

Big Data Security

OVERVIEW



What is Big Data about?



Big Data Security



Security Big Data Project



We are an IT services company delivering business value.





SOGETI

What is Big Data about?

Big Data?

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

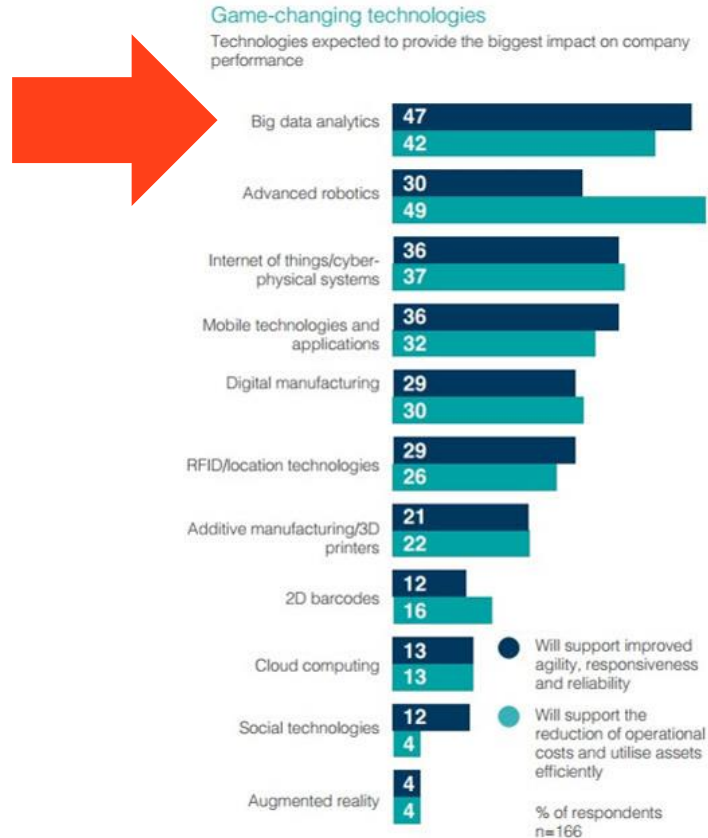
Investment & disruption

Technology investment priorities and their future impact

Bubble size reflects level of impact on top KPIs

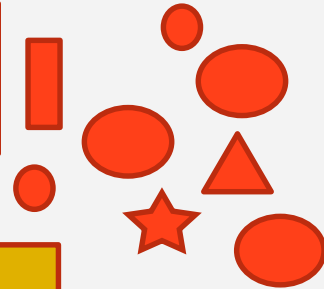
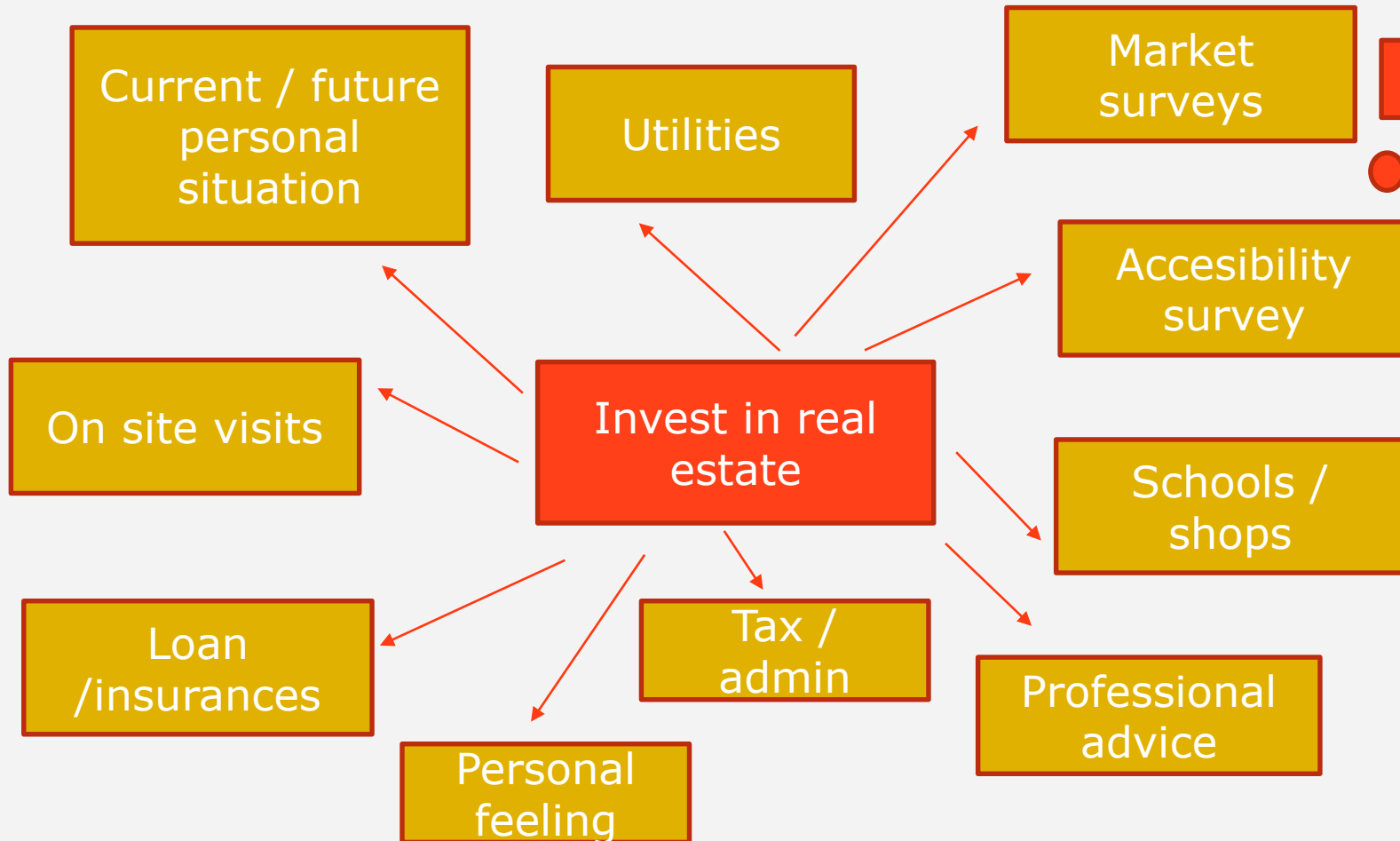


Game-Changing Technologies



Source: SCM World-MESA International survey

We all do Big Data





SOGETI

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





SOGETI

Security Big Data Project

Why is this project different?



Actual SIEMs	Our Prototype
<p>Focus on 'Hard' Security threats:</p> <ul style="list-style-type: none">-Focus on IT side of Security-Do not correlate with Business Processes	<p>Deals with 'Soft' security threats:</p> <ul style="list-style-type: none">-Focus on Business side of Security-Detect abnormal behavior in Business Processes
<p>Re-active mode:</p> <ul style="list-style-type: none">-Tackle known Security Threats ('Anti-virus' approach)-Limited automatic discovery (re-active analytics)	<p>Pro-active mode</p> <ul style="list-style-type: none">-Focus on Anomaly detection, not on 'rule matching'-Automatic self learning 'normal' behavior to detect 'abnormal'
<p>Proprietary Software Components</p>	<p>Latest Open Source Big Data technology and Process Mining</p>

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?

