Outreaching advanced threats

Towards Intelligence-driven Information Security

Ioannis Askoxylakis
Head of FORTHcert

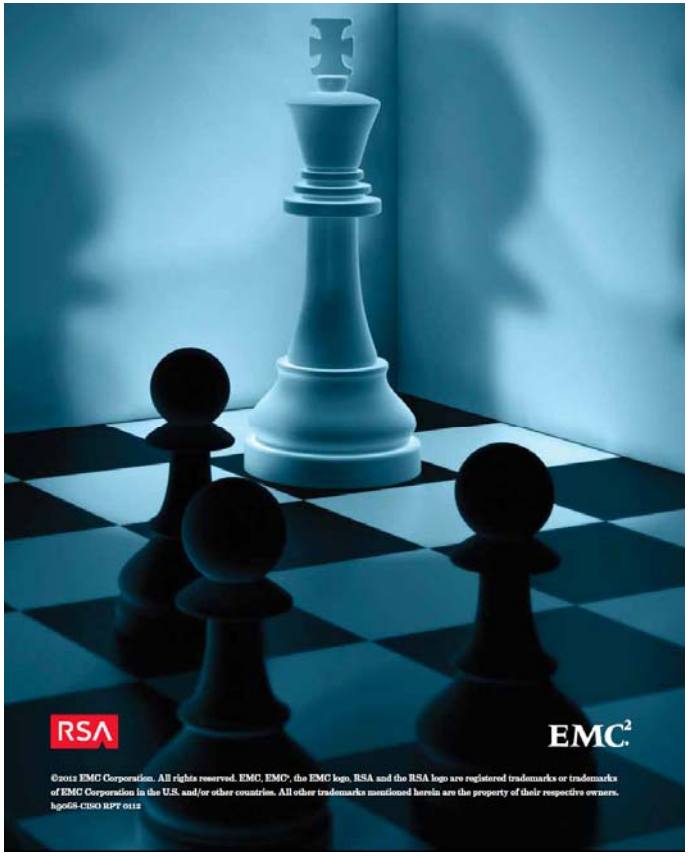
Fraud Prevention Forum

Athens, 5 November 2013

Today's threat landscape

- Open hyperconnected world
  - Mobile computing
  - Cloud computing
  - Social networking
  - Fast adoption of ICT by consumers

- Adversaries are:
  - taking advantage at Gaps in Security
  - moving faster
  - better coordinated
  - developing intelligence
  - easily penetrating traditional perimeter defenses



Security trends

- Risk Management
- Cloud security
- Mobile Security-MDM
- Exploitation of “big data”
- CIIP
- Cyber-physical systems
- SaaS
- CERT-CSIRT
- Consumerization of IT, CYOD, BYOD

Quiz

- It is considered larger than the black market of marijuana, heroin and cocaine combined
- Its size was recently estimated to exceed 1 trillion dollars
- It adversely affected more than 88% of Europeans last year

What is it?

The global market of **cyber crime…**

Time for a new approach

- Consistent collection of reliable data
- Ongoing research on prospective adversaries
- Growth of new skills
- Full visibility into actual conditions
- Efficient processes
- Sharing practices
- Informed risk decisions

Intelligence-driven information security

Definition

Developing real-time knowledge on threats and the organization's posture against those threats in order to prevent, detect and/or predict attacks, make risk decisions, optimize defensive strategies and enable action.

Roadmap to Intelligence-driven Security

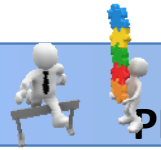
1 **START WITH THE BASICS**

- Inventory of strategic assets
- Incident Response process
- Risk assessment

2 **MAKE THE CASE**

- The value proposition
- Key Stakeholders
- Opportunities for “quick win”

3 **FIND THE RIGHT PEOPLE**



- Train existing
- Hire excellent

4 **BUILD SOURCES**

- Evaluation
- Cost
- Relationships

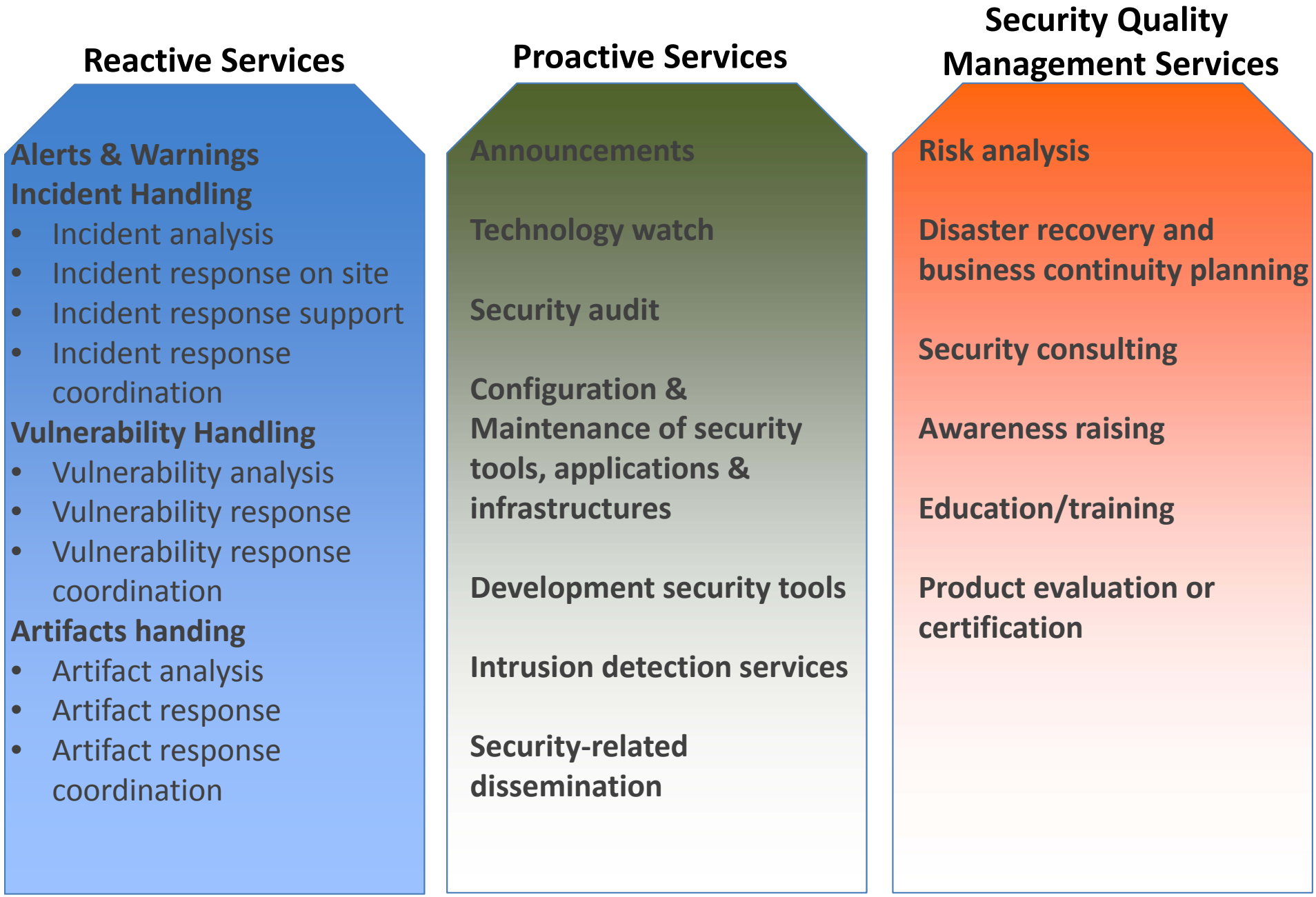
5 **DEFINE A PROCESS**

Take action → Obtain data → Filter data → Perform analysis → Communicate result → Make risk decisions → Take action

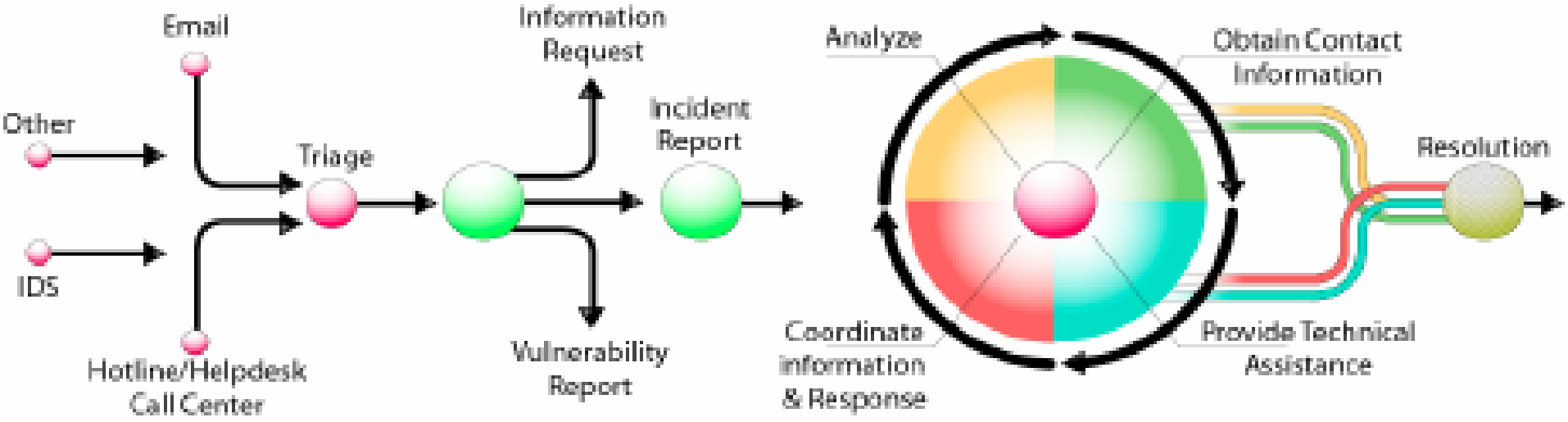
6 **IMPLEMENT AUTOMATION**

- Consumption of threat feeds
- Collections of employees observations
- Log analysis and full packet capture
- Fusion of data from multiple sources

Computer Emergency Response Teams – CERTs



Computer Emergency Response Teams – CERTs



No Organization is an Island

Improving Information sharing is essential

- CSIRT/CERT
- Requirements:
  - Trust
  - Formalized structure
  - Adequate funding
  - Mechanisms, protocols and clear rules
  - Legal framework
  - Standardized procedures
  - Genuine participation

FORTHcert at a glance

Authorized to use CERT, *Jul 2008*

Accredited by TI-TERENA, *Jan 2009*

Accredited by *FIRST, May 2009*

ISO 9001:2000 certified, *Dec 2009*

Certified by TI-TERENA, Oct *2012*

Invest in Cyber Security!

www.itv.com/news/update/2013-01-09/government-invest-650-million-in-cyber-security/ — Government to invest £650 million in cyber security – ITV News

Reader

Google T... | internati... | csis.org/... | Advance... | CERTs by... | Digital A... | Type a word or phrase to search for, or a webpage address, title, or bookmark | ATO an... | Governm... | Announc...

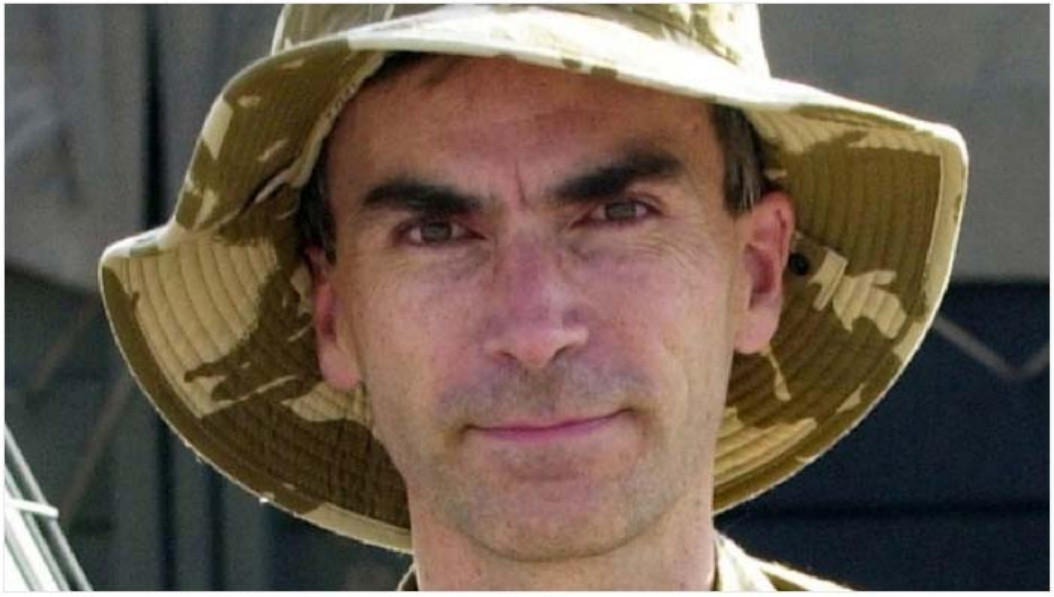
3:34AM, WED 9 JAN 2013 'URGENT' CYBER THREAT TO UK

Government to invest £650 million in cyber security

Last updated Wed 9 Jan 2013

Politics • Defence • Government

Recommend 0 Tweet +1



Surgeon Commander Dr Andrew Murrison Conservative MP for Westbury, on duty at Az Zubayr Port in southern Iraq Credit: David Cheskin/PA Archive

Defence Minister Andrew Murrison has rejected accusations that the Government isn't doing enough to protect cyber security

'Urgent' cyber threat to UK

MPs warn that UK armed forces are so dependent on information technology that their ability to operate could be "fatally compromised" by a cyber attack. The Defence Select Committee urged the Government to "urgently create" a contingency plan.

LATEST ON THIS STORY

3 NEW UPDATES

8:51 AM, WED 09 JAN 2013

Invest in Cyber Security!

www.scmagazine.com/obama-proposes-800m-cyber-budget-increase-for-pentagon/article/288672/ — Obama proposes $800m cyber budget increase for Pentagon - S... Reader

Google... interna... csis.org... Advanc... CERTs... Digital... www.w... ITU - G... nato cy... obama... Obama... Pentag...

Obama proposes $800m cyber budget increase for Pentagon

Despite proposed cuts to defense spending for next fiscal year, the Pentagon will devote more funding to cyber security initiatives – to the tune of an $800 million increase.

President Obama proposed a $3.8 trillion federal budget (PDF) for the 2014 fiscal year, which begins Oct. 1. The U.S. Department of Defense (DoD) would be allocated $4.7 billion for cyber security initiatives, up from $3.9 billion last year. But the overall defense spending plan is $526.6 billion, a $3.9 billion cut from 2013.

Proposed Wednesday, the 2014 budget will be discussed with Congress before being enacted.

Part of the additional funding would help develop

Obama proposes $800m cyber budget increase for Pentagon

Conclusion

“If trees move, he (the enemy) is advancing.”

…….

“Where one can come and go, this is called open ground.”

…….

“On open ground, do not become separated.”

…….

“One who knows the enemy and knows himself will not be in danger in a hundred battles.”

…….

“What enables the enlightened rulers and good generals to conquer the enemy at every move and achieve extraordinary success is foreknowledge.”

…….

“This (Intelligence) is essential for warfare, and what the army depends on to move.”