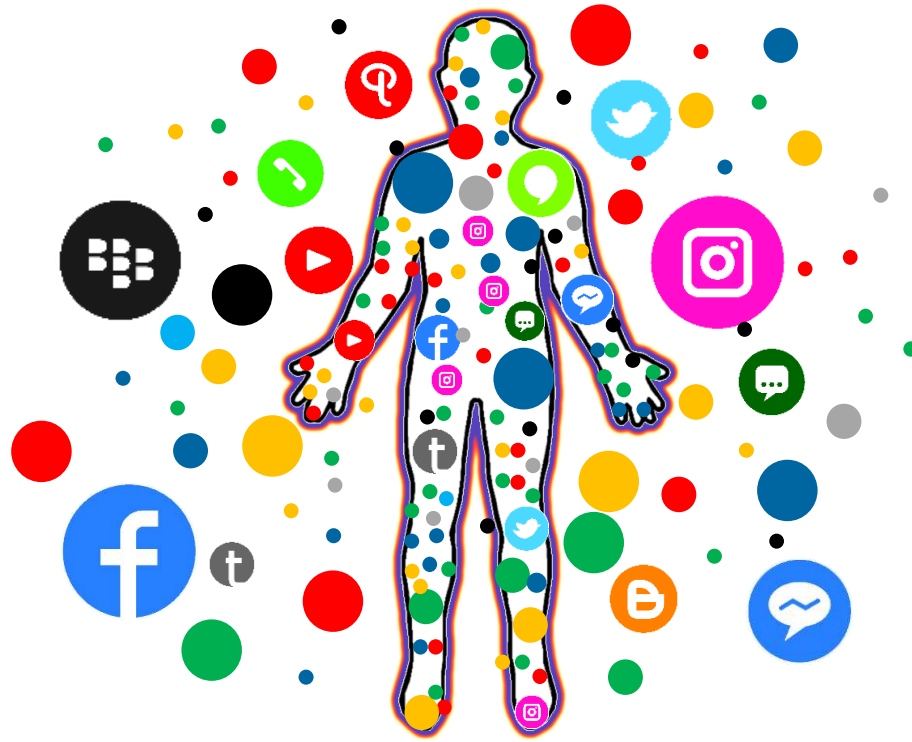


Information Security Days

Prepare for the unknown

2017

You and your data



From IT Security to Cyber Security

In the beginning

The era of IT security is born

- The outside = evil and dangerous
- Building walls based on perimeter security prevention tools
- Ad-hoc approach
- Clueless of insider threat
- Once inside all areas allowed
- Bottom up approach
- Operational



From IT Security to Cyber Security

After a while

Management attention

- Building Security Framework
- Standards on security
- New organizational structure are incorporated into the organization security prevention tools
- Shift from IT to Information
- ISO 2700x wide adopted
- Tactical level



From IT Security to Cyber Security

Some time later

Integrates into corporate governance

- **Attention from the board**
- **Transversal across the organization**
- **Aligned with business expectations**
- **Strategic**
- **Top down**
- **Holistic approach**

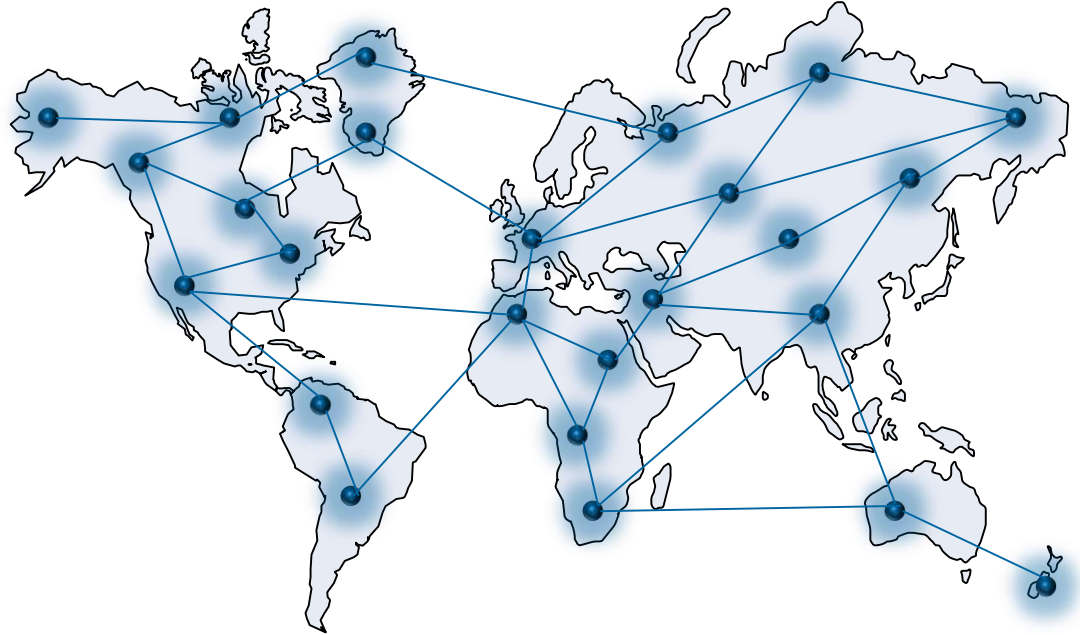


From IT Security to Cyber Security

Today

Transforming to Cyber

- Awareness on all levels of the organization
- Organization ≠ stronghold or fortress
- Agility and flexibility required
- Data outside organization
- Increased number of threats
- Increased complexity



Threats are everywhere

Who and what is threatening us



Threats are everywhere

Business /vs Crime



Dropbox

SaaS



PaaS



IaaS



Staring into the abyss



Addicted to old models and concepts



Concept of known bad

- Identify malicious software
- Technology oriented
- Limited to what is known
- Relies on preventative measures
- Reactive approach
- Build on external knowledge

TALLER WALLS

WON'T SOLVE OUR PROBLEM

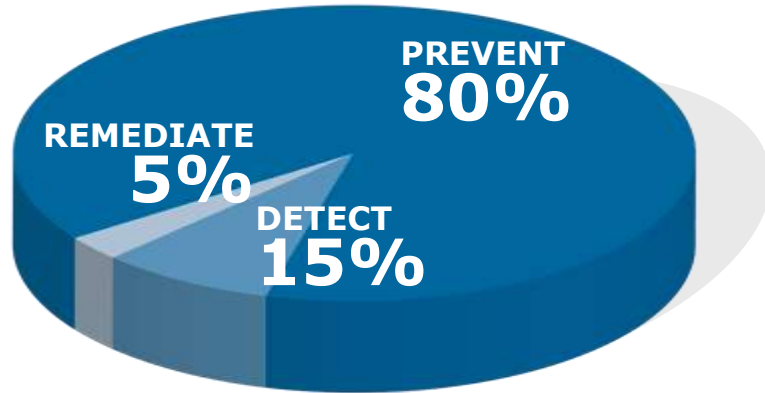


010110
101100111
110100
11

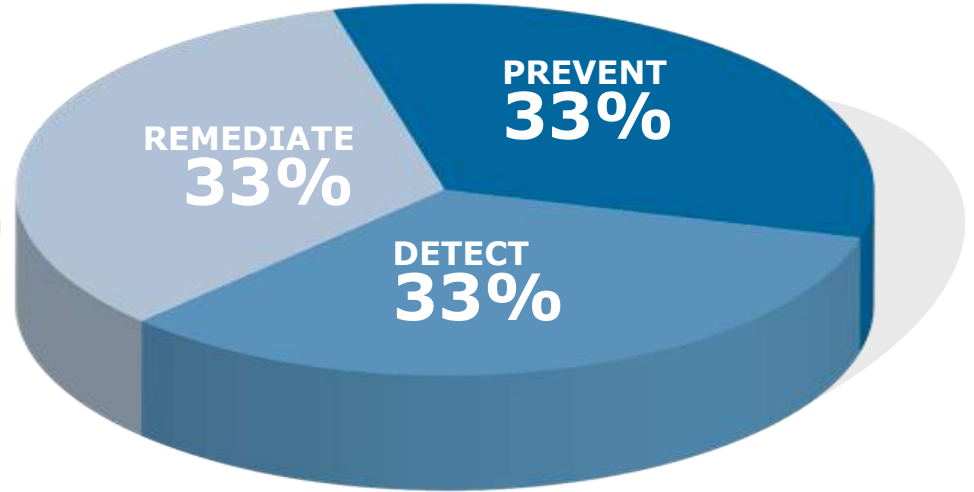
010110
101100111
110100

010110100
101100111
110100110
11

A paradigm shift takes place...

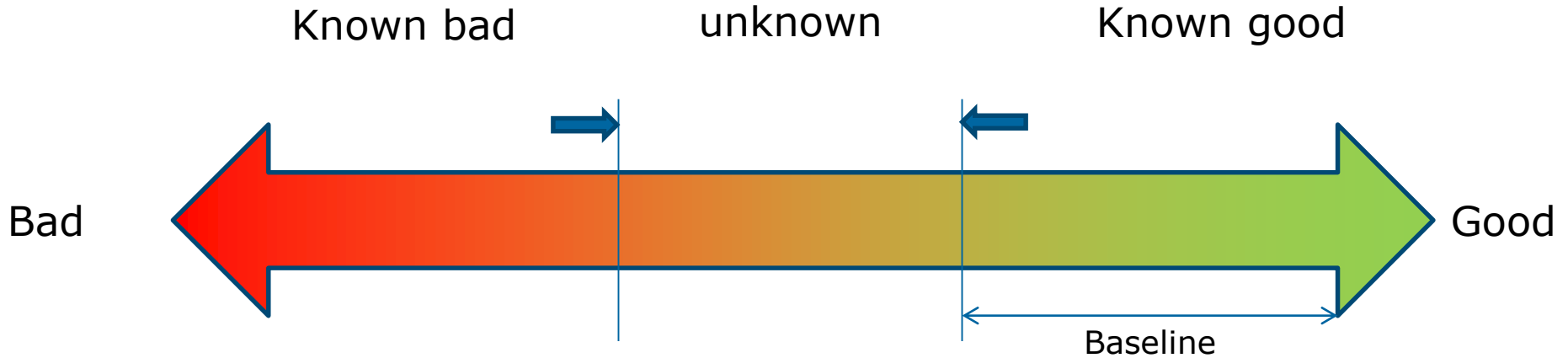


**Today's
spend**



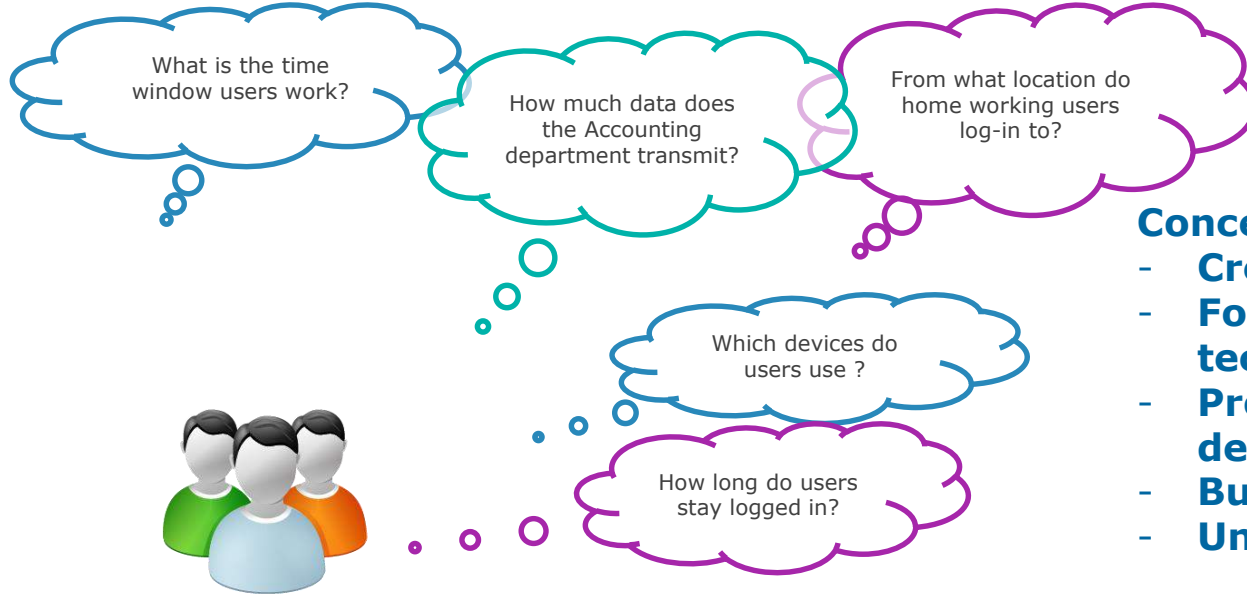
recommended balance:
**Intelligence
driven security**

The good, the bad and the unknown



The known good

Understanding your environment



Concept of known good

- **Create baselines**
- **Focus on people and technology**
- **Proactively investigate deviations on the baseline**
- **Build on internal knowledge**
- **Understand your environment**

Sentient security operations

We need to increase our capabilities

- ▶ Cyber Security is a
 - Business problem
 - fuelled by the human factor
- ▶ Our focus is
 - on the damage done and not the cause
 - focus on technical aspects and insufficient on the motives and people
 - known bad without the integration of known good
- ▶ Distinguish risk from certainties
- ▶ Understand
 - user communication / behaviour
 - M2M communication / behaviour

Thanks

For more information please contact:

M+ 352 621174128
koen.maris@atos.net

Atos, the Atos logo, Atos Codex, Atos Consulting, Atos Worldgrid, Worldline, BlueKiwi, Bull, Canopy the Open Cloud Company, Unify, Yunano, Zero Email, Zero Email Certified and The Zero Email Company are registered trademarks of the Atos group. February 2017. © 2017 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.

The Atos logo is displayed in a white, bold, sans-serif font. The letters 'A', 't', and 'o' are lowercase, while 'S' is uppercase. The 't' and 'o' are connected, and the 'S' has a distinctive shape with a curved bottom.