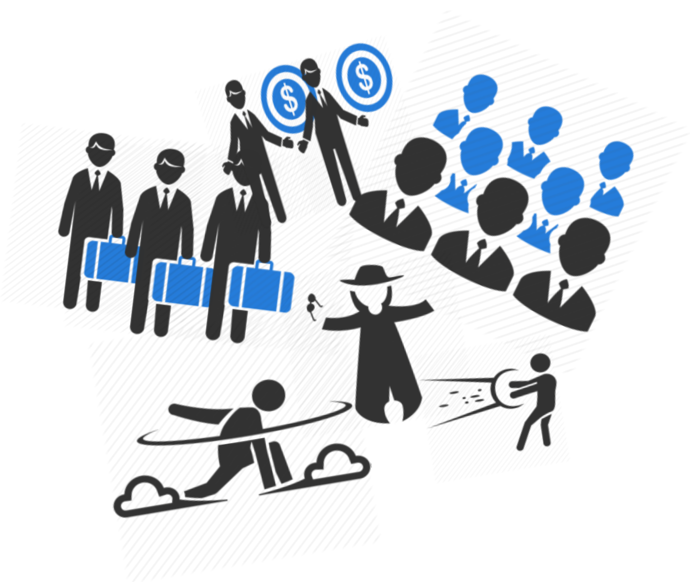
Working group Incident Management and Preparedness

Begin of Year Event 2016

Our Team



14 members

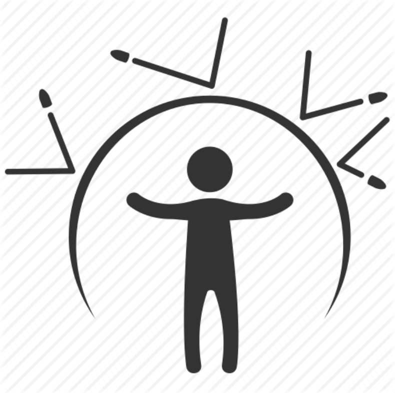
IT sector (security, engineering)
Risk analyst
Auditor
etc.

public and private sector

12 meetings in 2015

Collaboration with Cert.lu

Objectives of collaboration :



Improve the IT security in Luxembourg

.

Keep members up-to-date with current trends

.

Raise awareness and increase pro-activity

.

Align IT security needs to local laws and regulations

.

Review of IMP deliverables

Collaboration with Cert.lu

Common
recommendations
on incident management

A
collaboration
charter

…

Collaboration

…

Inherit
Clusil’s reach
to help
raise security

An
anonymized
incident database
(lessons learned
included)

Collaboration with Isaca

ISACA®

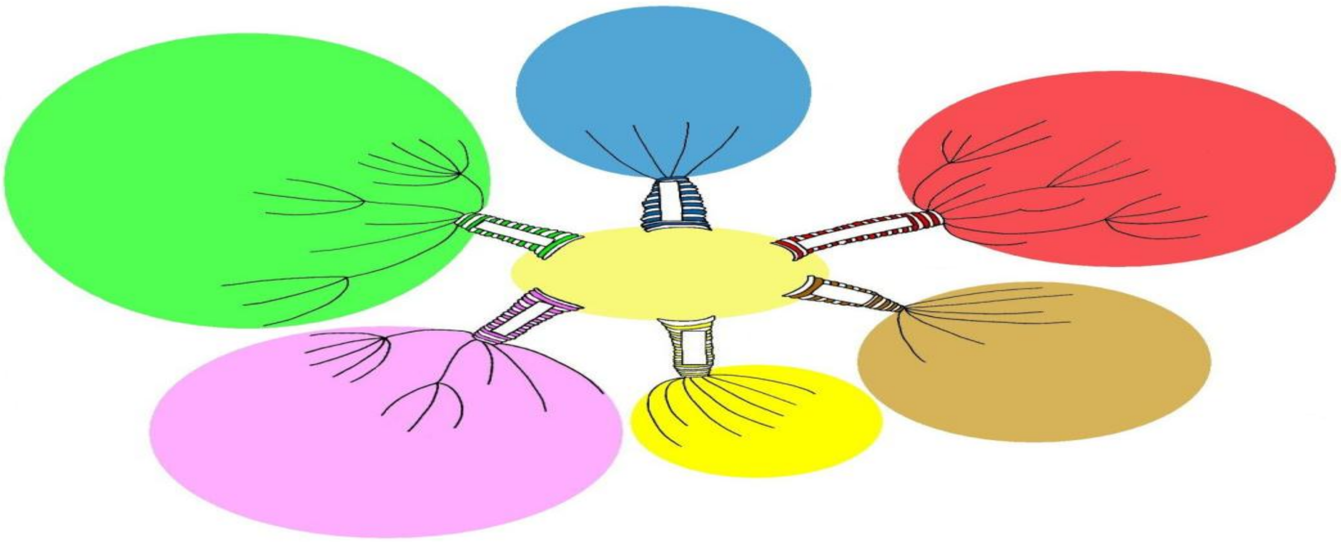
Trust in, and value from, information systems

- Conference Digital Forensics :
  - Police Grand Ducal
  - Private sector
  - 100 attendees
- Objectives for 2016 :
  - Organization of several workshops together

From Wiki/Webdav to Mindmap

- Wiki/Webdav :
  - 3 big parts (preparedness, handling, mitigation)
  - 2 levels of description
  - Too heavy for SMEs with very low IT maturity
- Mindmap :
  - More user-friendly
  - More graphical
  - More practical
  - More checklist/cheat sheet-based
  - More effective to improve maturity

MINDMAP
Steve Muller



© Paul Foreman http://www.mindmapinspiration.com

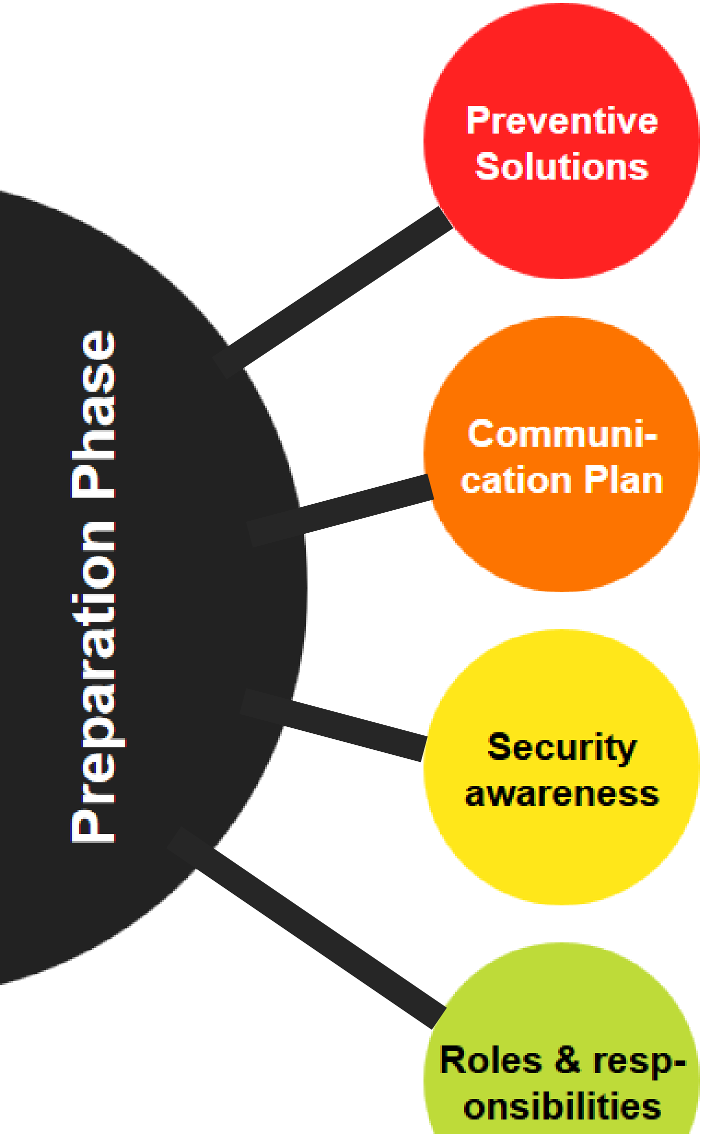
Collection and classification of IMP topics

Section	Title	Point	
		Level 1	Level 2
Plan, prepare, be ready!	Planning (presume known)	1. Risk Management	1. Context Establishment
			2. Risk Assessment
			3. Risk Treatment
		2. Create & manage policies	1. Plan
			2. Do
			3. Check
			4. Act
		3. Acquire management support	1. Support Objectives
			2. Support Procedures
			3. Information security governance and internal controls principles
			4. Submit business case to management for budget approval & delivery
		4. Develop user awareness - Training	1. Training
			2. User
			3. Application
		5. On Governance through Policies, Standards, Procedures and Guidelines	
		6. Build a response capability - BCM	1. Perform a threat assessment
			2. Develop the planning basis
			3. Allocate responsibilities
			4. Present the Emergency Plan
			5. Test the capability
			6. Establish on-going QA, maintenance

Extraction of most important topics

- Preventive Solutions
- Communication Plan
- Security awareness
- Roles & responsibilities
- BCM
- Process & procedures
- Risk management

Mindmap $^{1/2}$



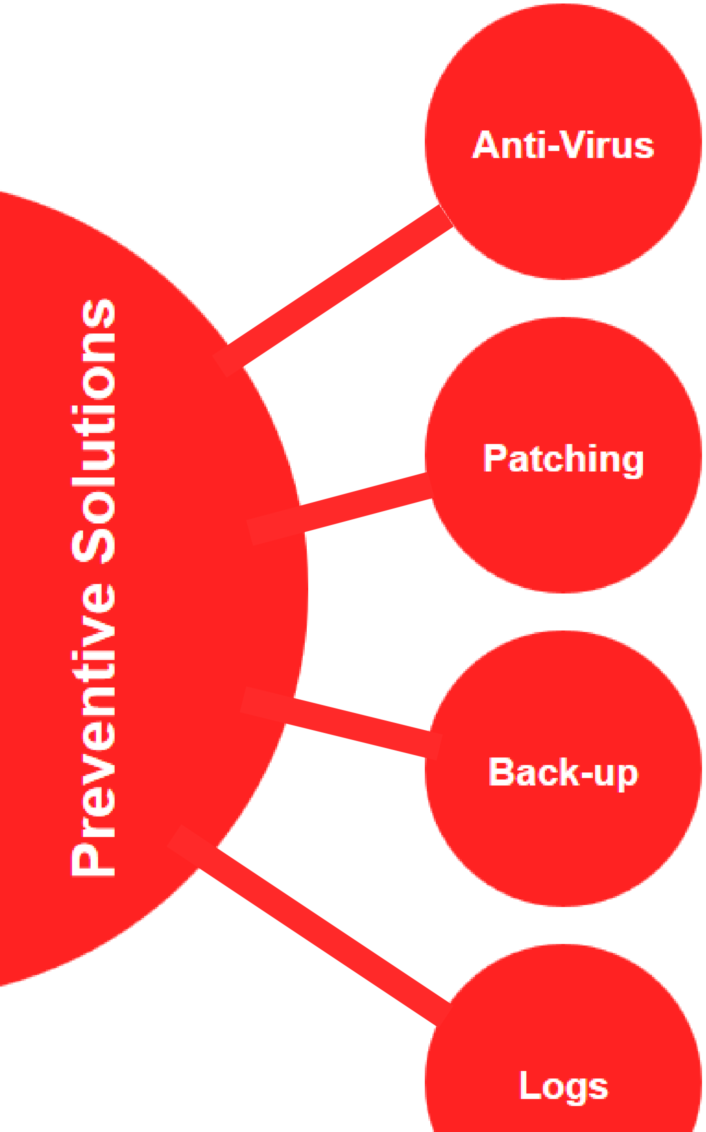
→ Anti-Virus
→ Patching
→ Back-up
→ Logs
→ Firewall

→ Internal
→ External

→ Sub-item 1
→ Sub-item 2
→ Sub-item 3

→ Sub-item 1
→ Sub-item 2
→ Sub-item 3

Mindmap $^{2/2}$



Preventive Solutions

Anti-Virus

- ✓ An anti-virus solution is in place. More information on anti-virus.
- ✓ Signatures are continuously updated.

Patching

- ✓ Computers and user devices (phones...) have automatic updates enabled.
- ✓ Servers and appliances are kept up-to-date (checked by an admin).

Back-up

- ✓ Critical data is replicated at least once (in real-time).
- ✓ Back-ups of all data are created regularly and frequently.

Logs

- ✓ Log files are created on all appliances.
- ✓ Log files can be easily retrieved/inspected.
- ✓ Logs are continously monitored or inspected.

Mindmap: Outlook

- Encode remaining content from wiki
- Translate into FR / EN

Conclusions

- Development of mindmap during the year 2016
- Objective for EOY 2016 : basic cheat sheet for 7 points and related subpoints
- Objective for EOY 2017 : advanced cheat sheet for 7 points and related subpoints
- 3 workshops in 2016
- More members

?
Q
&
A
!

THANK
YOU