Public

Lloyd's Market Briefing: SAP GRC for Risk, Fraud and Cyber

Dr. Neil Patrick, COE GRC (EMEA), SAP
4th July 2016

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

Key themes: solutions for GRC and security from SAP

Access governance

Audience:
- CIO or director of IT
- CFO
- CISO

Cyber security risk and governance

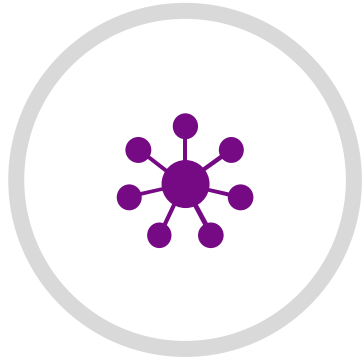
Audience:
- CIO
- CFO
- CISO

Three lines of defense

Audience:
- CxO (CFO, CRO, CCO, or CAE)
- Director of IT and access management

International trade management

Audience:
- VP of supply chain
- Director of trade compliance
- CFO



Fraud management and screening

Audience:
- CAE
- Director of internal audit
- LoB VP (Procurement)
- Legal

NP

SAP solutions for governance, risk, and compliance (GRC)

Simplify, gain insight, and strengthen

SAP Access Control

Enable business-driven access governance

SAP Access Violation Management by Greenlight

Identify and quantify the impact of actual access risk violations

SAP Dynamic Authorization Management by NextLabs

Secure applications, protect application data, and simplify role management

SAP Regulation Management by Greenlight, cyber governance edition

Manage cyber-related regulatory requirements and align with internal controls

SAP Process Control

Maintain effective controls and ongoing compliance

SAP Regulation Management by Greenlight

Manage regulatory requirements and align with internal control activities

SAP Risk Management

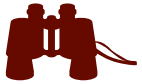
Preserve and grow value with enterprise risk management

SAP Audit Management

Transform auditing and move beyond assurance

SAP Fraud Management

Detect and prevent fraud better



SAP Business Partner Screening

Grow your business network with confidence

SAP Global Trade Services

Optimize global trade and screen restricted parties

SAP Technical Data Export Compliance by NextLabs

Automate trade compliance for digital goods and technical data

SAP Electronic Invoicing for Brazil

Meet electronic invoicing requirements for Brazil

Solutions for security from SAP

SAP Enterprise Threat Detection

Detect, investigate, and respond to anomalies

SAP Single Sign-On

Authenticate once to access all business applications

SAP Identity Management

Know your users and what they can do

SAP Cloud Identity

Manage the identity lifecycle in the cloud

SAP NetWeaver AS, add-on for code vulnerability analysis

Analyze code for security risks

SAP Mobile Secure

Manage cyber risks for mobile devices

Cyber-Attack: Enterprise Defence

Overview: This is Your Digital Transformation Future

In the last two years:

90%

Of the world's data has been generated[1]

40%

Growth in adoption of business networks[2]

7-fold

Increase of MTM patents through WIPO 2010 to 2014

6

Devices per person on-line by 2025 (50 billion)[3]

205

Average days to realize there is a cyber breach

51%

Of workload processed in the cloud in 2014[4]

1 *ScienceDaily*, May 22, 2013.

2 *Technology Adoption Report on Business Networks*, Ardent Partners, 2014.

3. *Ericsson*

4 *Cisco Global Cloud Index: Forecast and Methodology for 2013–2018*, Cisco Systems Inc., November 11, 2014.

Trends in Attack

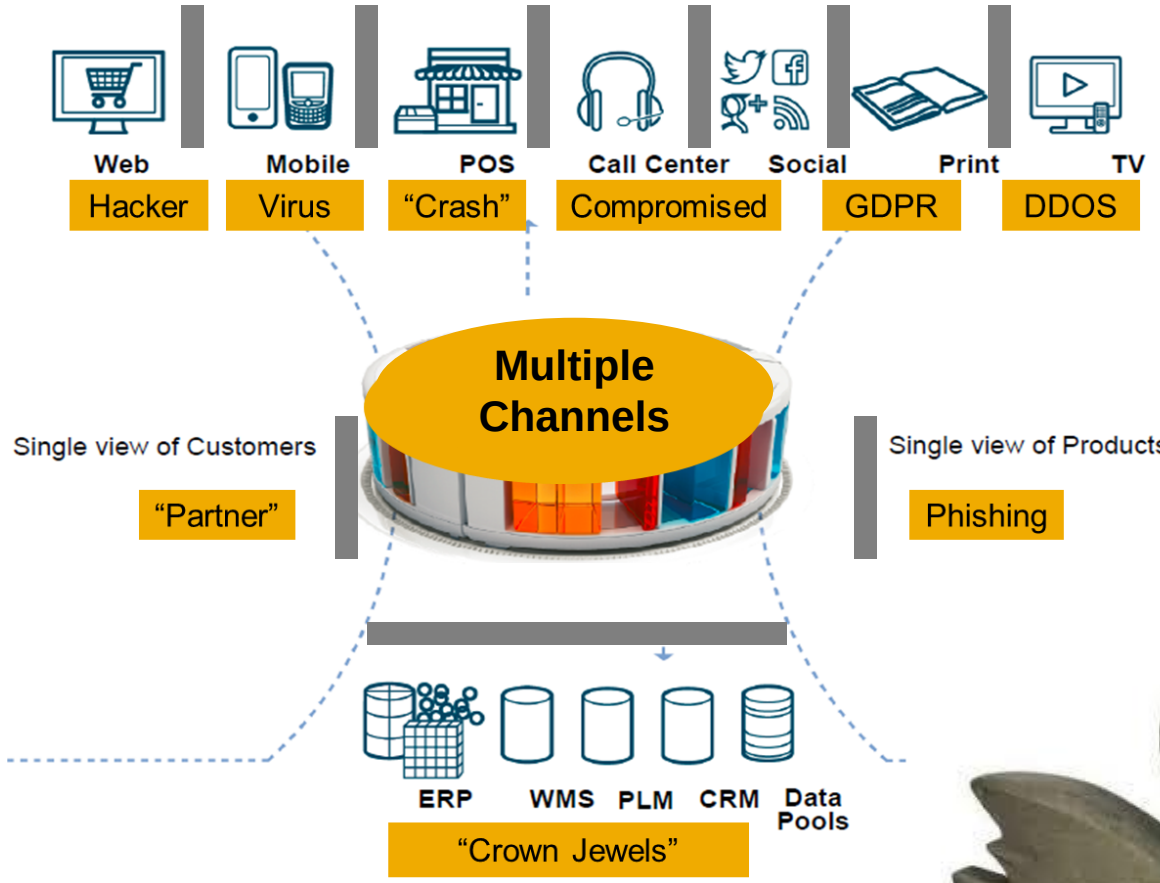
Evolution of Fraud - Visa Europe

	2000	2015
Fraudsters	Local crime rings	Global crime rings Decentralized
Target	Large retailers	Payment Industry
Technique	ID Theft, Phising Rudimental data	Cross Border, Online, ID, Phising Hacking: Cyber crime
Type	Mass market credit cards	All types of cards Bank Accounts
Resources	Technical know how	Audacity Technical expertise Global connections

Operates as a big business

Silo Defence vs Joined-up Attack

- Many more channels
- Criminals – organise to exploit channels
- Growth of internal fraud/criminal behaviour
- Fragmented & complex employee & partner community
- Increasingly intrusive and punitive regulator

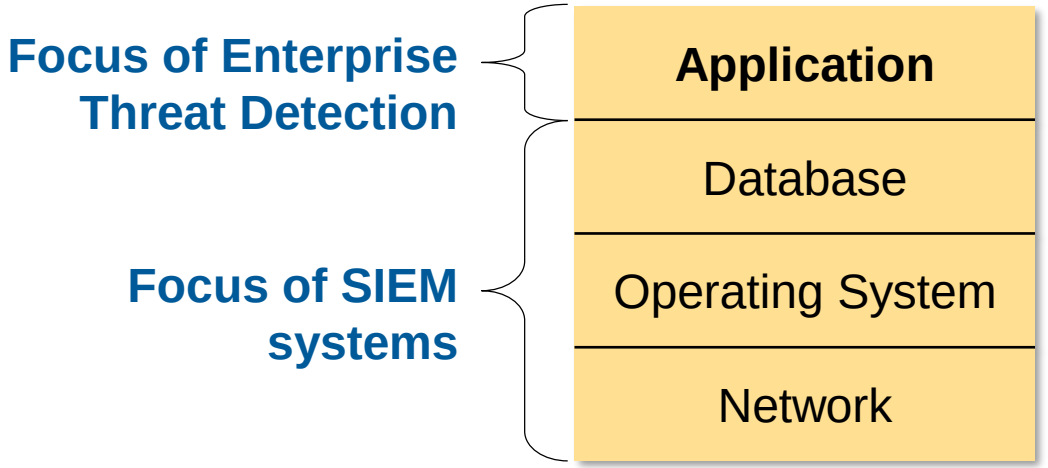


Fragmented Silos

Focus on Where the Important Data Resides

SAP Enterprise Threat Detection:

- **Applications** keep the **crown jewels,** yet they are often neglected
- Analysis of **application** log pinpoints activities **not visible** or understandable in other analyses
- Correlation of event **context** across logs and across systems, and not just “expected” threats
- Complexity and processing **speed** and power from HANA is significant



Security information and event management (SIEM) is a term for software products and services combining security information management (SIM) and security event management (SEM). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications.

WE **PARTNER** WITH SIEM SOLUTIONS

Broader Perspective: SAP Cyber Risk Defence Approach

Risk assess value of assets, determine cost of protection

Risk Management

Control access to approved visitors

Access Control

Detection of intruders

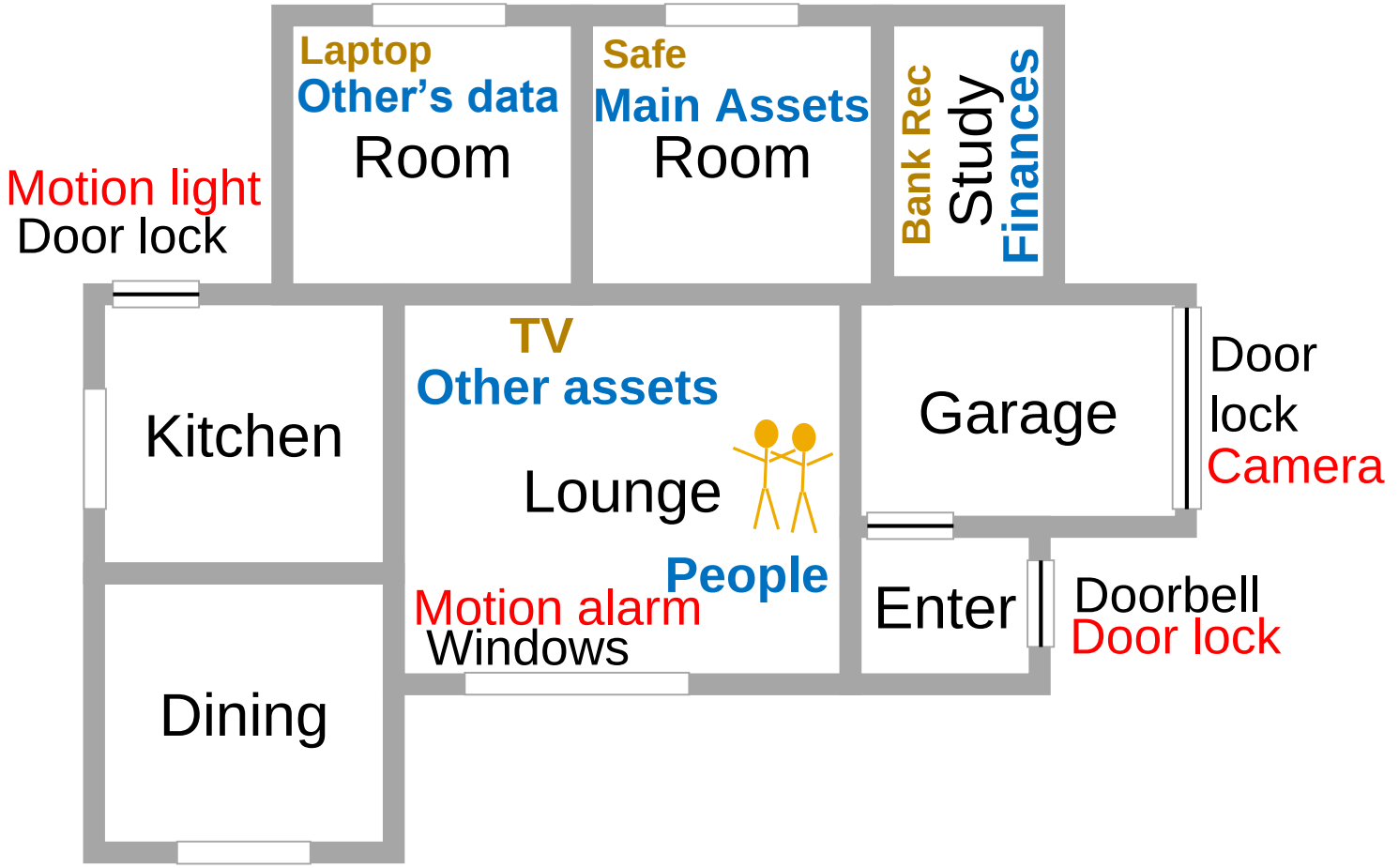
Enterprise Threat Detection
Fraud Management

Routines to ‘make safe’ at night, when away (BAU)

Process Control
Code Vulnerability Analysis

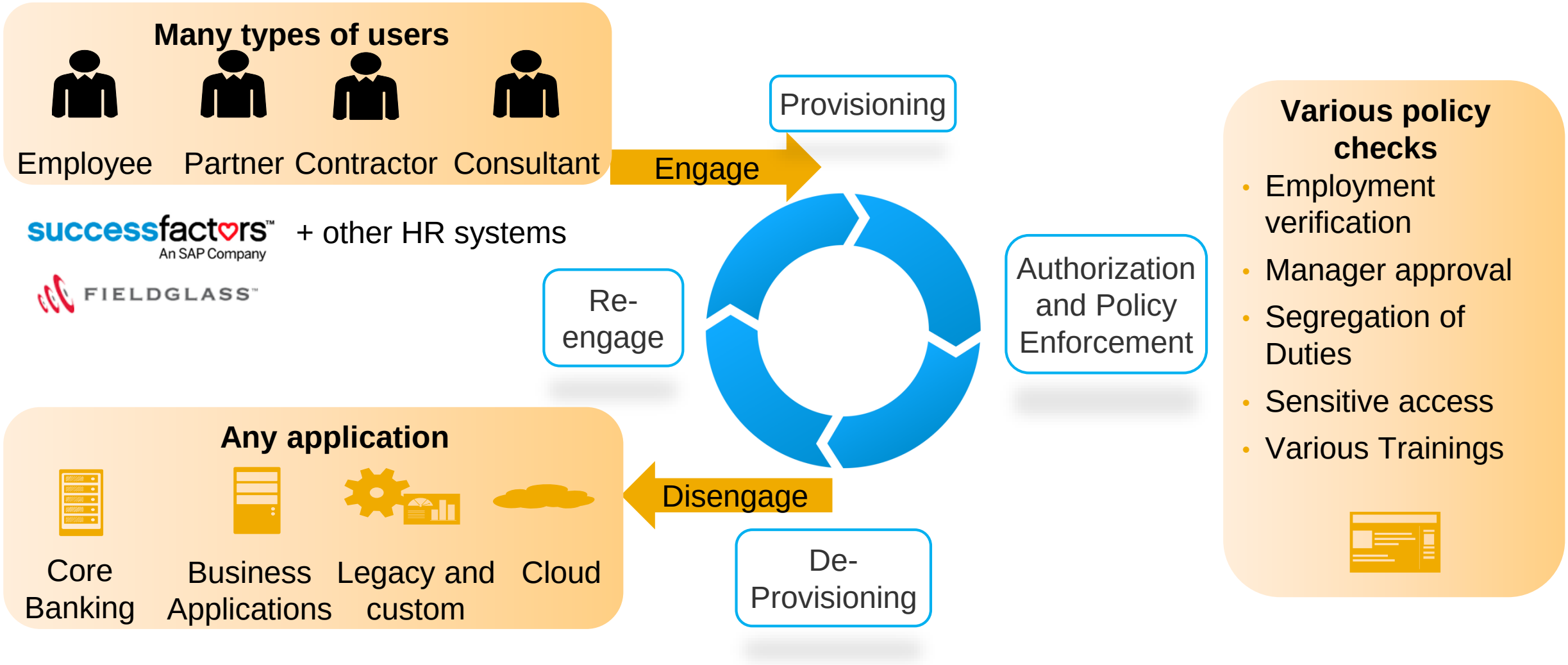
Read news for latest scams, am I protected?

Cyber Regulation Management



HR/AD Integrate to Provisioning

Access Governance via HR System: Manage Legitimate Access



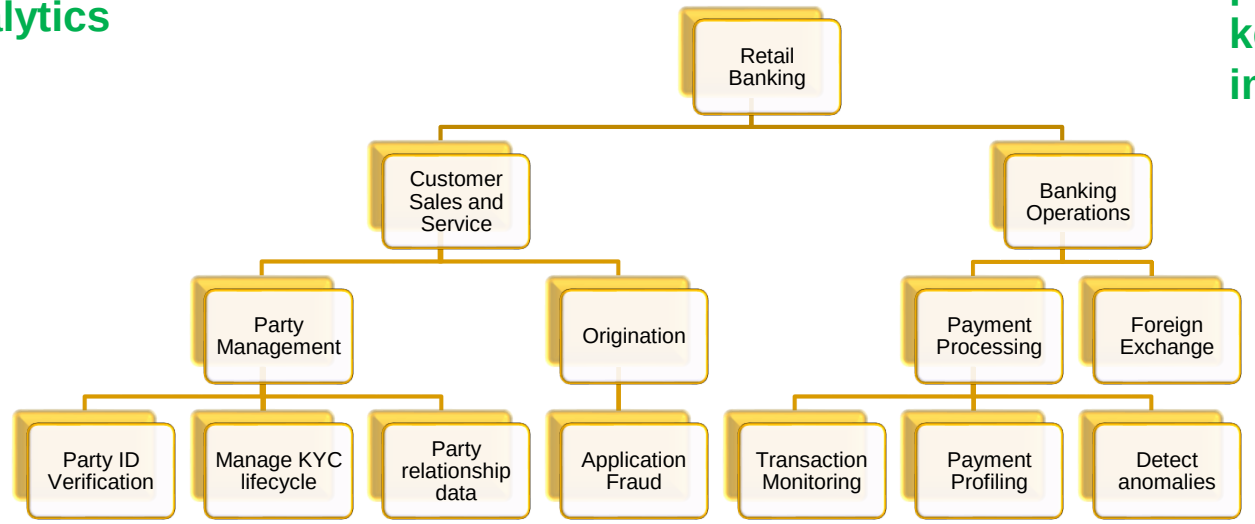
Policy, Process, Regulations

Policy + Controls + Processes + Tests + Audit Trail

Organization and Process …. **and Automation**

Support decisions and promote accountability with insightful analytics and sign-off

Document controls and policies centrally; map to key regulations and impacted organizations

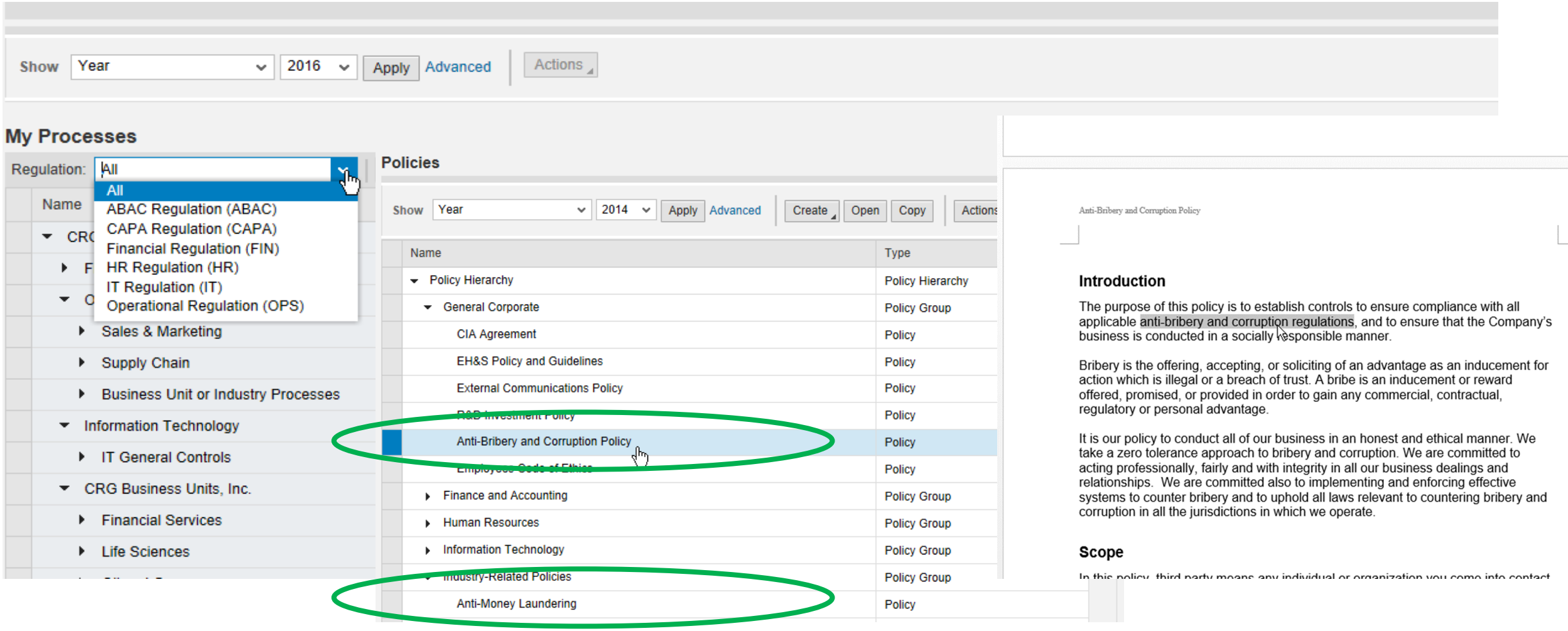


Perform automated, exception-based monitoring of ERP systems (includes non-SAP)

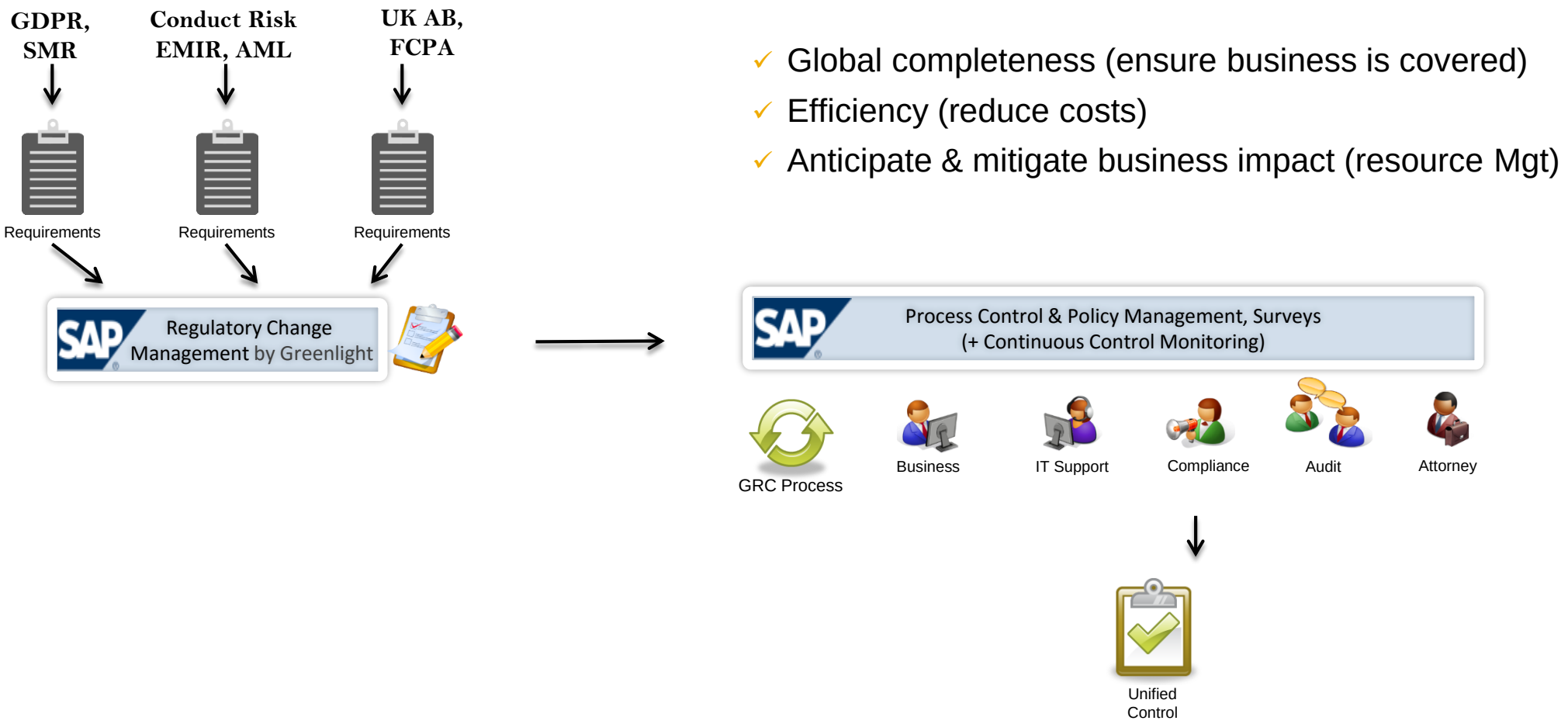
Evaluate control design and effectiveness; raise and remediate issues

Perform periodic risk assessments to determine scope and test strategies

Define Business as Usual Controls, Link to Org Structure + Policy



RegTech – Reduce Cost of Regulatory Compliance



- ✓ Global completeness (ensure business is covered)
- ✓ Efficiency (reduce costs)
- ✓ Anticipate & mitigate business impact (resource Mgt)

Putting it Together with Profiling

Achmea: Focus on Insurance Fraud

Company
Achmea

Industry
Insurance

Employees
22,000

Revenue
25B Euro

Customers
7M

Other details
Gross Written Premiums 20,223M €

- One of the largest financial service providers in NL
- Providing about half of all Dutch households with health, life, and non-life insurance.
- 60 FTEs in Fraud Investigation
- Business Case:
  - >3% of claims believed fraudulent
  - P&C
    - 1M claims p.a. (Auto, Homeowner, ..)
  - Health
    - Largest cases w/ health care services providers

"SAP Fraud Management enables Achmea to be successful in her fight against fraud in insurance"

Sjoerd van der Klaauw, Achmea

Focus on Real Fraud

- **Business Benefit #1: Single End-To-End FM Platform**
  Ability to detect/prevent claim fraud across mult. LOBs (Phase 1 P&C, Phase 2 Health)
- **Business Benefit #2: Minimize Fraud Losses**
  Minimizing payments on illegitimate claim requests & directly impacting company's loss ratio. Detection: Legacy (<1%); SAP (>1%)
- **Business Benefit #3: Fraud Investigator's Direct Control Over Rules**
  Quality (and ease of adjustment) of rules, resulting in speed to reduce # false positive hits

Pattern Spike based on Type, Threshold, new Vulnerability

1 Rules-based alert, real-time, calibrated.

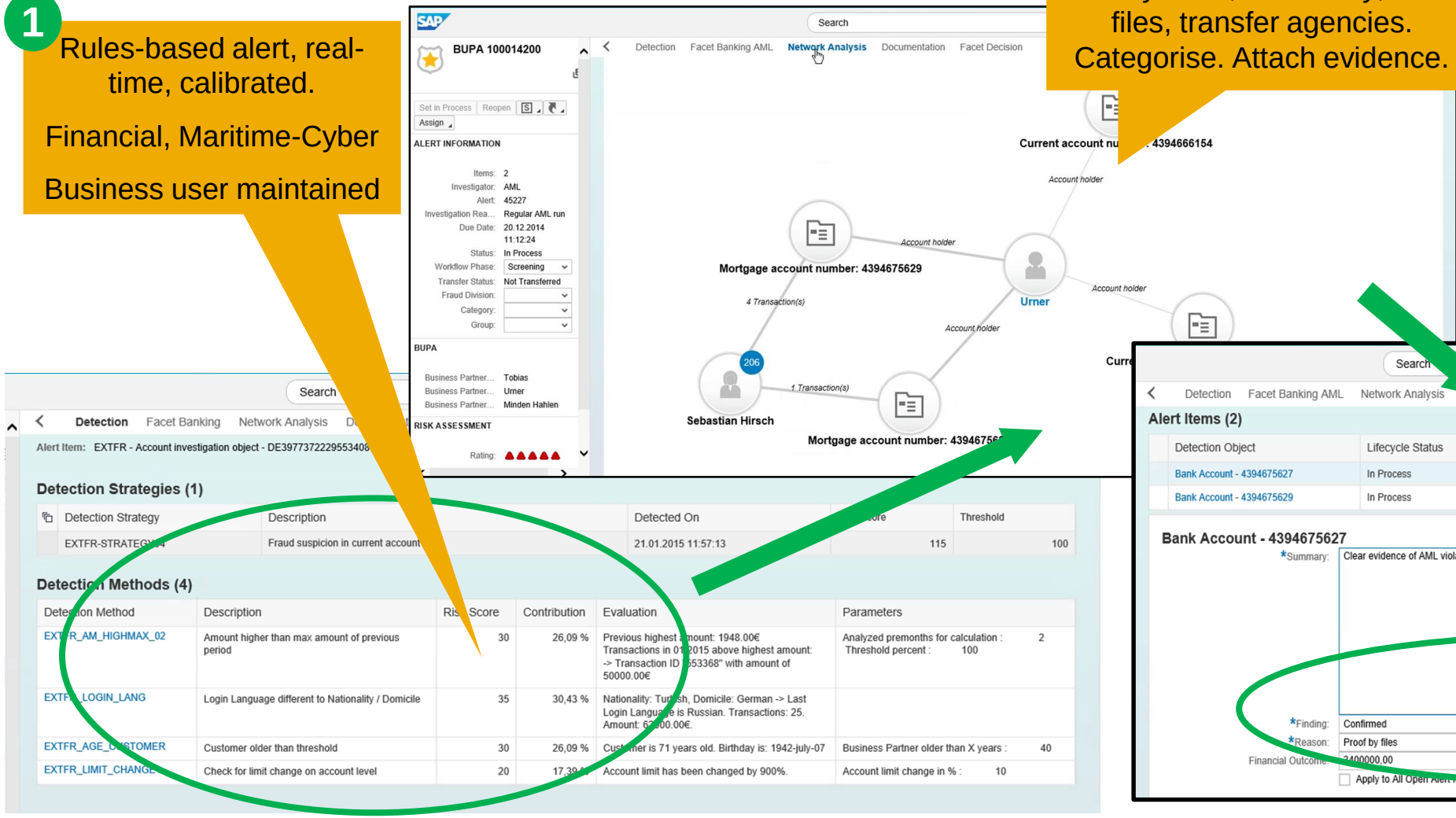
Financial, Maritime-Cyber

Business user maintained

2 Investigate alert for malicious activity. Geo, nationality, bank files, transfer agencies. Categorise. Attach evidence.

Patterns over time, contextualised data for 360º viewpoint

3 Conclude investigation. Calibrate strategy effectiveness. Feed back to design



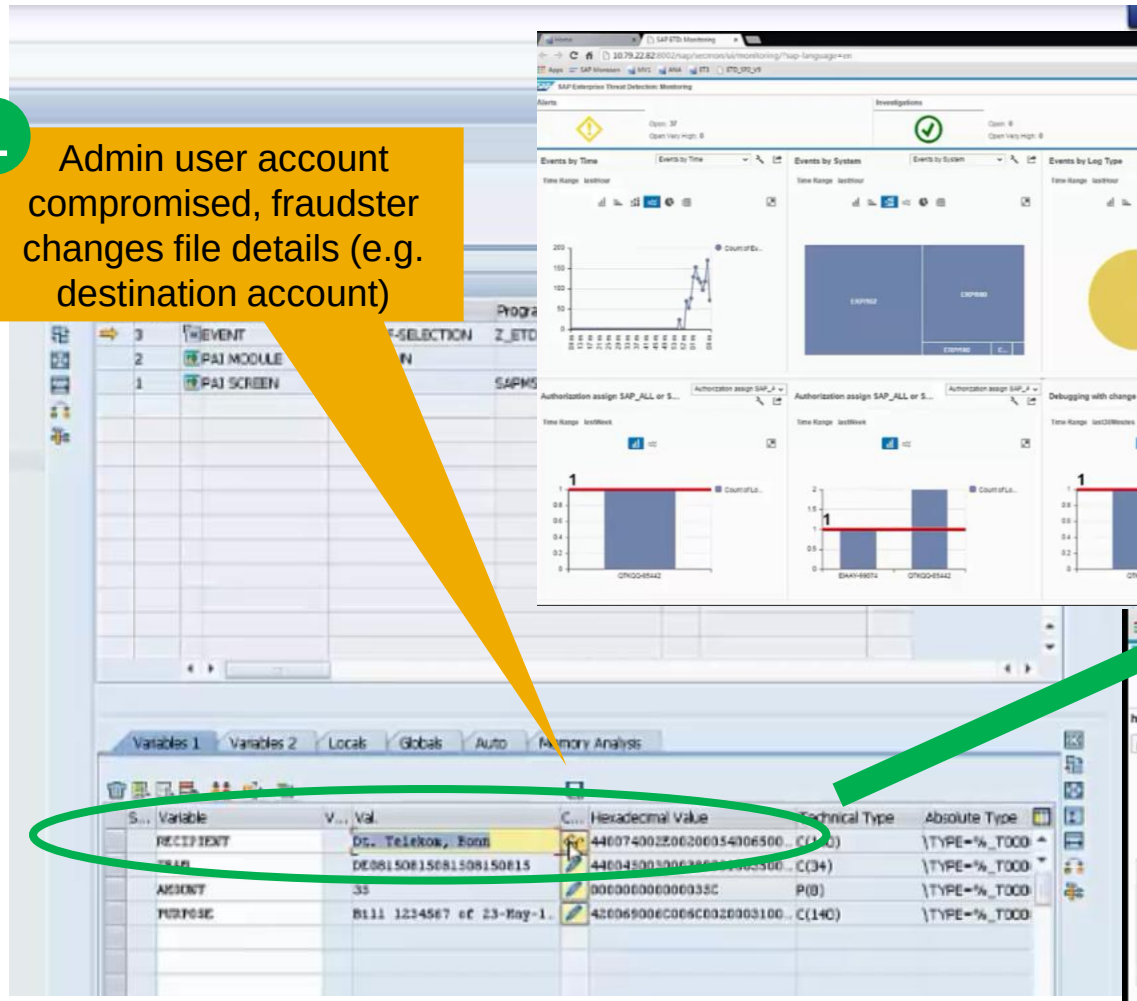
User Changes Payment Routing Data: ETD Application-level Alert

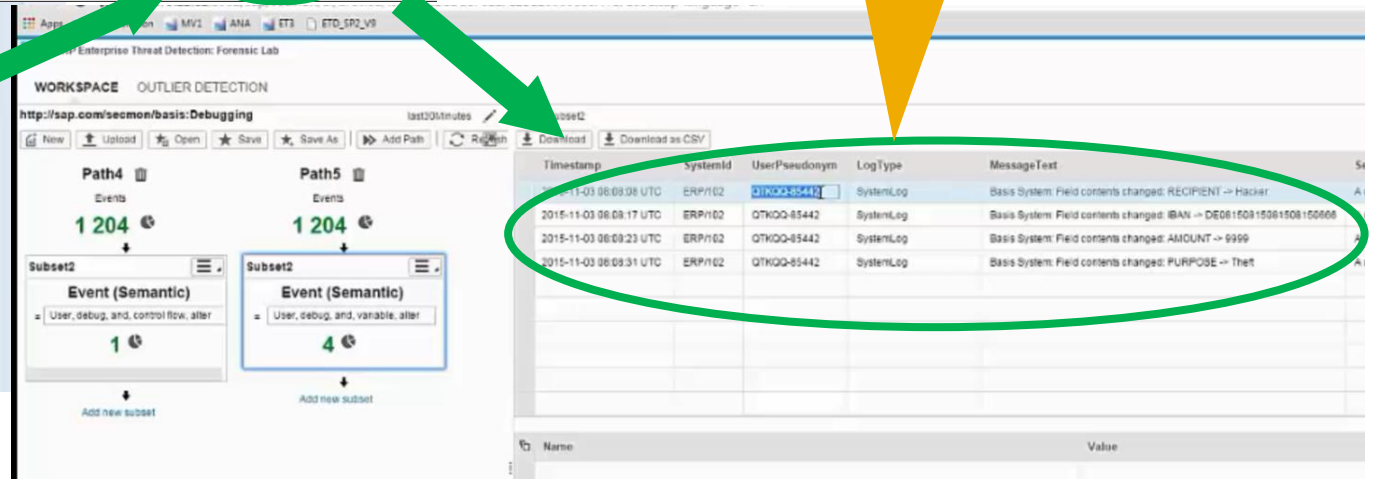
1 Admin user account compromised, fraudster changes file details (e.g. destination account)

2 ETD scanning Application logs real-time, alert: rule threshold exceeded

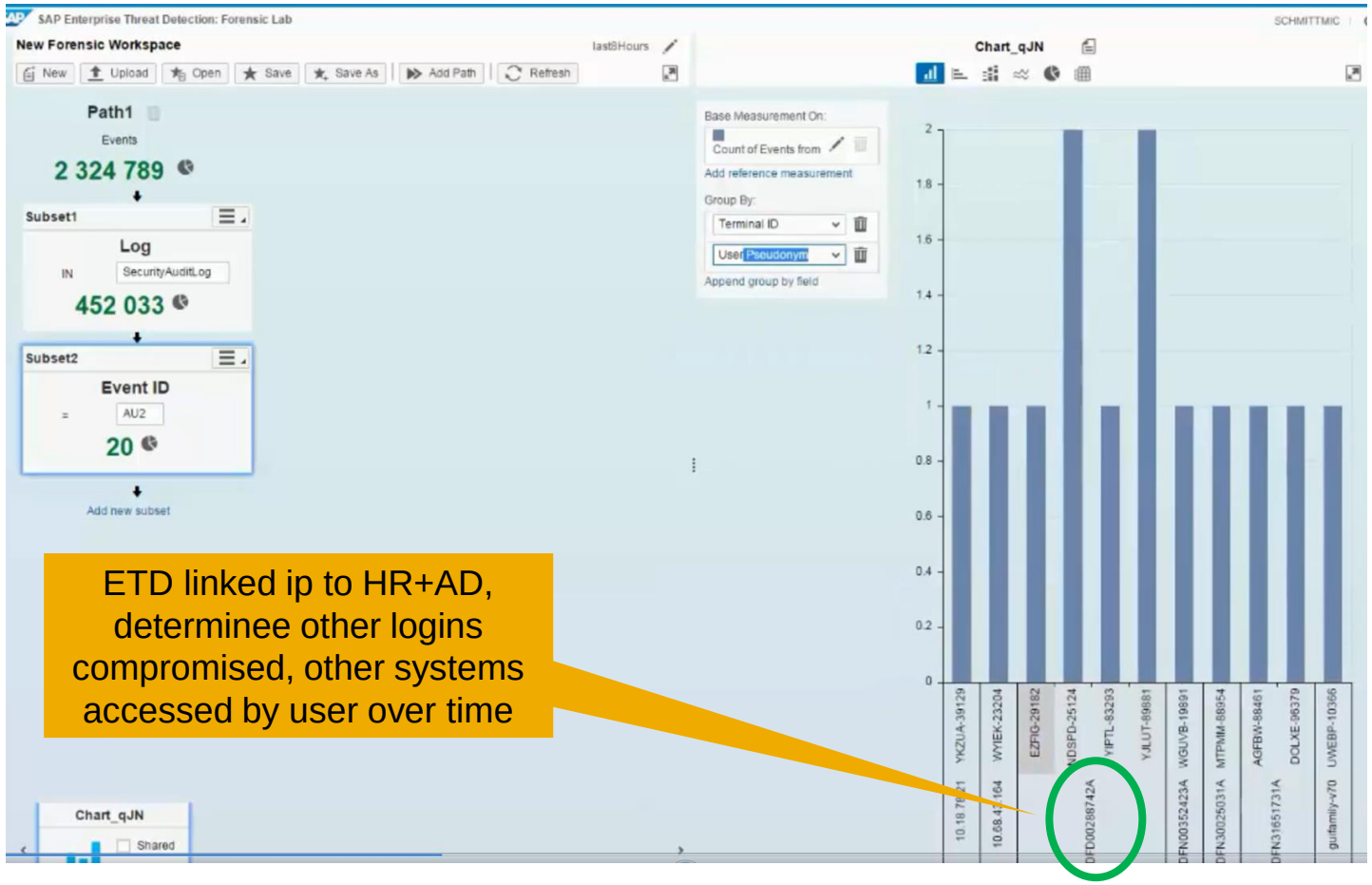
Cyber-attack Application changes raise alerts for analysis and investigation

3 ETD investigation team view data change script, determine malicious is true





Collaboration using Data - Deeper Contextual Analysis



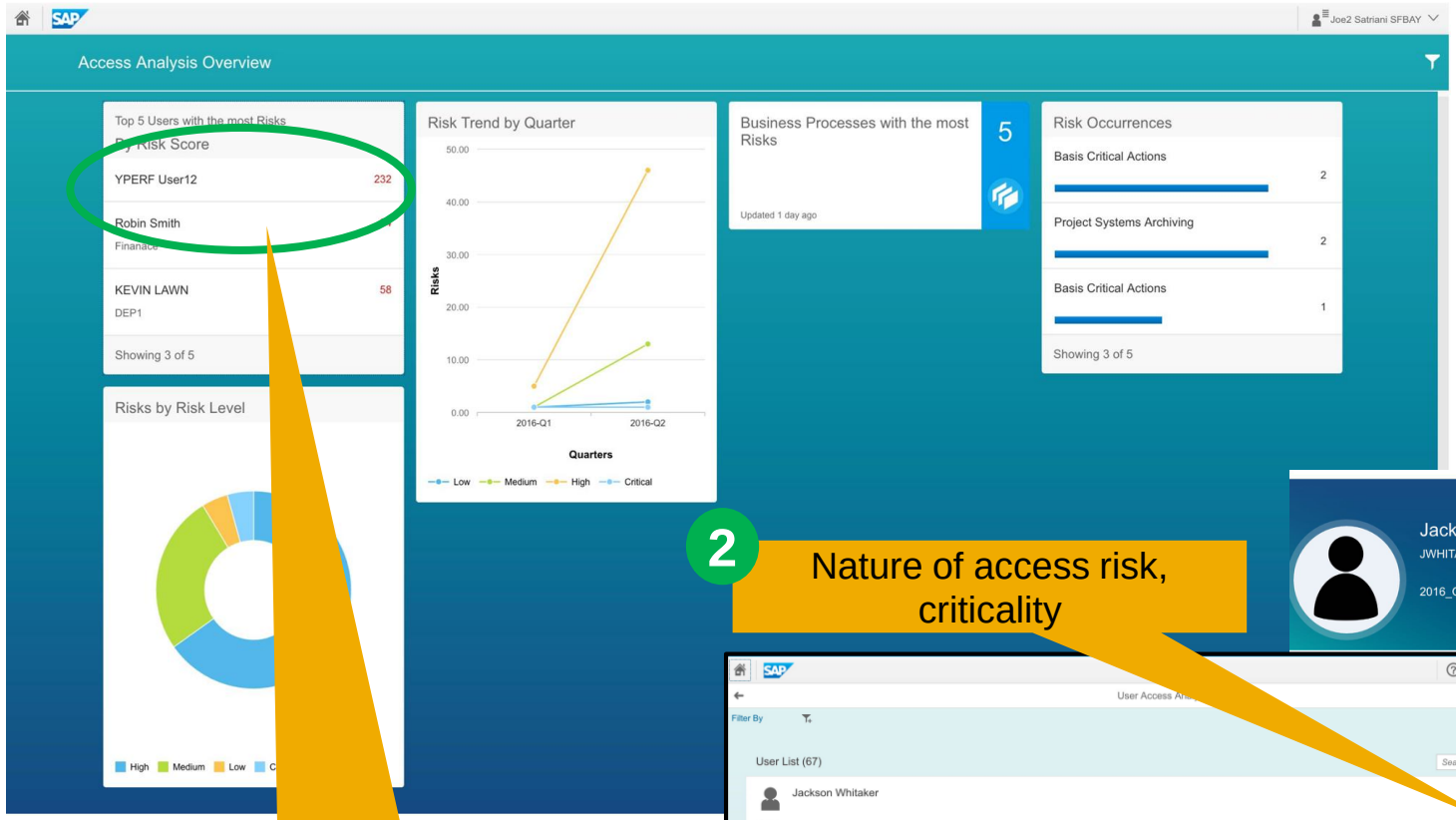
Compromised account may have performed other suspicious activity on other platforms, other applications.

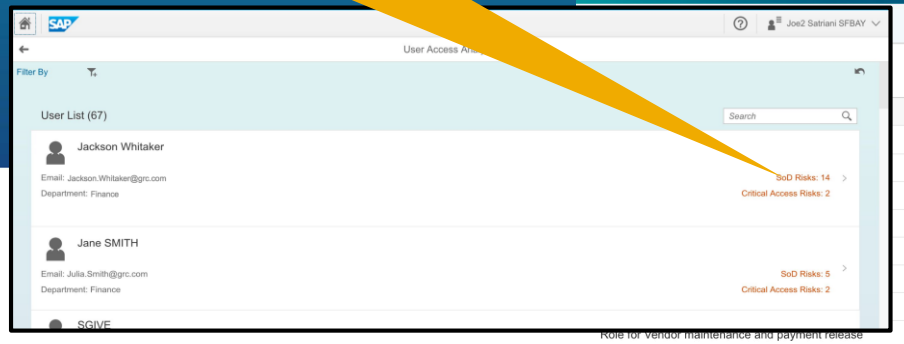
Pattern can be over several months.

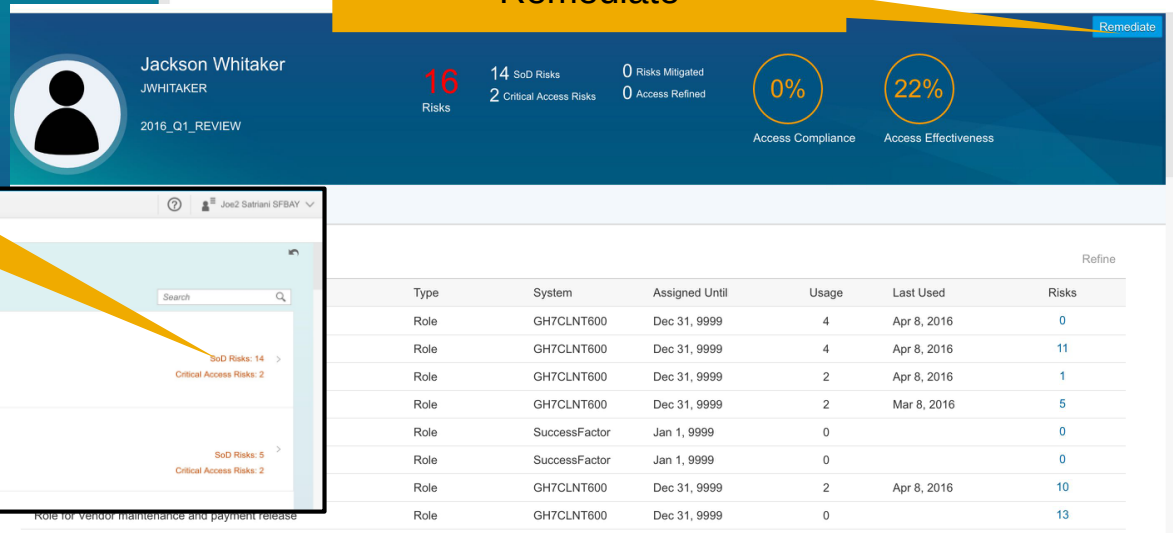
Unusual user behaviour:

- Sending emails with time threshold (e.g., after hours).
- >1 attachment/spike in volume of emails.
- Typical use is 9-5 Monday-Friday, weekend spike is unusual.

Example Dashboarding (System Access Violations)







1 Simple console for Access Permissions Violations

2 Nature of access risk, criticality

3 Remediate

Example central console for risk associated with data access, remediation.

Same can be achieved for financial transactions, combined reporting.

Platform Approach Adds Value, Agility, Assurance, Governance

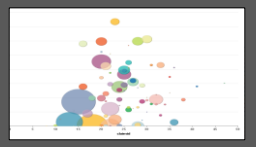
Insight and Monitoring

Information Cockpit

Analysis Workflow

Known patterns

Known 'bad' behaviours



Unusual behaviours

Similar, but different from known behaviours

Unknown /complex patterns

Unknown 'bad' behaviours

Cyber attacks and Patterns

Events and Patterns, & over time

- Known bad access
- Known bad transactions
- Master data changes
- Configuration changes

- Complex patterns, multiple rules
- Anomalies, geodata,
- Investigations

- Unknown patterns, rules
- Automated running of multiple analyses
- Propose causation, unstructured data

- Known bad threats
- Known bad patterns
- Application layer, logs
- Anomalous behaviour

Enabler

Data Aggregation and Early Warning Signals

In-memory

Data Sources

Thank you

Dr. Neil Patrick
COE GRC (EMEA)
SAP Governance, Risk and Compliance

neil.patrick@sap.com
www.sap.com/grc