SAP Security Group Deutschland

Xiting Kunden-Event
mit Partnern

9./10.
MAI
2023

SAP2SIEM - Wissen was passiert

Erfahrungsbericht der Allianz Technology über die Herausforderungen
bei der Implementierung einer SIEM-Schnittstelle

Bernhard Schulze (Allianz Technology) & Andre Tenbuß (Xiting GmbH)

parameters

- Projektart
- Architektur
- Aufwand
- Komplexität
- Fortschritt
- Dauer

HYBRID

S

M

AGENDA

1. Introduction Allianz Technology and Xiting
2. Xiting SIEM-Connector Fundamentals
3. SIEM Requirements (why?)
4. AZ Tech System Landscape (for whom?)
5. Target Architecture (how?)
6. Security Issues (what?)

Kapitel 1

Introduction Allianz Technology

Allianz

Allianz Technology at a glance

Facts from 2023

56%[1]

of Allianz' total IT spend with Allianz Technology

More than **12,000**[2]

employees worldwide

Presence in **51**

countries around the globe

814 services offered as **9**

simple product clusters

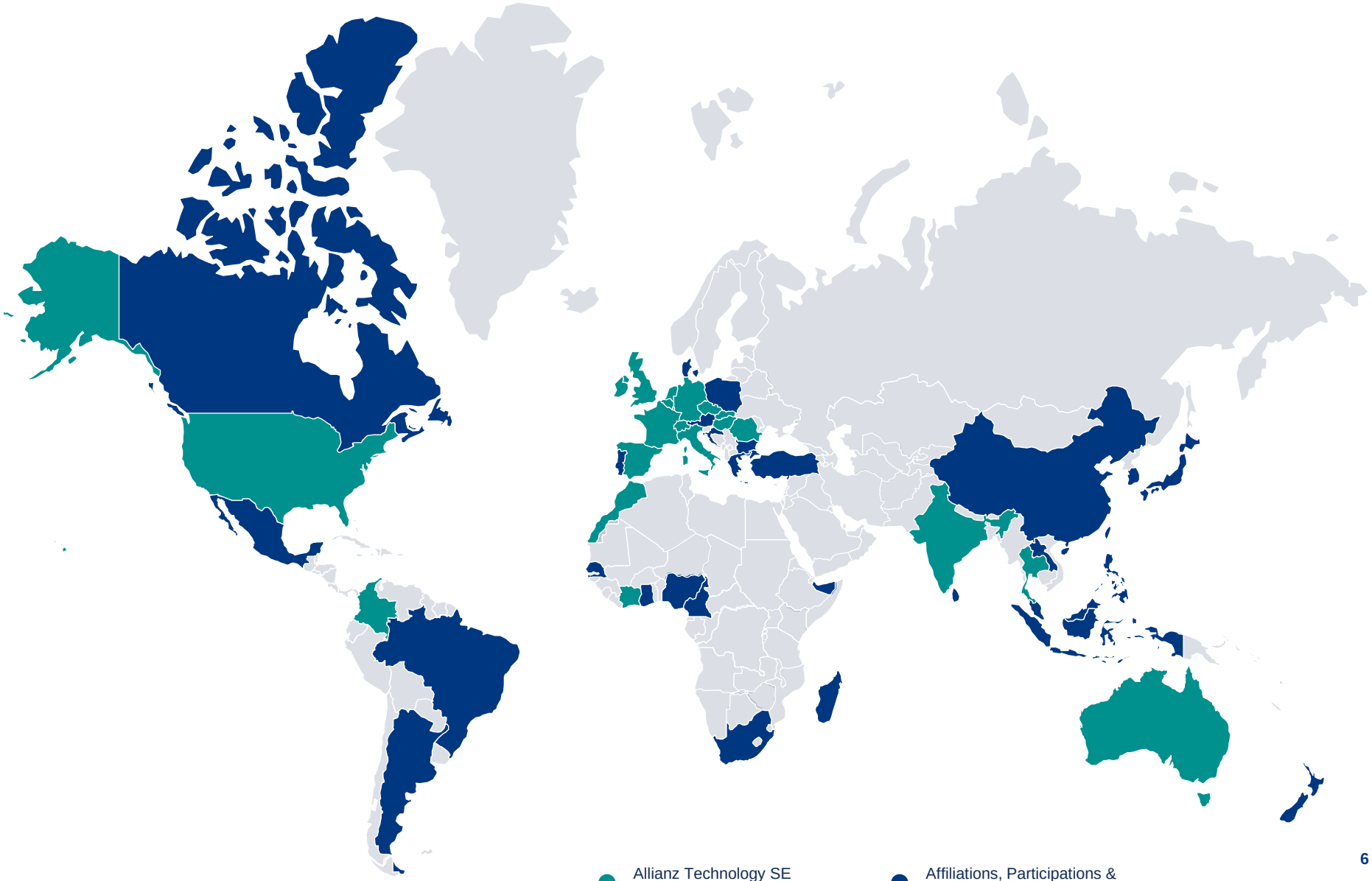
59%

of Allianz IT budget spent on target IT solutions

1. 4.3bn EUR total IT spend (insurance scope) in 2022FC
2 As of 2022FC

Our global presence

The Allianz Technology global footprint enables efficient service delivery worldwide and close interaction with OE business partners.



Kapitel 2

Xiting SIEM Connector Fundamentals

Challenges

Central Compliance Monitoring

Central landscape monitoring

The focus is on the central monitoring of safety-relevant settings and compliance with the defined processes

Overview and Drilldown Perspective

Extensive monitoring and auditing options as well as overview and detail perspectives

Real-Time Monitoring (RTM)

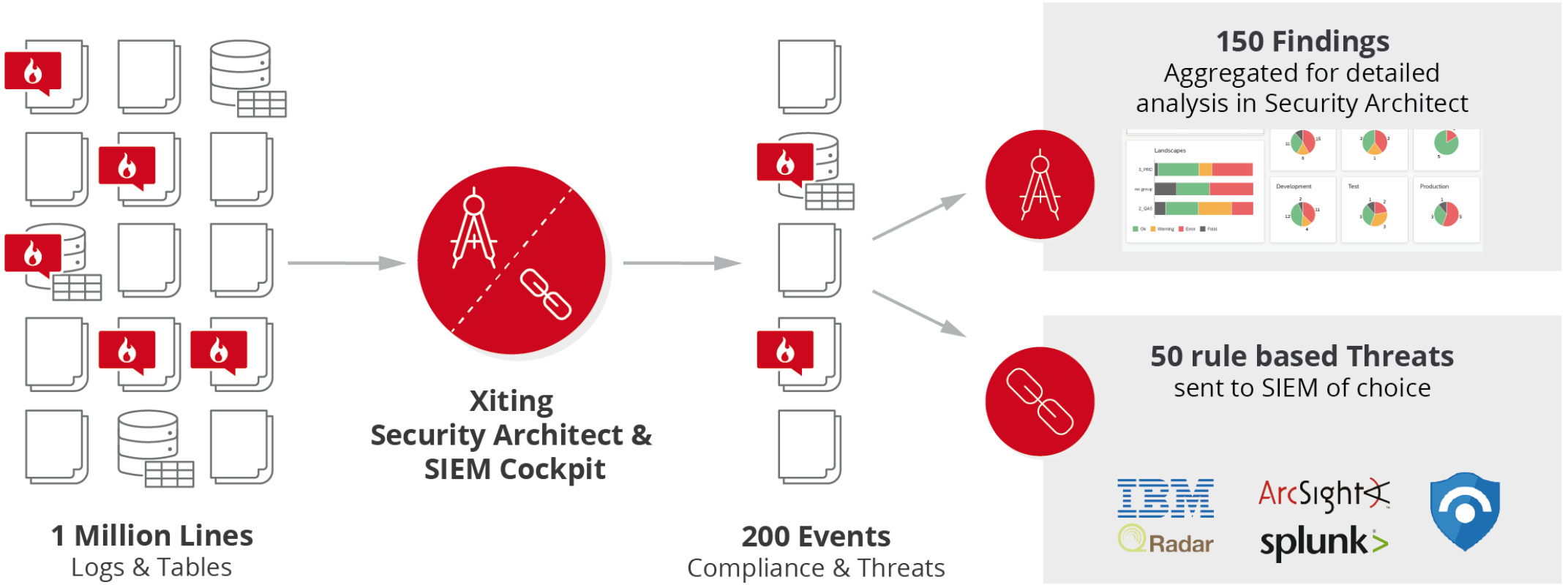
Report events to SIEM system

Focusses on immediate transfer of logs to connected SIEM system

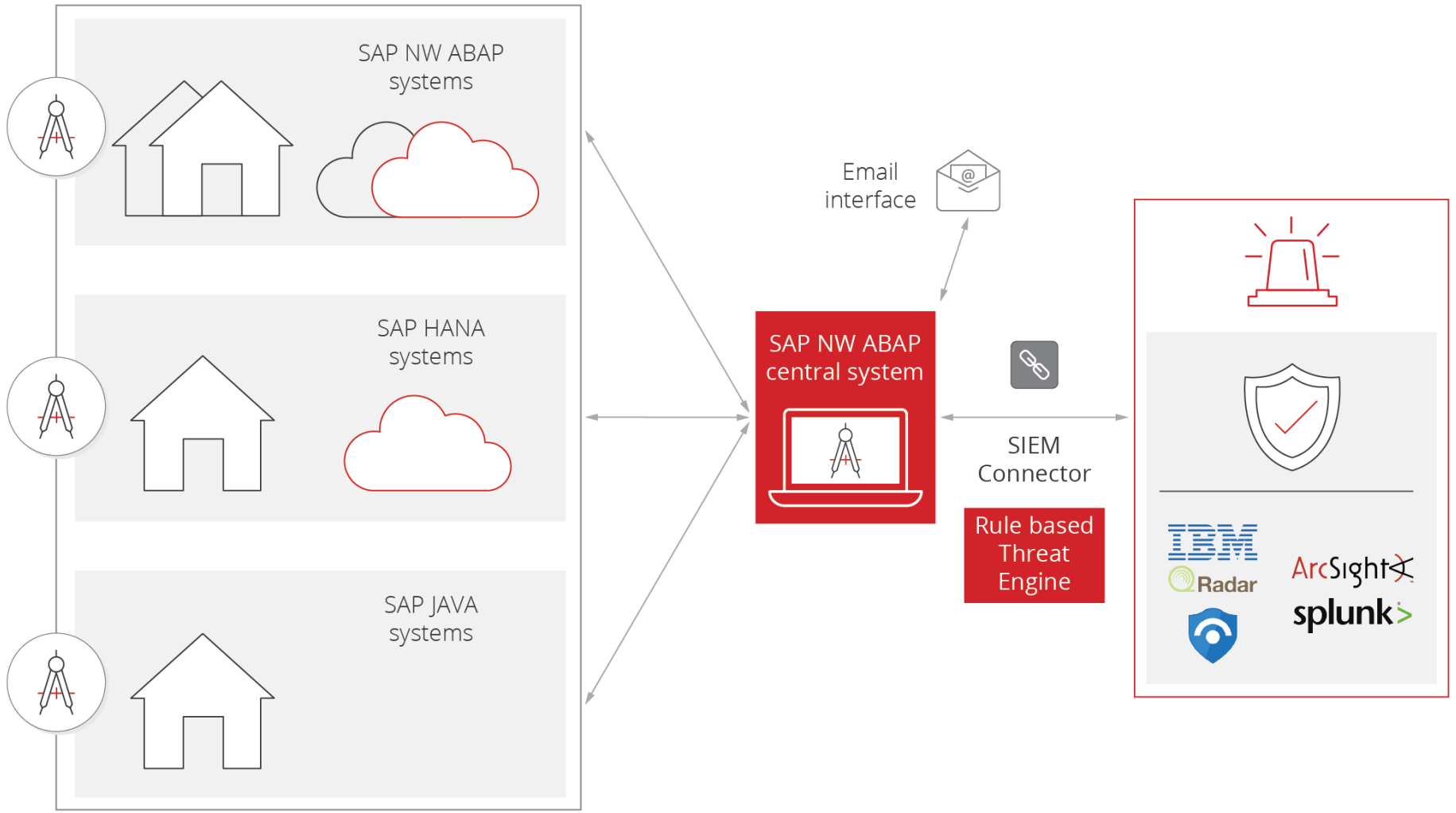
Threat-Intelligence

Complex Rule-based detection of suspicious activities in your SAP system through intelligent evaluation of log information

Principle



Architecture



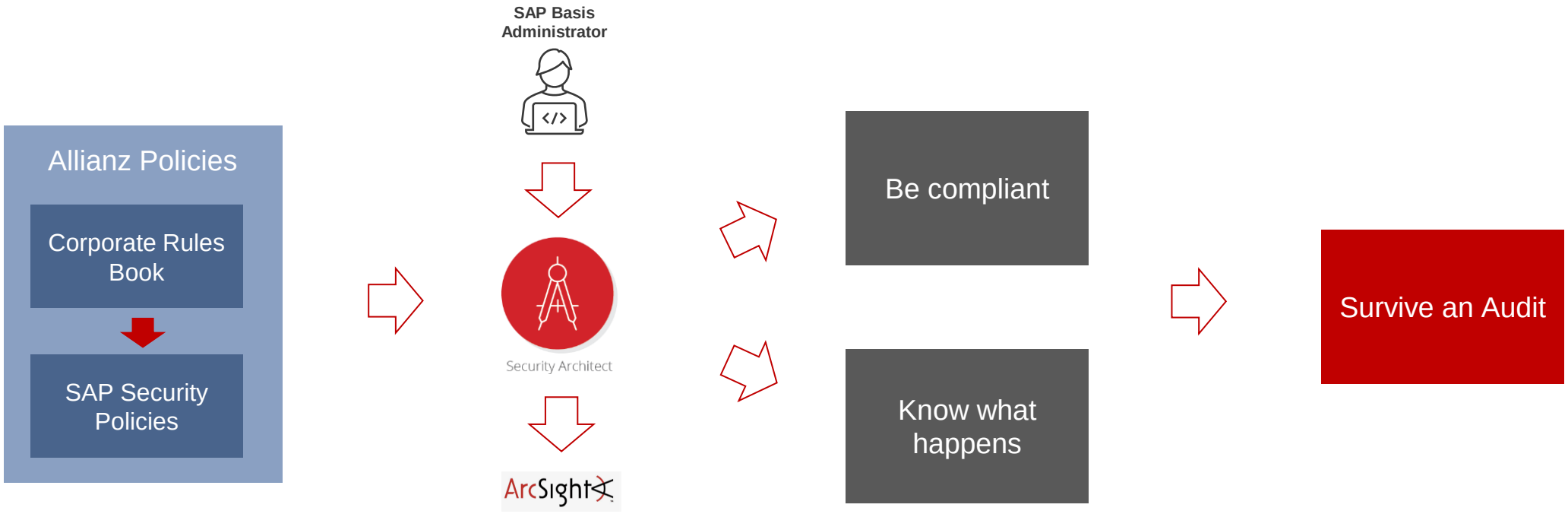
Standard Use Cases

- **Authorizations**
  - Assignment of critical roles
- **System configuration**
  - Changes to security-relevant system settings
- **Data leak**
  - View or extract data from confidential databases
- **Critical resources**
  - Calling prohibited transactions, programs and function modules
- **Debugging**
  - Debugging in productive systems including changing variables
- **Log settings**
  - Changing or deactivating SAP logs in order to conceal critical processes
- **SAP standard user**
  - Unauthorized use of SAP standard users

Kapitel 3

SIEM Requirements (why?)

AZ Tech SAP Security Essentials



Run Allianz Technology SAP systems compliant and secure

Kapitel 4

AZ Tech System Landscape (for whom?)

AZ Tech SAP System Landscape

Number of SAP systems	~ 90 (ABAP and Java stack)
Number of clients	~ 220
Supported SAP Netweaver Releases	7.00 to 7.57
SAP Service Owners	~ 20; multiple customers per Service Owner
Locations	On-Premises and Cloud (IaaS and SaaS)

Challenges

- One security solution for multiple SAP releases
- Huge number of SAP systems and SAP clients
- Multiple customers with local deviations and technical restraints
- “Hidden” security critical workarounds
- High number of false-positive alerts

The road to success:

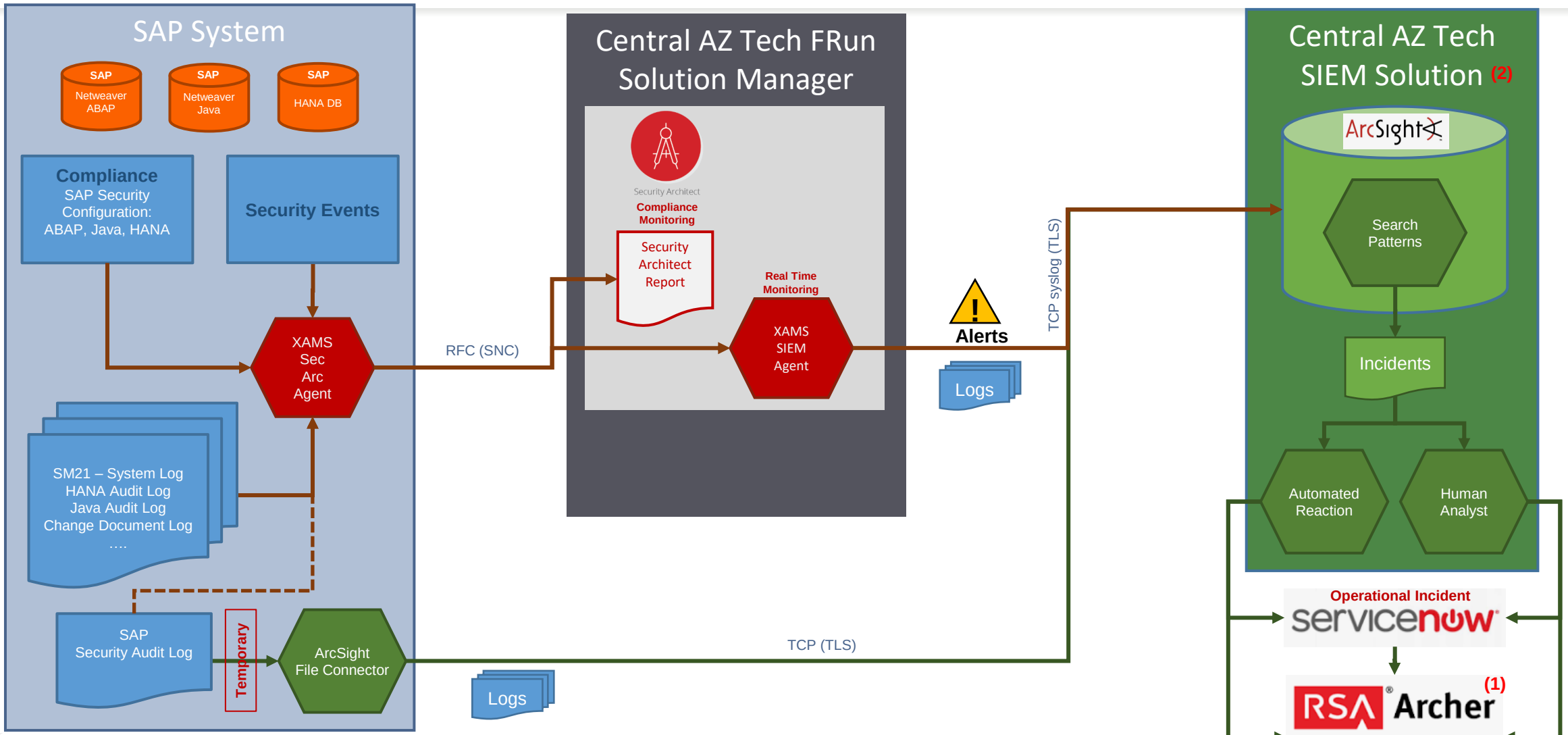
- **Standards**
- **Automation**
- **Deviation Handling**
- **Central Tool (information at your fingertips)**

One SAP Security Standard for all

Kapitel 5

Target Architecture (how?)

AZ Tech SAP Security Essentials



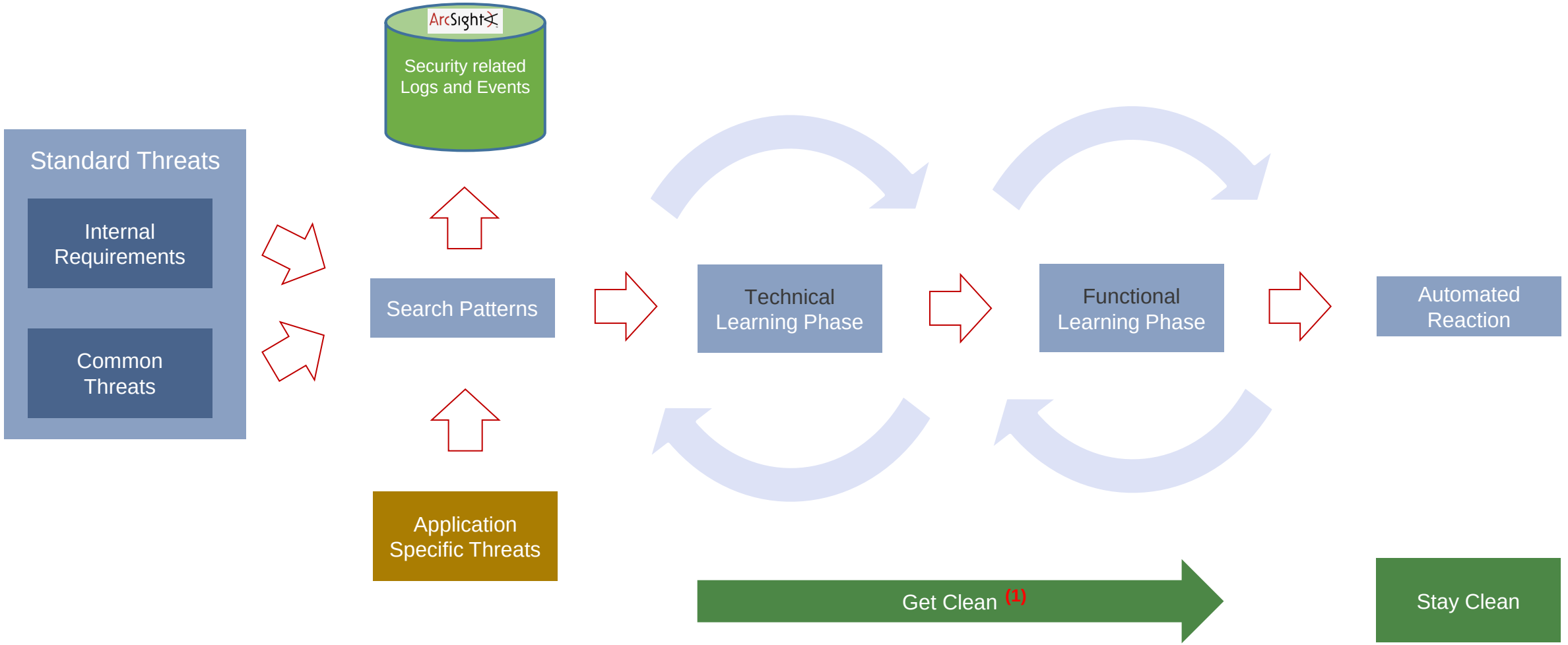
(1) Automatic information of the ISO of the responsible OE; Issue must be fixed within 72hrs.

(2) Class 1 standard

Kapitel 6

Security Issues (what?)

Search Patterns - General



(1) This may require the adaptation of existing processes

Avoid False Positive Alerts

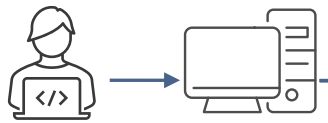
- Maintenance Mode
- Temporary deactivate SIEM Collecting
- Only for automated LaMa stop/start procedures

Security Architect

- Compliance Check after maintenance / configuration activities

Security Architect

SAP Basis Administrator

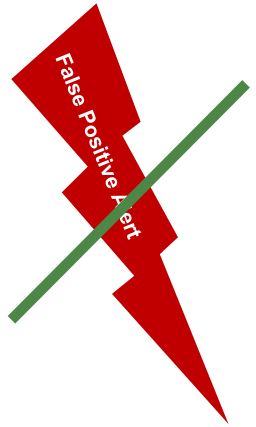


Upgrade

System Copy

Client Copy

Configuration



servicenow

- Standard service requests
- Temporary suppress only affected alerts in ArcSight
- Approval required

Procedures are in place to temporarily suppress alerts for approved activities

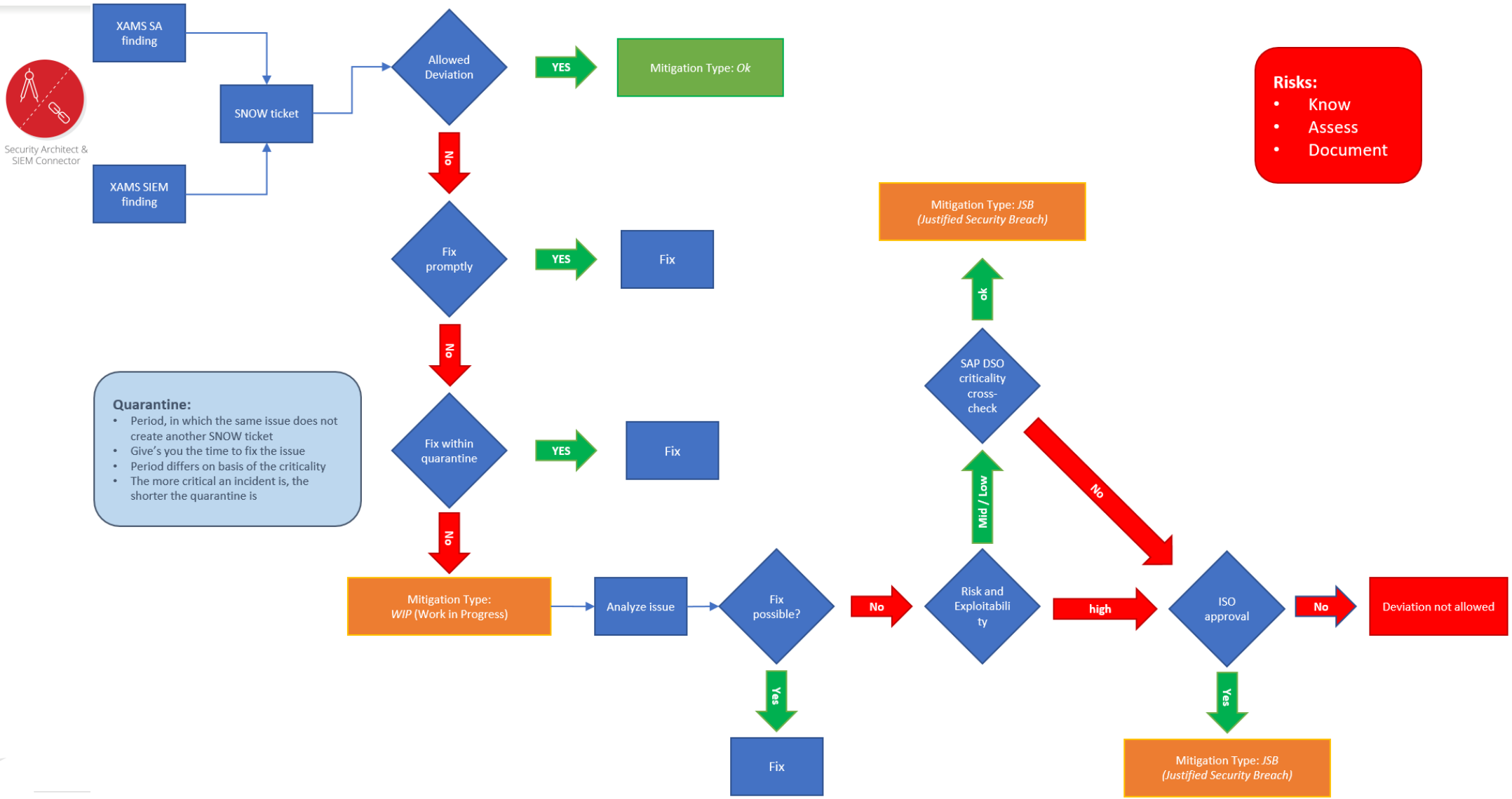
Zero False Positive Tickets

General Issues

- Reestablish security settings after a maintenance
- Activate and deactivate maintenance mode
- Maintain deviations:
  - Some deviations are permitted under certain conditions
  - If an issues can't be fixed promptly, use a temporary mitigation
  - Not all issues can be fixed →long-term mitigation (requiring an audit proof reason)

Set up processes to avoid false positive tickets

Incident Process – Workflow



Challenges (Tool independent)

Challenge	Problem	Recommended Solution
Technical		
▪ One security solution for multiple SAP releases ▪ High number of SAP systems and SAP clients ▪ Secure Run of the SIEM interface ▪ Why not only use the XAMS SA Maintenance Mode? ▪ Stable Run of the SIEM interface (sort out problems with RFC connections; system which do not answer may block the collection process)	▪ Full functions not for all systems ▪ Maintenance and Completeness ▪ Monitoring gaps ▪ Log based events detected in SIEM are not blocked ▪ Network problems may block collecting process; data loss	▪ Manual checks, SIEM alert suppression ▪ Central tool, checks (also completeness) and deployment ▪ Selected solution must support secure run ▪ Processes to temporary suppress only affected alerts ▪ Automated monitoring and restart of the SAPS2SIEM solution
Alerts		
▪ What shall we do with all the collected data? ▪ Who cares about the SIEM hits? ▪ Who cares about the Security Incidents created by SIEM? ▪ High number of false-positive alerts at the beginning ▪ Condition based alerts (e.g., parameter setting) ▪ Activation of changed security settings (restart)	▪ Data grave, miss threads and alerts ▪ Miss alerts, initiator is processor ▪ Nobody feels responsible, 7x24 ▪ Miss threads, huge number of tickets ▪ Recurring alarms in high numbers ▪ It can take a long time to fix issues	▪ Security awareness, talk with service owner ▪ Clean-up: Initiator; stay-clean: security team ▪ Security awareness, central security team ▪ Clean-up, start with limited search patterns ▪ Involve stakeholder early, define and implement mandatory standards, mitigations ▪ Quarantine on basis of criticality ▪ Temporary suppress affected alerts ▪ Transparence

Challenges (Tool independent)

Challenge	Problem	Recommended Solution
Security awareness		
▪ “Hidden” security critical workarounds ▪ Tension between ISO and local SAP service owners ▪ Multiple customers with local deviations and technical restraints ▪ Multiple local SAP Service Owners (responsible)	▪ Security breach, false-positive alerts ▪ Different “beliefs” about security ▪ Security awareness	▪ ISO support, mandatory standards, redesign ▪ The ISO is sometimes your friend 😉

Connecting to SIEM doesn't finish the job; just wait until something happens is not an option; you must take care about the logs and events

...last words

A secure infrastructure can only be physically achieved together with all stakeholders.

Without a general security awareness, you are lost.

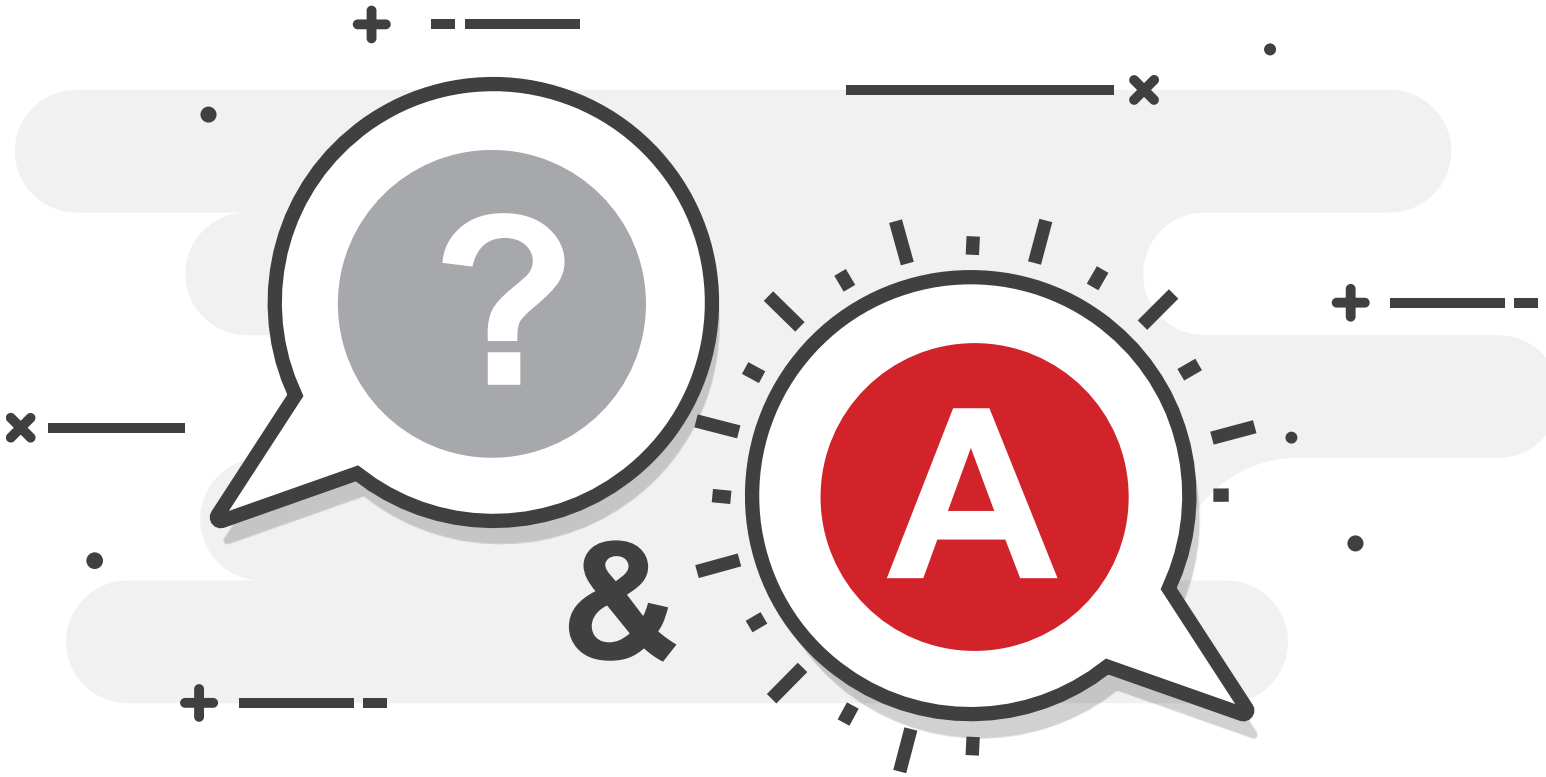
Standards and automation are the key to success.

The simpler the solution, the more time you have to focus on the security of your systems.

Outlook & Integration of new Functions

- **Reducing False Positive on SIEM side:**
  - Rule engine with best practice templates for patterns (definition of critical events)
- **Monitoring of Cloud Application:**
  - SAP BTP integration and log & event monitoring of cloud applications
- **Optimizing Data Load:**
  - Detailed analysis and filtering of logs for efficient and resource-saving monitoring

FRAGEN UND DISKUSSIONEN



Ansprechpartner

Andre Tenbuß

SAP Security Consultant

Xiting GmbH

Bernhard Schulze

SAP Technology CCoE

Allianz Technology

Wir sollten uns unterhalten

Sprechen Sie mit uns über Ihre Fragen und Anforderungen

Individuelle Demo

Vereinbaren Sie einen Termin für eine individuelle Demo mit uns

Proof-of-Concept Workshop

Wir stellen die Funktionalitäten des Werkzeugs in Ihrem SAP System vor

Security Konzept

Wir liefern Best Practices und entwickeln mit Ihnen ein nachhaltiges Security Konzept