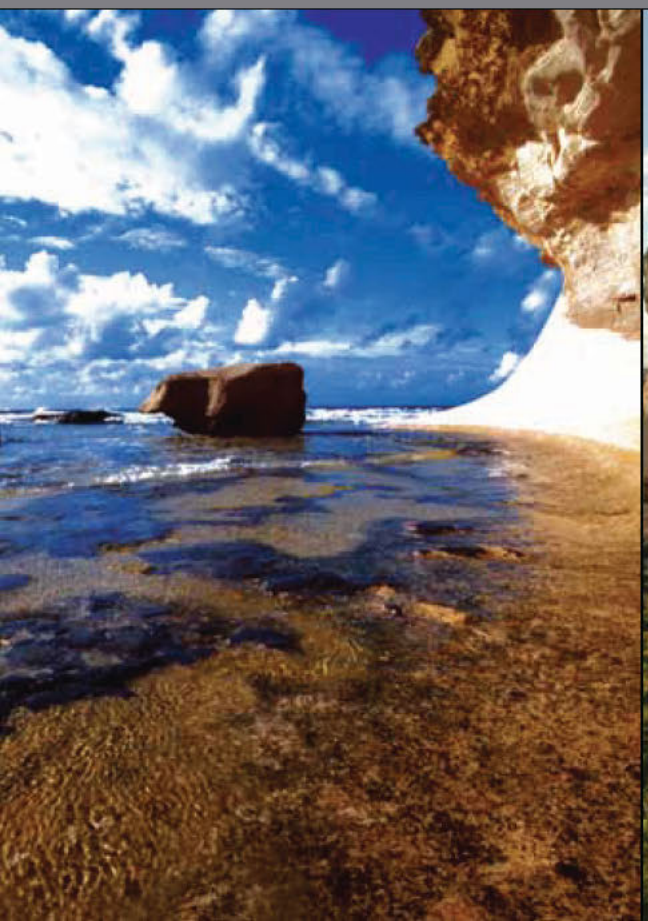
conference program.

THURSDAY, 21 JUNE 2012

General Session			
09:30-09:45 Grandmaster Suite CC6	**Opening Remarks** ***Chris Gibson**, Chair, FIRST.Org, Inc. & Director, Citi, UK*		
09:45-10:45 Grandmaster Suite CC6	**Plenary | Securing Social** ***Chad Greene**, CERT Manager, Facebook, US* ***Ryan McGeehan**, Manager, Security Incident Response, Facebook, US* With over 800 million monthly active users communicating with friends and family, sharing and expressing themselves through online content, Facebook faces a significant set of security threats. In this talk, we'll focus on several threats against our infrastructure and discuss the defensive measures that we've developed to combat them.		
10:45-11:15 Main Lobbies CC5&6	**Networking Break with Exhibits**		
11:15-12:00 Grandmaster Suite CC6	**Plenary | Proactive Detection of Network Security Incidents - A Study** ***Andrea Dufkova**, Expert in Computer Incident and Response Handling Operational Security, ENISA* ***Piotr Kijewski**, Head of CERT Polska, CERT Polska / NASK, PL* The talk is going to cover a recently published ENISA report on the "Proactive Detection of Network Security Incidents." Proactive detection of incidents is the process of discovery of malicious activity in a CERT's constituency through internal monitoring tools or external services that publish information about detected incidents, before the affected constituents become aware of the problem. It can be viewed as a form of early warning service from the constituents' perspective. Effective proactive detection of network security incidents is one of the cornerstones of an efficient CERT service portfolio capability. It can greatly enhance a CERT's operations, improve its situational awareness and enable it to handle incidents more efficiently, thus strengthening the CERT's incident handling capability, which is one of the core services of national / governmental CERTs. The study was largely community driven - it was based on a survey of 45 different CERTs and on input from an security expert group specifically formed for the study, supplemented by the research and knowledge of members of the CERT Polska team and ENISA. Results of the survey will be covered in the presentation.		
12:00-13:30 Spinola Suite CC5	**Lunch**		
Breakouts	**Deep Technical Dives** Portomaso I+II Hilton Level 3	**Technical Foundations** Portomaso III Hilton Level 3	**Policy & Management** Grandmaster Suite Level 6 CC
13:35-14:20	**Honey Spider Network 2.0: detecting client-side attacks the easy way** ***Pawel Pawlinski*** *IT Security Specialist, CERT Polska/ NASK, PL*	**From Zero to CERT in 60 Days** ***Sindri Bjarnason*** *Researcher, CERT-IS, Icelandic National CERT Team, IS*	**Panel: Security Incidents Management within the Government of Malta** ***Martin Camilleri*** *Information Security Specialist, MITA* ***Giovanni Grixti*** *Magistrate, Malta* ***Rodney Naudi*** *Director, MITA* ***Timothy Zammit*** *Police Force Cyber Crime Unit, Malta*

THURSDAY, 21 JUNE 2012 (continued)

Breakouts	Deep Technical Dives Portomaso I+II Hilton Level 3	Technical Foundations Portomaso III Hilton Level 3	Policy & Management Grandmaster Suite Level 6 CC
14:25-15:10	**Overseeing the orchard– Hands-on Tutorial** ***Kenneth van Wyk*** *President, KRvW Associates, LLC, US*	**Feasibility study of scenario based self-training material for incident response** ***Masato Terada*** *Chief Technology and Coordination Designer, Hitachi Incident Response Team, JP*	**Panel: Global and Regional CERT Collaboration to Reduce Cyber Conflict Risk Panel** ***Greg Rattray*** *Partner, Delta Risk LLC, US* ***Yurie Ito*** *Director of Global Coordination, JPCERT/CC, JP* ***Suleyman Anil*** *Head, Cyber Defence/Emerging Security Challenges Division, NATO* ***Yuejin Du*** *Director of National Institute of Network and Information Security, Deputy CTO of CNCERT*
15:00-17:00 Vilhena CC6	**Common Vulnerability Scoring System Special Interest Group (CVSS SIG)** *Open to all attendees; voting is restricted. Contributers must sign an IPR.		
15:15-16:15 Main Lobbies CC5&6	**Networking Break for Non-Members with Exhibits**		
15:30-17:30 Grandmaster Suite CC6	**Annual General Meeting (AGM)** Members-only. Please be on time and have a valid government issued photo ID for entry into meeting. No exceptions. Coffee break will be served in the room		



conference program.

FRIDAY, 22 JUNE 2012

General Session			
09:30-09:45 Grandmaster Suite CC6	**Opening Remarks** ***Chris Gibson**, Chair, FIRST.Org, Inc. & Director, Citi, UK*		
09:45-10:45 Grandmaster Suite CC6	**Keynote | Surviving the World of Security—The Past, Present and Future** ***Lance Spitzner**, Director, SANS Securing the Human Program, SANS Institute, US*		
10:45-11:15 Main Lobbies CC5&6	**Networking Break**		
11:15-12:00 Grandmaster Suite CC6	**Plenary | What we found about BCP on 3/11** ***Takuho Mitsunaga**, Security Analyst, JPCERT/CC. JP* Business Continuity Planning (BCP) was said to be ready for any natural disaster in Japan. In the event of an emergency in a corporate headquarters; satellite offices, backup systems for critical information and disaster recovery plans were all considered ready to go. However after the earthquake on 3/11, we realized that BCP processes were not enough to deal with "REAL" disasters. Responders faced expected problems such as power outages, but were ill-equiped to deal with the unexpected problems...including the human factor. For this presentation, we interviewed enterprises in Japan focusing on BCP to discuss what worked and what did not. Based on our interview results, we will present the BCP processes actioned on 3/11 and discuss what we need for "REAL" BCP.		
12:00-13:30 Spinola Suite CC5	**Lunch**		
Breakouts	**Deep Technical Dives** Portomaso I+II Hilton Level 3	**Technical Foundations** Grandmaster Suite CC Level 6	**Policy & Management** Portomaso III Hilton Level 3
13:35-14:20	**AbuseHelper case studies: Gathering and sharing incident data among different communities** ***Jussi Eronen*** *InfoSec Adviser, CERT-FI, FI*	**Are Cyber Security Exercises Useful? The Malaysian Case Study.** ***Adli Wahid*** *VP Cyber Security Response Services / Head of Malaysia CERT, CyberSecurity Malaysia, MyCERT, MY*	**Visualizing Cybercrime Campaigns using Triage analytics** ***Olivier Thonnard*** *Sr. Research Engineer, Symantec, FR*

conference program.

FRIDAY, 22 JUNE 2012 (continued)

Breakouts	Deep Technical Dives Portomaso I+II Hilton Level 3	Technical Foundations Grandmaster Suite CC Level 6	Policy & Management Portomaso III Hilton Level 3
14:25-15:10	**Sharing data's hard, here's how we did it** ***Wes Young*** *Principal Security Engineer, REN-ISAC, US*	**FS-ISAC—A Private/Public Partnership** ***Kevin Thomsen*** *Senior Vice President, Citi*	**How Visualization Makes it Possible** ***Sebastian Tricaud*** *Chief Technology Officer, Picviz Labs*
15:15-15:45 Main Lobbies CC5&6	**Networking Break**		
15:50-16:30	**Proposal for a new model for information sharing between CSIRTs** ***David Durvaux*** *Security Analyst, CERT.be/Belnet, BE* ***Christian Van Heurck*** *Team Leader, Coordinator, CERT.be/Belenet, BE*	**Automated incident notification helper** ***Javier Berciano*** *Reactive Services Team Leader, INTECO-CERT, ES*	**SCADA Security: The fight to protect critical infrastructure** ***Kevin Hemsley*** *Vulnerability Handling Lead, Idaho National Laboratory, US* ***Ryan Kimmitt*** *Senior Fusion Analyst, Idaho National Laboratory, US*
16:35-17:00 Grandmaster Suite CC6	**Closing Remarks & Raffle Drawings** ***Chris Gibson**, Chair, FIRST.Org, Inc. & Director, Citi, UK*		

keynote speakers.

Francisco García Morán

Director General, Directorate General Informatics (DIGIT)
European Commission

Francisco García Morán holds a degree in Mathematics from the University of Seville and a degree in Computer Science from the Polytechnic University of Madrid. He started his career as a teacher and IT engineer at the University of Seville and worked for several years at the IT Departments of the Ministry of Education and Science at national level and of the Regional Government of Andalusia where he worked as a head of several IT services. Since he joined the European Commission in November 1986, he has continued working in the IT area, first at the Informatics Directorate and then at the Directorate-General for Translation.

In 2001 he was appointed Director of Informatics at the Directorate-General for Personnel and Administration. He was responsible for establishment of the Directorate-General for Informatics (DIGIT) in May 2004 of which he was appointed Director General in November 2005.

The Directorate-General for Informatics defines the IT strategy of the European Commission, provides ICT corporate services and is also responsible for the European programme ISA (Interoperable Solutions for Public Administrations).

He is member of the Management Board of ENISA (European Network and Information Security Agency) and member of World Bank's HLEG (High Level E Transformation Group).

Presenting Monday @ 09:45 "IT Security @ EC: Challenges & Experiences"

Suleyman Anil

Head, Cyber Defence/Emerging Security Challenges Division
NATO

Since August 2010, Mr. Anil is the Head of Cyber Defence Section in the Emerging Security Challenges Division in NATO HQ Brussels. The responsibilities of his section includes development of NATO's policy, action plans and input on Cyber Defence, cyber defence coordination within NATO, with Nations and with International Organizations, organizing Annual Cyber Defence Exercises and provision of cyber threat assessments.

Mr. Anil joined NATO in 1989. Until 2003 he was responsible for the creation and management of NATO's operational Computer Network Defence services (later known as NATO Computer Incident Response Capability; NCIRC) provided from SHAPE HQ in Mons Belgium. In 2003, Mr Anil has moved to NATO Office of Security in NATO HQ Brussels to manage the Coordination Centre of NCIRC, dealing with policy development, international relations and intelligence aspects of cyber defence. Before he joined NATO, Mr. Anil worked for ITT and ALCATEL groups for ten years on various ICT projects in USA and Europe. Mr. Anil, born in 1955 in Turkey, has a degree in Electrical Engineering from METU in Turkey and attended master studies in Computer Science in USA.

Presenting Wednesday @ 09:45 "Defending Cyberspace—Global Challenges Require Global Responses"

keynote speakers.

Lance Spitzner

Director, SANS Securing the Human Program
SANS Institute

Mr. Lance Spitzner is the Training Director of SANS Securing The Human program. He is an internationally recognized leader in the field of cyber threat research and security training and awareness. He has helped develop and implement numerous multi-cultural security awareness programs around the world for organizations as small as 50 employees and as large as 100,000. He invented and developed the concept of honeynets, is the author of several books, and has published over thirty security whitepapers. Mr. Spitzner started his security career with Sun Microsystems as a senior security architect, helping secure Sun's customers around the world. He is founder of the Honeynet Project; an international, non-profit security research organization that captures, analyzes, and shares information on cyber threats at no cost to the public.

Mr. Spitzner has spoken to and worked with numerous organizations, including the NSA, FIRST, the Pentagon, the FBI Academy, the President's Telecommunications Advisory Committee, MS-ISAC, the Navy War College, the British CESG, the Department of Justice, and the Monetary Authority of Singapore. He has consulted around the world, working and presenting in over 20 countries on six different continents. His work has been documented in the media through outlets such as CNN, BBC, NPR, and The Wall Street Journal. He serves on the Distinguished Review Board for the Air Force Institute of Technology, Technical Review Board for CCIED, and the Information Assurance Curriculum Advisory Board at DePaul University. Before working in information security, Mr. Spitzner served as an armor officer in the Army's Rapid Deployment Force and earned his MBA from the University of Illinois-Chicago.

Presenting Friday @ 09:45 "Surviving the World of Security—The Past, Present and Future"

Be a part of FIRST 2013!

The official Call for Speakers occurs every Autumn. Please ensure you watch for our conference announcement emails and news posting for the latest information. All submissions must be made through the FIRST submission form and during the allotted submission window.

Need direction on a presentation topic? Want to join the program committee? Please be sure to talk to the 2013 Program Chair, Adli Wahid, VP of Cyber Security Response Services / Head of Malaysia CERT, CyberSecurity Malaysia (MyCERT) this week. If you'd like an introduction, please do not hesitate to ask the conference staff for assistance.

General Questions: first-2013@first.org
Contact the Program Chair: first-chair2013@first.org

exhibitors.

BT Assure serves the security and business continuity needs of BT's global customers. BT helps these customers manage and maintain resilient and secure networked IT infrastructures. Through its professional services arm, BT Advise, BT offers a full portfolio of security consulting services, covering secure networking, business continuity, and identity and fraud management. For more information, please visit http://www.bt.com/btassure/securitythatmatters.

Secunia is the leading provider of IT security solutions that help businesses and private individuals globally manage and control vulnerability threats and risks across their networks and endpoints. This is enabled by Secunia's award-winning Vulnerability Intelligence, Vulnerability Assessment, and Patch Management solutions that ensure optimal protection of critical information assets. For more information, please visit http://secunia.com.

Cisco is the worldwide leader in networking for the Internet. Its hardware, software, and service offerings are used to create Internet solutions that allow individuals, companies, and countries to increase productivity, improve customer satisfaction and strengthen competitive advantage. Our vision is to change the way people work, live, play and learn. For more information, please visit http://www.cisco.com.

Vodafone Malta is the market leader in the provision of mobile electronic communication services and it is the local provider of choice for high-speed internet bandwidth, hosting and co-location services and international private leased lines. With its very own submarine cable and a high capacity link on another third party subsea cable, Vodafone provides a resilient connection to mainland Europe where multiple international carriers route all traffic to anywhere around the world. For more information, please visit https://www.vodafone.com.mt/ipbandwidth.

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps organizations solve their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments. www.RSA.com.

exhibitors.

Lancope®, Inc. is a leading provider of flow-based monitoring solutions to ensure high-performing and secure networks for global enterprises. Unifying critical network performance and security information for borderless network visibility, Lancope provides actionable insight that reduces the time between problem identification and resolution. For more information, please visit http://www.lancope.com.

Codenomicon develops proactive software security testing and situation awareness tools which find software bugs. Defensics is a fully automatic security testing bundle for over 200 communication interfaces. Situation awareness tools collect, filter and visualize network and abuse information concurrently. Governments, leading software companies, operators, and manufacturers use Codenomicon's solutions. For more information, please visit http://www.codenomicon.com.

FireEye is the only provider that detects and prevents both targeted spear phishing attacks via email as well as web borne APT style, 0-day exploits without relying on signatures for detection. FireEye Malware Protection systems effectively shut down the main vectors of targeted attacks with email and web solutions that perfectly complement traditional and next-generation firewalls (NGFW), IPS, Web gateways and AV solutions. Based in Milpitas, California, FireEye is backed by premier financial partners including the venture capital arm of the CIA, In-Q-Tel. For more information, please visit http://www.fireeye.com.

Verint® Systems Inc. (NASDAQ: VRNT) is a global leader in Actionable Intelligence® solutions and value-added services. More than 10,000 organizations in over 150 countries use our solutions to improve enterprise performance and make the world a safer place. For more information, please visit http://verint.com.

Fidelis Security Systems provides organizations with the network visibility, analysis and control necessary to manage advanced threats and prevent data breaches. Built on a patented Deep Session Inspection®, platform, Fidelis XPS™ is the industry's only network security solution capable of seeing, studying, and stopping advanced threats in real-time by uniquely working at the session-level where today's threats occur.

ValidEdge offers the world's leading anti-malware solution for faster identification and better mitigation against zero day and single target malware attacks. ValidEdge purpose-built anti-malware systems, running on LynuxWorks proprietary secure virtualization, allow you to detect and analyze the most sophisticated and insidious types of malware even when packed and obfuscated. For more information, please visit http://www.validedge.com.

global initiatives.

Special Interest Groups (SIGs)

Special Interest Groups exist to provide a forum where FIRST Members can discuss topics of common interest to the Incident Response community. A SIG is a group of individuals composed of FIRST Members and invited parties, typically coming together to explore an area of interest or specific technology area, with a goal of collaborating and sharing expertise and experiences to address common challenges.

SIG meetings are free to build their own meeting schedule but are also encouraged to co-locate meetings with FIRST Conferences, Technical Colloquia or other events.

SIGs can generate papers and publications for the industry covering their area of interest. While these papers and publications shall be distributed by the FIRST, they do not represent the official position of the FIRST members, or the FIRST itself.

Visit http://www.first.org/global/sigs for more information on SIGs.

SIGs meeting at FIRST 2012.....

Common Vulnereability Scoring System (CVSS-SIG)

FIRST, the worlds leading incident-handling forum, is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs. FIRST sponsors and supports the CVSS-SIG, a diverse group of security professionals who have a keen interest in security vulnerabilities and use CVSS in their daily work. In addition, FIRST hosts a special interest group to update and promote CVSS and provides a central repository for CVSS documentation. Visit http://www.first.org/cvss for more information.

Internet Infrastructure Vendors (Vendor SIG)

The goal of this SIG is to provide forum for Internet Infrastructure Vendors. In this context Internet infrastructure is considered to be Operating Systems, computer hardware, networking equipment and critical applications. This list is by no means exhaustive nor comprehensive.

In order to become a member, applicants must be recognized by, at least, two existing members. Forum moderators have final word in all matters regarding SIG. Membership in FIRST is not a Just aherequirement to become a member of Vendor SIG. Visit http://www.first.org/vendor-sig for more information.

Law Enforcement/CSIRT Co-operation (LECC SIG)

Mission: To further co-operation between Incident Response and Law Enforcement, by the development of better understanding of organisational mission and specific requirements and producing practical trust and information-sharing protocols. Visit http://www.first.org/global/sigs/lecc for more information.

FIRST is the global Forum for Incident Response and Security Teams

About FIRST.Org

FIRST is a premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents by providing access to best practices, tools, and trusted communication with member teams.

Mission Statement

FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs.

.....

Metrics (Metrics SIG)

The scope of the Metrics SIG is to bring together interested members of the FIRST community to discuss and identify approaches for internally evaluating CSIRT and incident management practices within an organization. The work of this SIG focuses on determining further refinements for best practices for CSIRTs (e.g., building off existing metrics work, FIRST materials, ISO 17799, ITIL, NIST, etc.), defining key performance indicators for a team, determining measures for effectiveness, identifying appropriate performance metrics, and determining appropriate approaches for evaluating systems. Visit http://www.first.org/global/sigs/metrics for more information.

FIRST™
Improving Security Together

thank you

2012 Program Chair

Jose Nazario	Arbor Networks, US

2012 Program Committee

Shin Adachi	NTT-CERT, US
Jeff Boerio	Intel, US
Chris Camacho	World Bank, US
Till Dörges	PRESENSE Technologies GmbH, DE
Sherif Hashem	EG-CERT, EG
David Jimenez	CERT-MX, MX
Baiba Kaskina	CERT LV, LV
Piotr Kijewski	CERT Polska / NASK, PL
Jorge Lopez	INTECO-CERT, ES
Rob Lowe	Red Hat, AU
Jacomo Piccolini	Team Cymru, BR
Anu Puhakainen	Ericsson, FI
Jon Ramsey	Dell SecureWorks, US
Hamid Sadiq	Q-CERT, QA
Kevin Thomsen	Citi, US
Marco Thorbruegge	ENISA, EU
Ronaldo Vasconcellos	CAIS/RNP, BR

FIRST Secretariat Staff

NeuStar Secretariat Services

Nora Duhig

Michael Lee

FIRST Conference Staff

Conference & Publication Services, LLC

Phoebe Boelter

Kristen Jacobucci

Brenda Schweda

Traci Wei

FIRST Membership –here's an offer you shouldn't refuse...

....Join FIRST application fee-free at our 2012 Conference

Non-member teams attending FIRST's 24th annual Conference in Malta this June are eligible to waive the $800 per-team application fee if their completed application package is received before December 31, 2012. In addition, whenever you join in 2012, you'll only pay dues for your months of active membership, and not for the entire year.

So why should you join FIRST?

YOU GET ACCESS TO A WORLDWIDE COMMUNITY OF LIKE-MINDED EXPERTS
Computer security incidents respect neither geographical, nor time-zone nor administrative boundaries. Resolving them almost invariably involves input from multiple sites and nations. By working together through FIRST's network, each incident response and security team assists other teams and pools expertise to coordinate the most effective response, providing fast, global solutions.

IT'S A TRUSTED FORUM
Many companies find it difficult to share information. FIRST provides an internationally trusted forum for confidential interactions among incident response and security teams. Interactive assistance is available either on a team-to-team basis (through introductions to teams) or by using the FIRST's infrastructure to share information among all members via secure channels

OUR ANNUALCONFERENCE
The annual FIRST Conference on Computer Security Incident Handling is a unique event. Focused exclusively on the field of computer security incident handling and response, it addresses the global spread of computer networks and the common threats and problems faced by everyone involved - and it's an excellent place to network and to forge alliances and contacts from every continent.

DON'T JUST TAKE OUR WORD FOR IT...
Writing about FIRST, the leading British commentator David Lacey declared in Computer Weekly:
Of all the security clubs and associations, the one that impresses me most is FIRST http://www.first.org/, the Forum for Incident Response and Security Teams. Why? Because it's focused, born out of real business requirements and it's highly selective, i.e. you have to be sponsored and audited to gain membership. FIRST is not a club that exists to make an income for its organizers. It's an international community that serves a real purpose: helping Government, Industry and Academia to respond quickly and effectively to new security threats. So I have no hesitation in recommending that you book a space in your busy diary to attend their Annual Conference.

And the benefits don't stop there...

OUR SYMPOSIA and TECHNICAL COLLOQUIA
FIRST hosts Symposia and Technical Colloquia in different parts of the world throughout the year - providing an exclusive discussion forum for FIRST member teams to share person-to-person the very latest information about vulnerabilities, incidents, tools and all the other issues that affect the operation of incident response and security teams.

BEST PRACTICES, PRESENTATIONS, PODCASTS AND TRAINING MATERIALS
New incident response and security teams can benefit from FIRST membership by improving communication, forming alliances with peer teams and exchanging ideas and best practices. FIRST members have written many papers, presentations and podcasts that you can download from the FIRST members' web site. FIRST also collects coaching materials you can use as part of your in-house training and CERT team start-up resources.

SIGN-UP FOR COMMUNICATIONS AND DISCUSSION LISTS

As we've said, FIRST was created and is run to facilitate communication between incident response and security teams so we can promote prompt and effective resolutions of computer security incidents. As members you can join FIRST discussion lists to keep abreast of the latest intelligence about security incidents, to read and share interesting stories and to become part of a group where you can post your questions, concerns and thoughts for discussion. The collection of teams which comprises FIRST commands expertise covering the widest variety of incident response and security issues, with globally recognized experts intervening to solve problems.

JOIN SPECIAL INTEREST GROUPS

FIRST has several Special Interest Groups [SIGs] which provide round-tables where members can discuss topics of common interest to the Incident Response community. A SIG is a group combining FIRST Members with invited specialists, typically coming together to explore specific technological, social or commercial issues, with a goal of collaborating and sharing expertise and experiences to address common challenges.

Current FIRST Special Interest Groups

- Common Vulnerability Scoring System (CVSS-SIG)
- Internet Infrastructure Vendor (Vendor SIG)
- Law Enforcement/CSIRT Cooperation (LECC-SIG)
- Malware Analysis (MA-SIG)
- Metrics SIG

Don't see a SIG that interests you? Then join and help establish one. Let us know what it is at first-sec@first.org.

So - are you interested in joining FIRST? We hope so...

Please leave your business card or e-mail address and phone number at the registration desk and the FIRST Secretariat will contact you and guide you through the process. You may also contact the FIRST Secretariat at first-sec@first.org.

1. Spend time networking at the conference: you need two sponsoring full FIRST members to apply. But if you're having trouble, let us know and the FIRST Steering Committee will make the introductions for you.
2. FIRST Secretariat Services (FSS) is available to answer your questions at the conference or at first-sec@first.org. FSS can also assign you a shepherd - a member of the FIRST membership committee who will help you and your sponsors through the whole process.
3. Fill out the membership application form that can be found online at www.first.org. Your sponsors will help if there are any problems.
4. Write an application letter stating that you want to join FIRST, and outlining the benefits you can bring the organization.
5. One of your sponsors must conduct a site visit and submit a report. Both sponsors write a letter introducing and recommending the applying team for FIRST full membership. Sponsors must also sign the applying team rep PGP key and team key.
6. Both of the sponsors submit the entire application package to first-sec@first.org.
7. FSS will review the application and post for the members to review. If there are questions, your team will be contacted.
8. The whole application is posted for FIRST member feedback and the FIRST Steering Committee reviews with a recommendation for the membership to welcome you aboard. Once accepted, you will be notified by the SC Chair and sent a dues invoice - ***remember, if you've come to our Malta conference, we'll waive your $800 team application fee, provided the full application is submitted by December 31, 2012.***

*What would **you** like FIRST to address?*

Are we covering all the areas you believe we should be? Are there any areas or subjects that you believe FIRST as an organization should be addressing?

Let us know at first-sec@first.org.

FIRST™
Improving Security Together

note pad

Incident Response:
Sharing to Win

Bangkok, Thailand
16-21 June 2013

25th Annual FIRST Conference
Bangkok June 2013

SAVE THE DATE

FIRST
Improving Security Together

thank you 2012 sponsors

BT

Microsoft

200 YEARS citi

enisa
European Network and Information Security Agency

Secunia
Stay Secure

mita
MALTA INFORMATION TECHNOLOGY AGENCY
TRANSFORMATION · INNOVATION · EXCELLENCE

CISCO

vodafone

DRG
DragonResearchGroup.org
Here Be Dragons

SAP

Google

CIRCL
Computer Incident Response Center Luxembourg

BFK
edv-consulting GmbH
www.bfk.de

HITACHI

facebook

Lancope
Network Performance + Security Monitoring™

CODENOMICON
clarified™

FireEye

RSA

VERINT

FIDELIS
SECURITY SYSTEMS

validEDGE

SYNGRESS.

Hakin9
IT SECURITY MAGAZINE

netsecpodcast.com

EUROTRASH
Security with Funny Accents

www.first.org