IT Architecture Intelligence for Risk and Security Analyses

Thomas Trojer, Matthias Farwick, Ruth Breu

Research Group Quality Engineering, *Universität Innsbruck*

Learning from Google Maps –

Txture
data center intelligence

Overlays of traffic data vs. **integration of real time data**

World map/city map vs**. abstract/drill-down visualizations**

Routes/itineraries vs. **infrastructure planning/transformation/analyses**

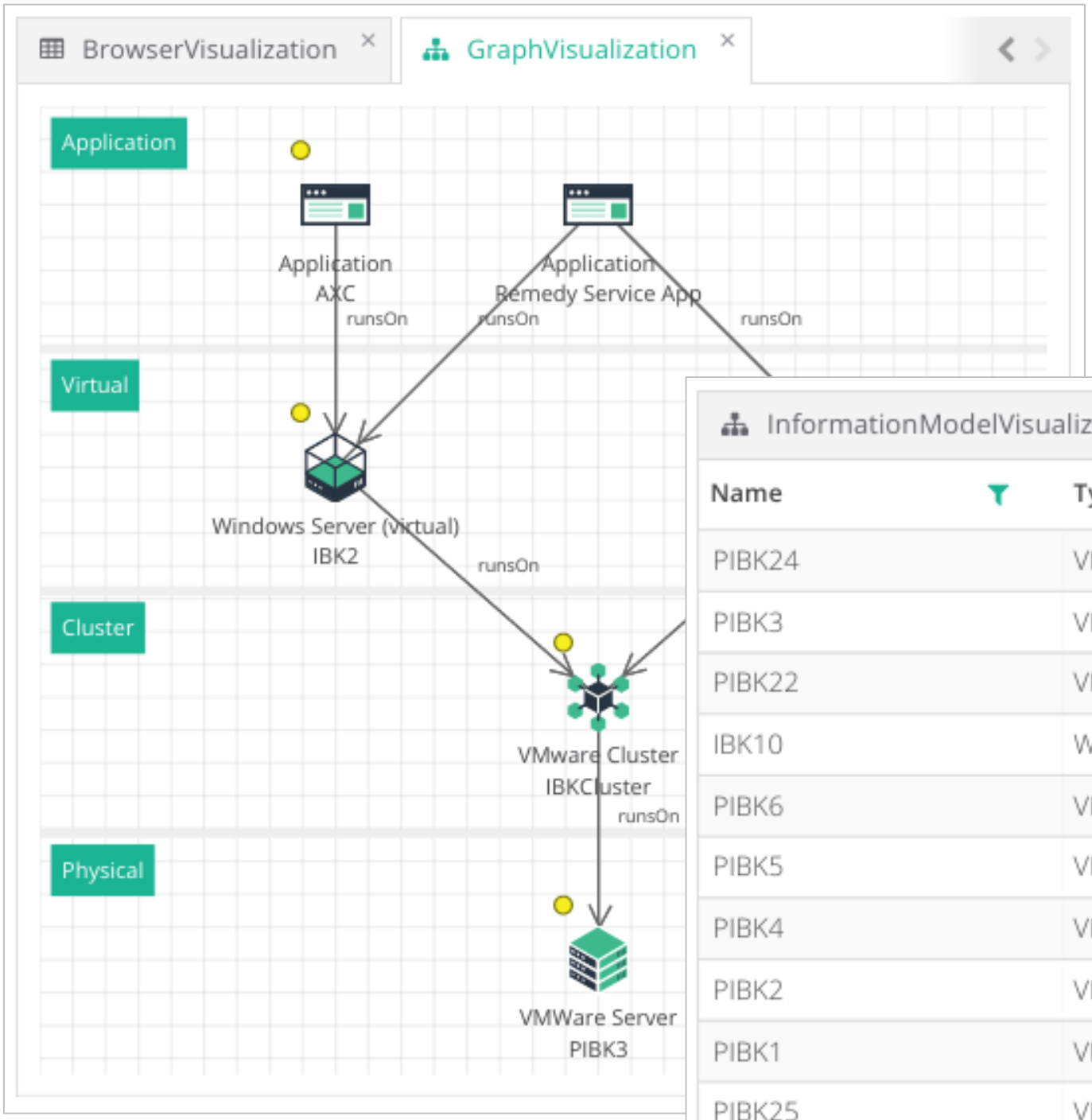
Location/map history vs. **IT architecture decisions/evolution**

Stadt Bern

ARZ

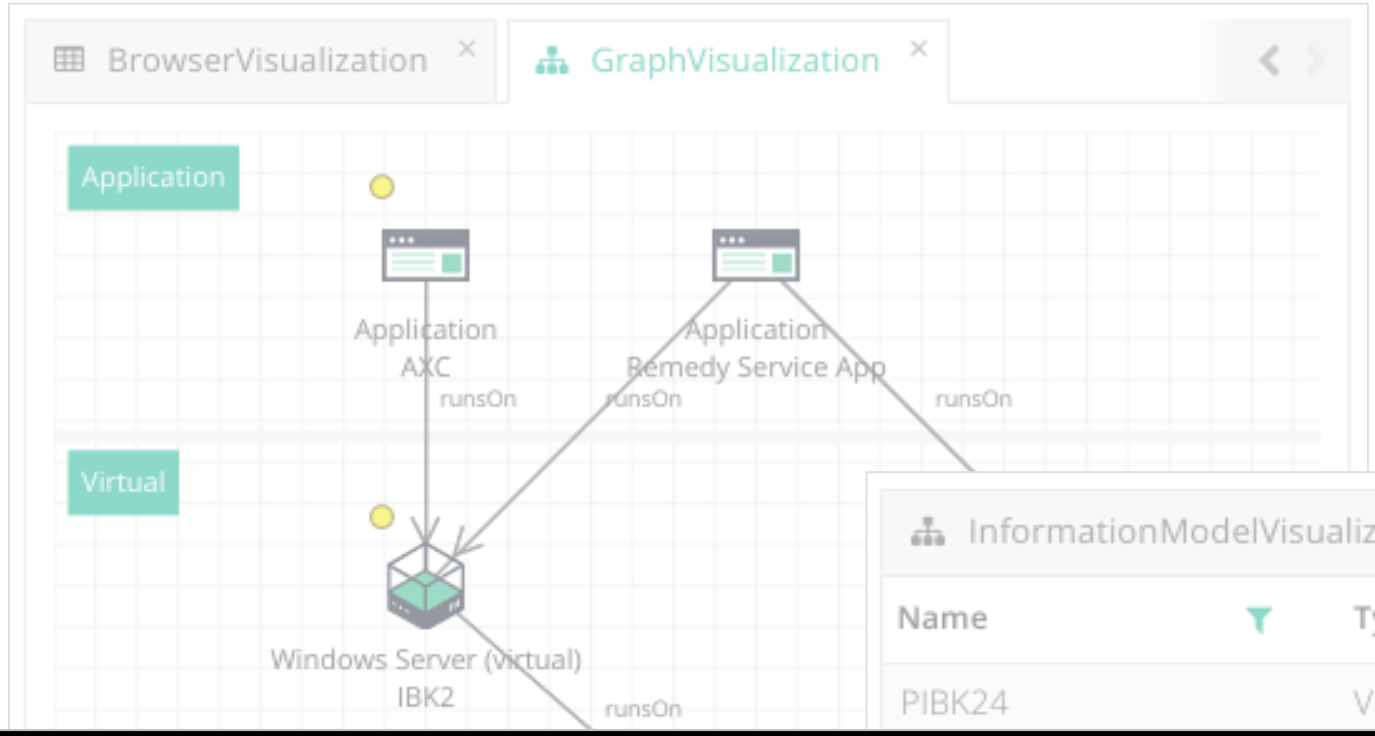
infineon

Research partner
Infineon GmbH
2013 – …



InformationModelVisualization | BrowserVisualizat

Name	Type	OLA
PIBK24	VMWare Server	
PIBK3	VMWare Server	Gold
PIBK22	VMWare Server	
IBK10	Windows Server (physical)	
PIBK6	VMWare Server	Bronz
PIBK5	VMWare Server	Silver
PIBK4	VMWare Server	Silver
PIBK2	VMWare Server	Gold
PIBK1	VMWare Server	Gold
PIBK25	VMWare Server	



IT Architecture Intelligence

(Outcomes of our research)

- Organization specific “information models”
- Interactive and navigable visualizations
- Versioning of IT architecture documentations
- Query framework considering structure and change-over-time
- Branching mechanism for planned IT architectures
- Automated data integration from external data sources

Contributing to Security and Risk Management
(Current research)

Security management is a continuous process …

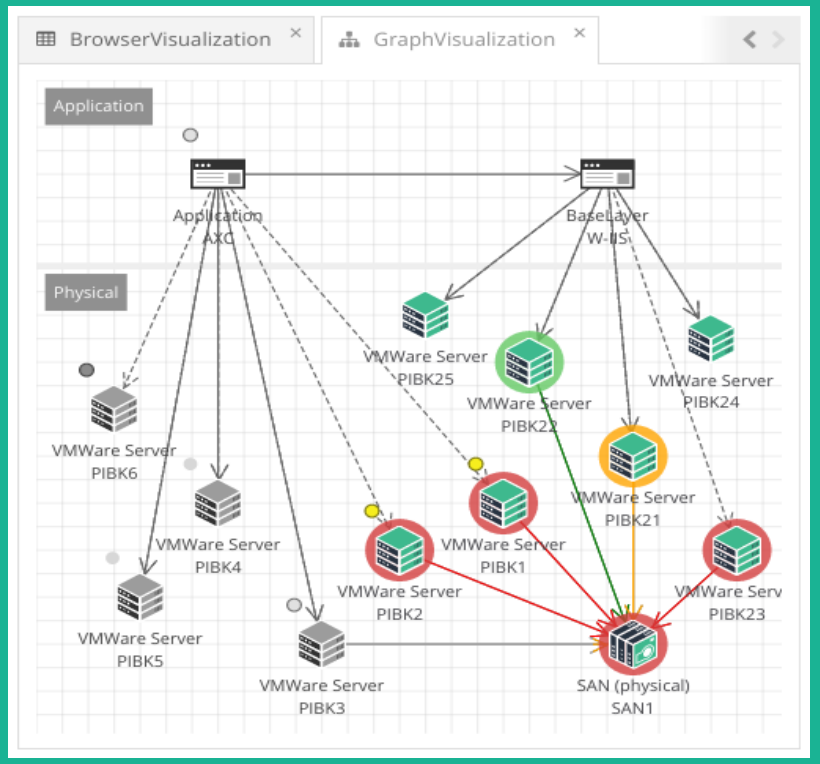
- Security requirements are formulated e.g. as part of SLAs for IT assets (cf. ITIL)
- Security metrics are computed based on e.g. ability to access IT services, exposure of servers, etc. (cf. OSSTMM RAV)
- Compliance needs to be checked, e.g. whether IT assets are protected within security zones or that person specific data is only archived in secured backup rooms (cf. BDSG)

… and benefits from an **up-to-date IT architecture documentation**

IT Architecture Intelligence for Security and Risk Management

Use case – Initiating Security Management Processes

- Import IT assets from different external datasources
- Import of runtime data to properties of IT assets
- Propagation of runtime state to connected IT assets
  - Expansion and reduction functions (e.g. “to all neighbors”, “average”, etc.)
  - Computation of metrics and KPIs
- Focusing on relevant IT architecture parts by means of views and queries
  - Drill-down views, transitive dependencies, etc.
  - “Neighborhood” of assets, filter assets, etc.



Contributing to Security and Risk Management
(Current research)

Security management is about proper organization specific security controls …

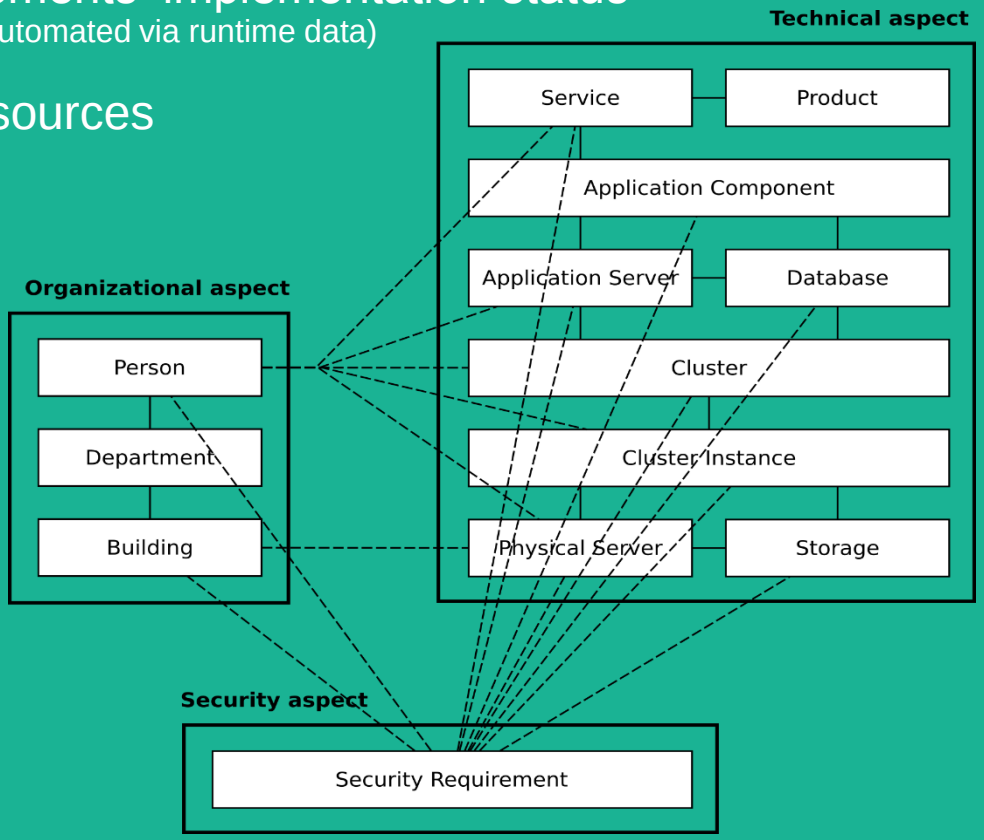
- Controls are designed to prevent threats from their manifestation (cf. type of controls, ISO 2700x)
- Controls are designed to lower the effects from already manifested threats (cf. ISO 2700x)

… and benefits from **customizable, evolvable information models**

IT Architecture Intelligence for Security and Risk Management

Use case – Planning and Implementing Security Controls

- Managing security requirements, personnel, etc. together with IT assets
  (by making use of different architectural documentation aspects)
- Defining triggers to update requirements' implementation status
  (through responsibles, reference architectures or automated via runtime data)
- Linking IT assets to external datasources



Contributing to Security and Risk Management
(Current research)

Security controls need to be evaluated and adjusted to maintain performance …

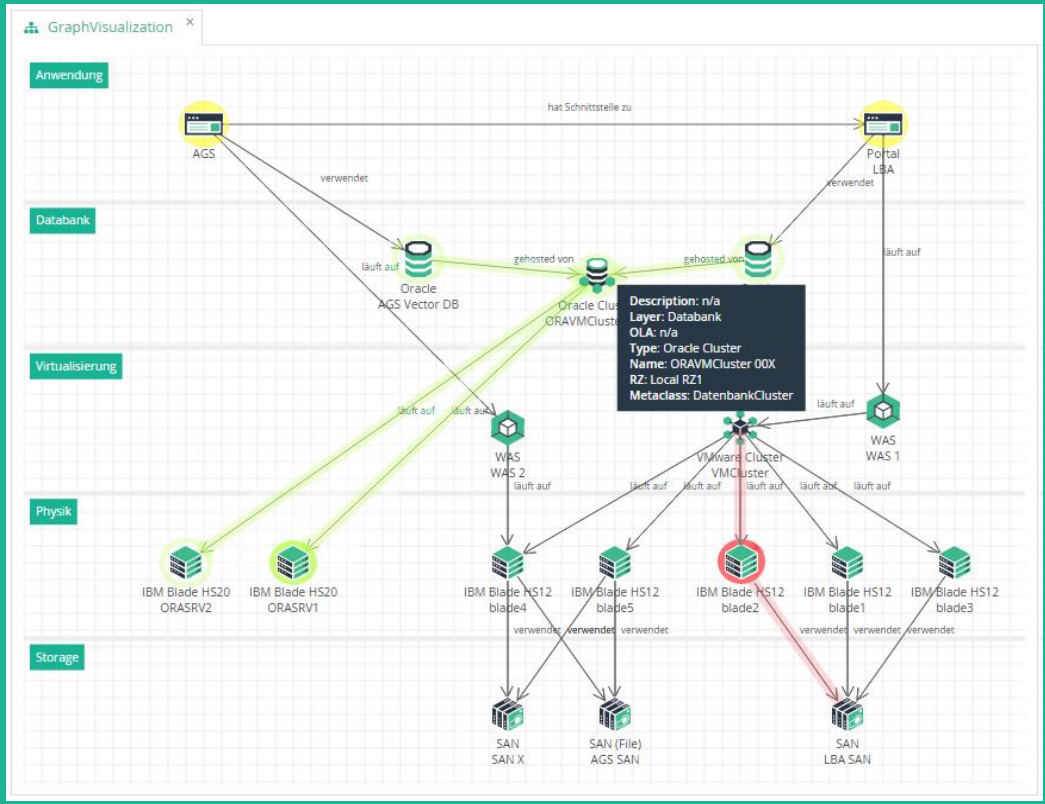
- Comparison of IT landscapes and their evolution over time (e.g. according to defined plans)
- Evaluation of security objectives of an IT system (cf. TOEs evaluated against ITSEC or TCSEC)

… and benefits from **sophisticated analysis capabilities**

IT Architecture Intelligence for Security and Risk Management

Use case – Visualizing Changes in “Attack Surface” Measurements

- Import of e.g. OSSTMM RAV values to properties of IT assets
  (in case some external source manages conducted RAV values)
- Propagation of worst RAV value towards service/product level
- Comparing alternative IT architectures
  (by making use of documentation branches, time based queries and “change-aware” visualizations)



Conclusion

- **Flexible information** models allow for increased level of detail just where it is needed
- **Automated data integration** allows security management to be in-sync with reality
- IT architecture **versioning**, **branching** and **analysis** allow to plan controls and track their implementation progress and performance

We are curious ...

Where are your **pain points** in Security and Risk Management?

What other **use cases** do you see in practice?

Many thanks …

Further information on our tool

under http://www.txture.tools
and http://qe-lab.at
or thomas.trojer@uibk.ac.at