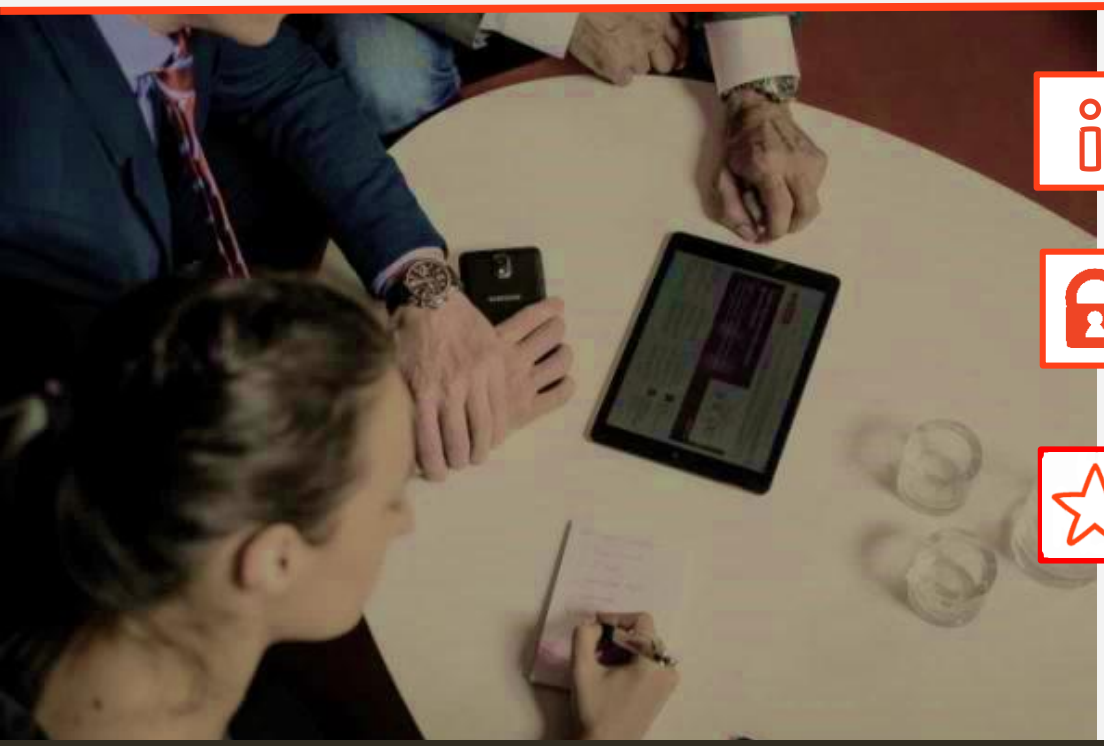
Big Data Security

SOGETI

Yves de Beauregard

OVERVIEW

SOGETI



- What is Big Data about?
- Big Data Security
- Security Big Data Project

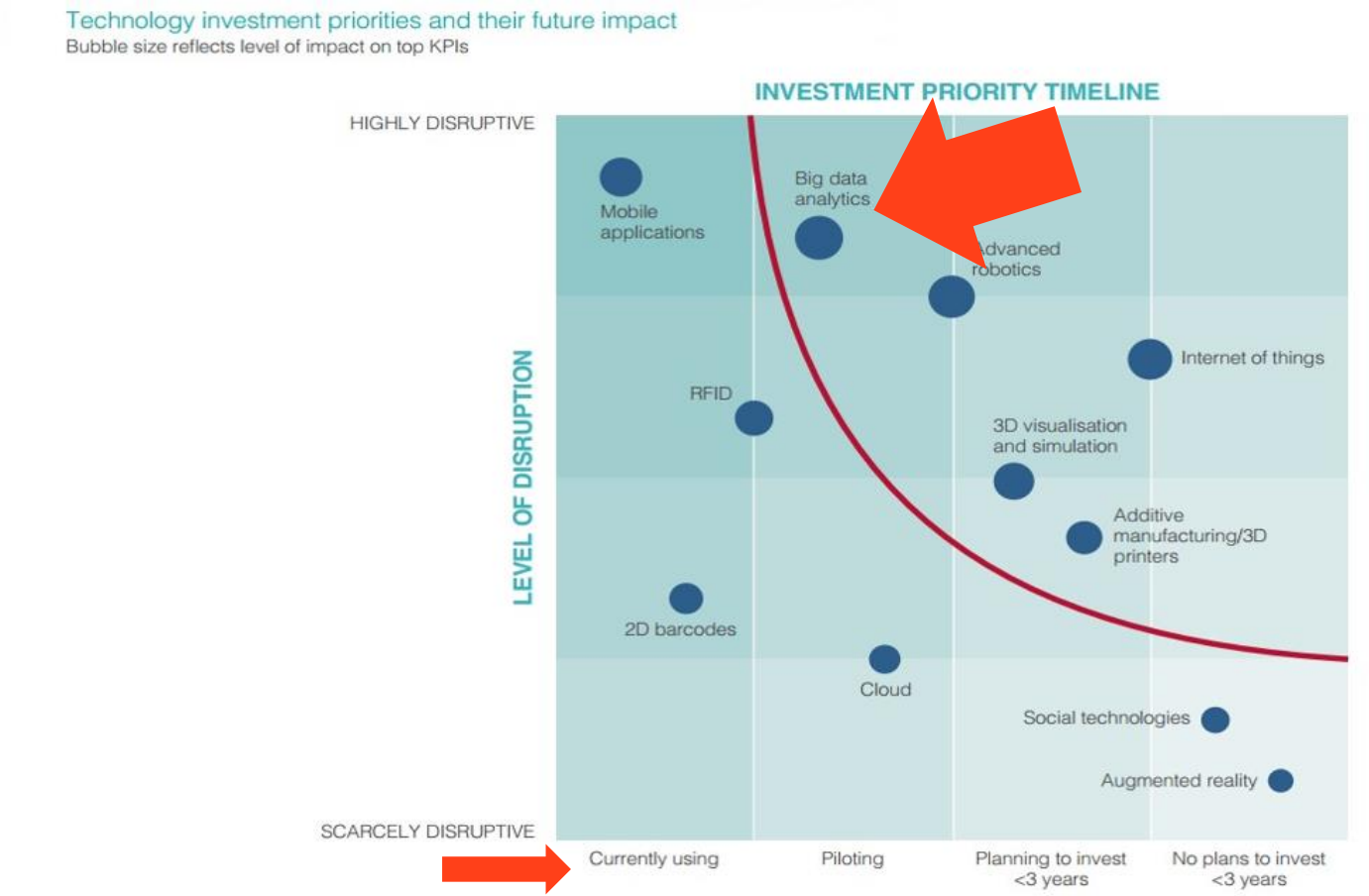
We are an IT services company delivering business value.

What is Big Data about?

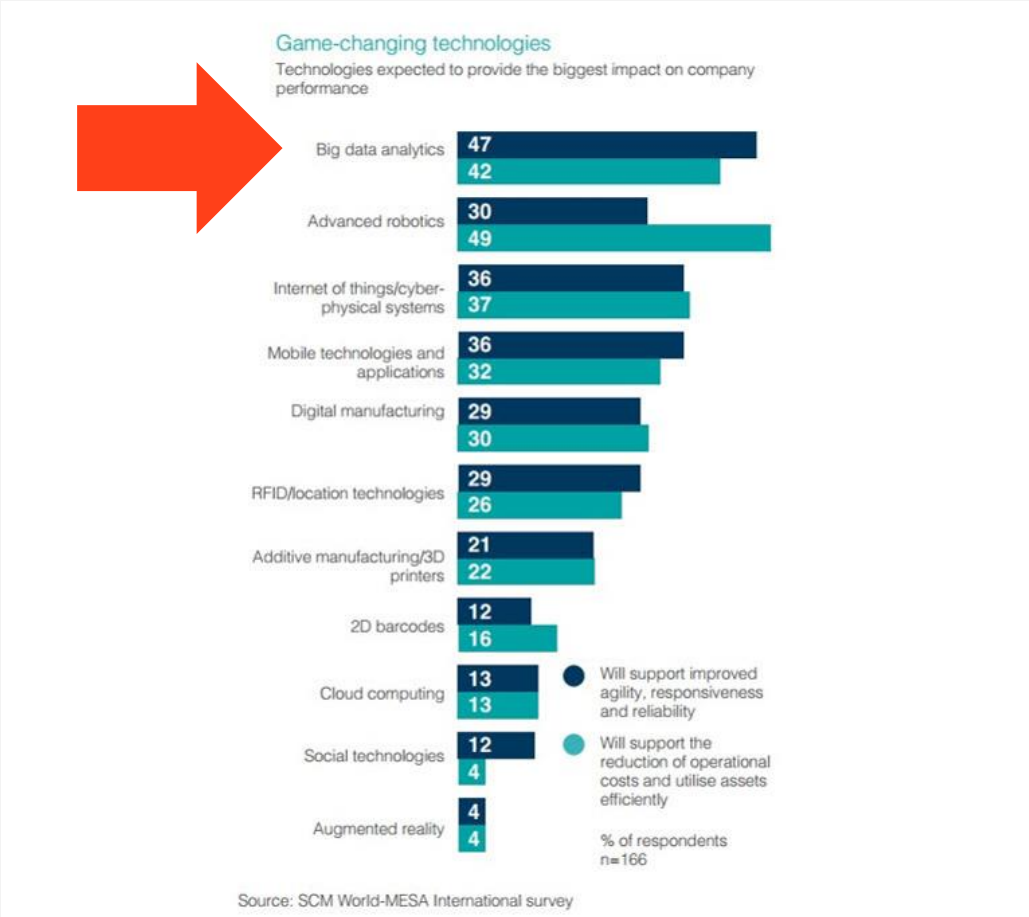
Big Data?

- Consequences of multiple technologies
- Influenced by many technologies
- Multiple forms

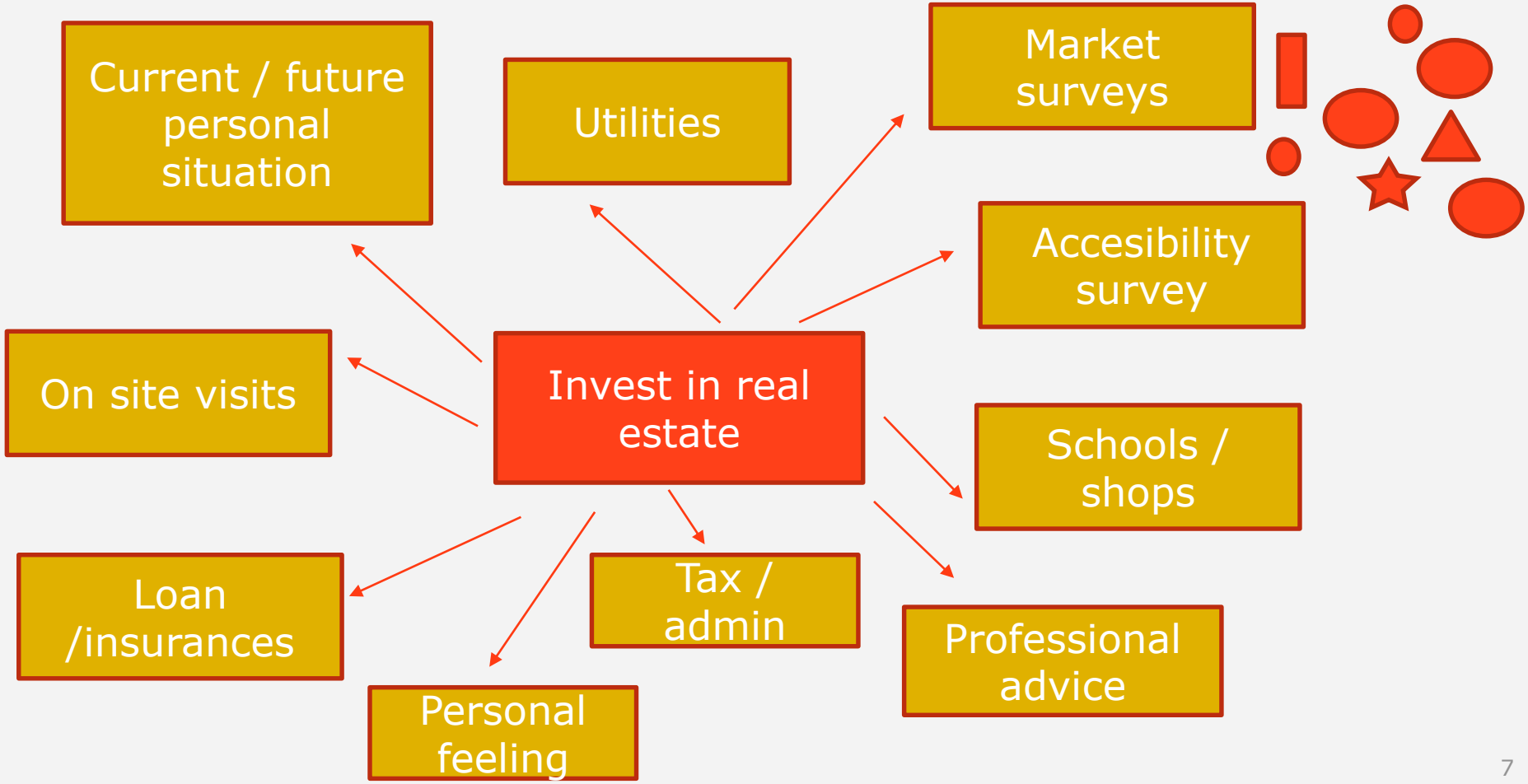
Investment & disruption



Game-Changing Technologies



We all do Big Data



Big Data Security

Security

- Expensive
- Often underscaled
- Serious break-in never done straight !

Big Data Security

- Ensure money is spent when most needed
- Detect & Look after internal & external risks
- Scale
- Learn & Adapt to new platforms
- Trends

Security Big Data Project

Why is this project different?

Actual SIEMs	Our Prototype
Focus on 'Hard' Security threats: -Focus on IT side of Security -Do not correlate with Business Processes	Deals with 'Soft' security threats: -Focus on Business side of Security -Detect abnormal behavior in Business Processes
Re-active mode: -Tackle known Security Threats ('Anti-virus' approach) -Limited automatic discovery (re-active analytics)	Pro-active mode -Focus on Anomaly detection, not on 'rule matching' -Automatic self learning 'normal' behavior to detect 'abnormal'
Proprietary Software Components	Latest Open Source Big Data technology and Process Mining

Security Big Data Project

- Objective
  - Proof of Concept (POC) of next-gen Security Operations Center (SOC)
  - Extend Sogeti Security Services

- Deliverable = Intelligent SOC prototype

- Research project:
  - Co-funded by Innoviris
  - Steered by Sogeti
    - Infrastructure Services, Application Services and Testing Services
  - Partners: ULB + UGent + Sirris
  - Oct 2013 → Oct 2015

Project Status & Future

- **Status:**
  - 8/9/2015: testing SOC POC prototype using Sogeti Tmap©

- **Future**:
  - Extend Sogeti's Security Big Data Analytics services
  - Scale up prototype to other Sogeti Services (eg Testing)
  - Integrate SOC-prototype in actual SIEMs
  - Share insights (eg via SPICES user group)

Any Questions?