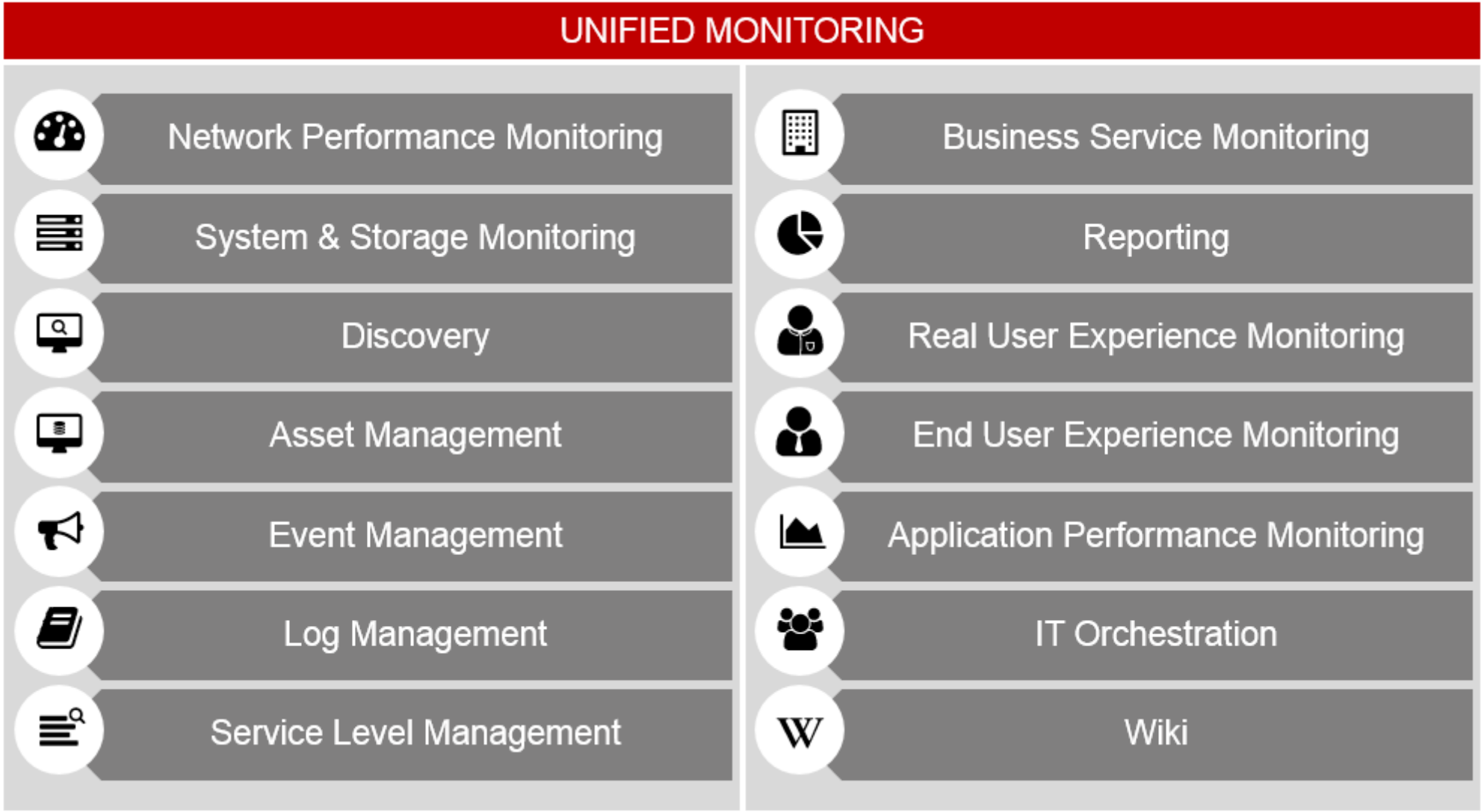
USERGOUP 2016

Neuheiten rund um das Unified Monitoring System NetEye mit Fokus auf Log Management

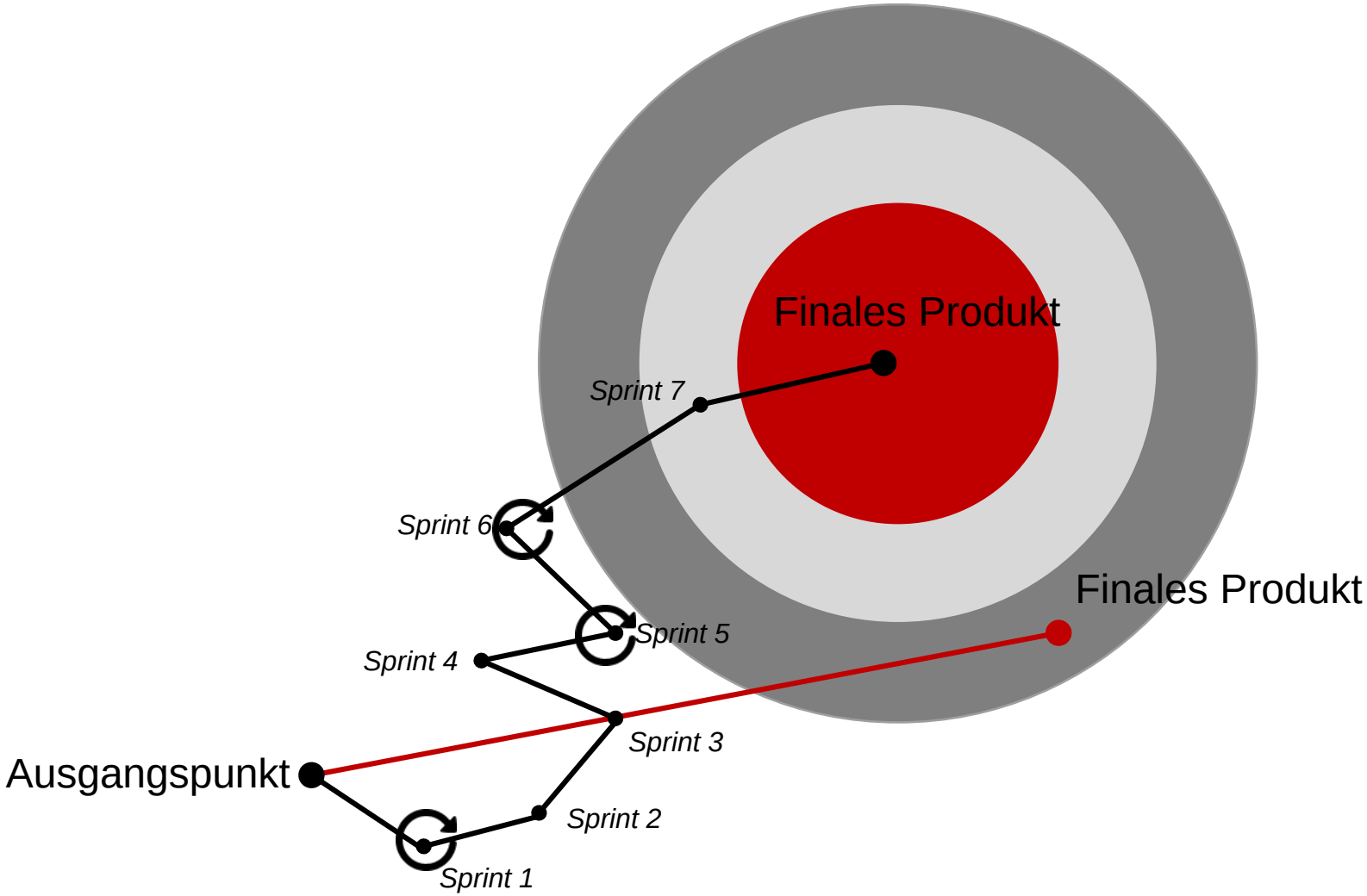
Georg Kostner

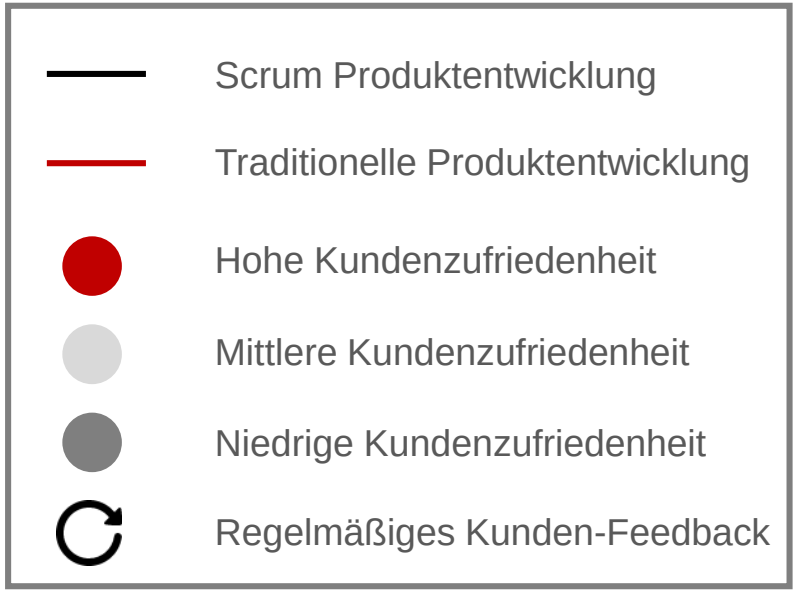
Ludwigsburg, 12. Mai 2016


UNIFIED MONITORING
Network Performance Monitoring
System & Storage Monitoring
Discovery
Asset Management
Event Management
Log Management
Service Level Management
Business Service Monitoring
Reporting
Real User Experience Monitoring
End User Experience Monitoring
Application Performance Monitoring
IT Orchestration
Wiki

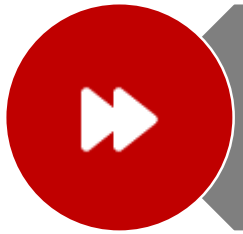
News rund um NetEye

Agile Produktentwicklung

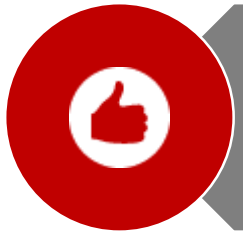




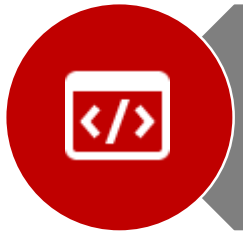
Neue Release-Strategie



Schnellere Durchlaufzeit der einzelnen Entwicklungsphasen durch kurze Entwicklungs-Sprints, welche getestete und funktionierende Software zum Ergebnis hat.



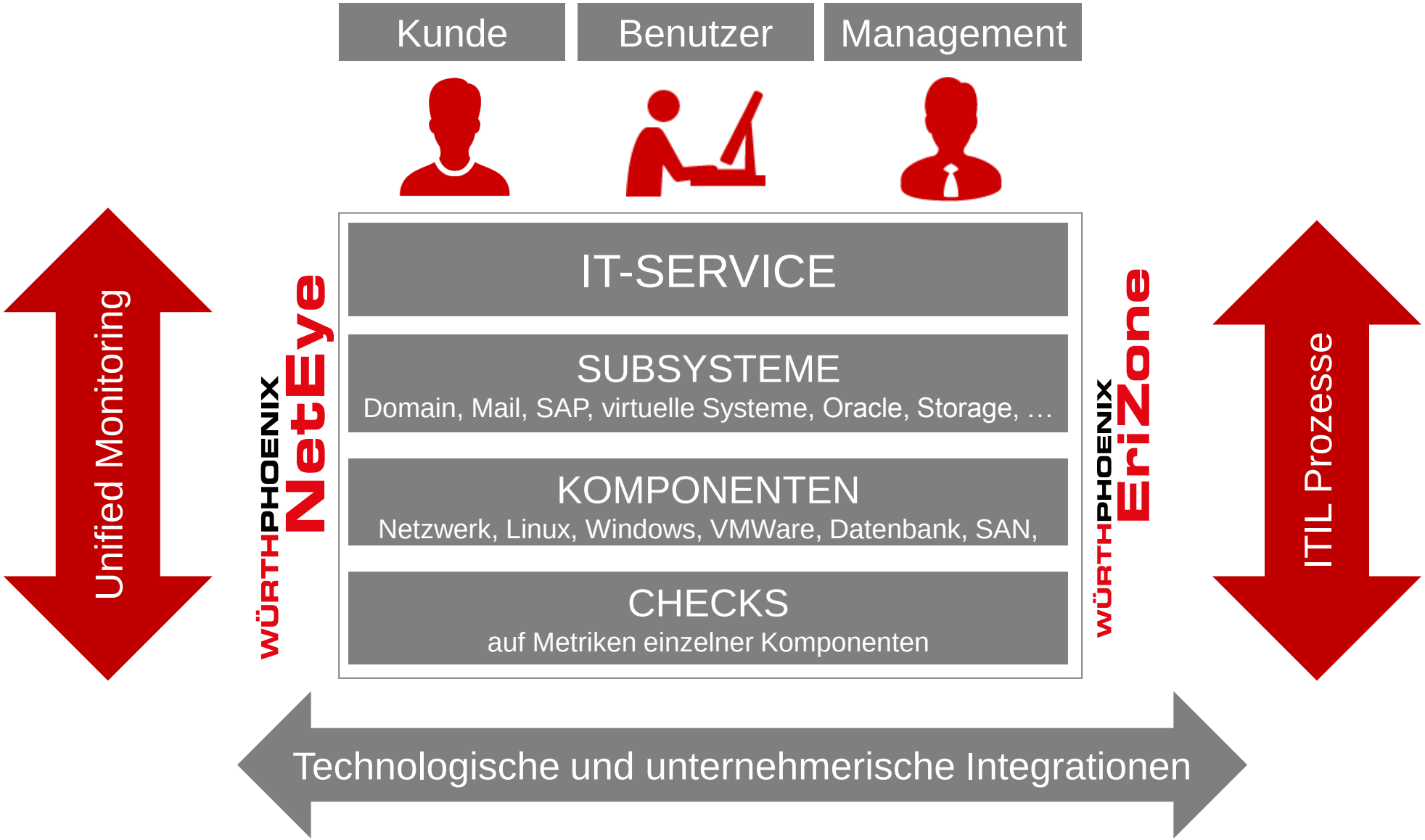
Steigerung der Qualität neuer Features durch die Einbindung der Stakeholder in den Entwicklungsprozess.



Verbesserung des bestehenden Quellcodes durch Pair Programming und Quellcode Reviews.

Bessere User-Dokumentation, durch die Integration der Erstellung der Dokumentation in den Entwicklungsprozess.

Effiziente Steuerung aller IT-Services



SLA – Event Correction

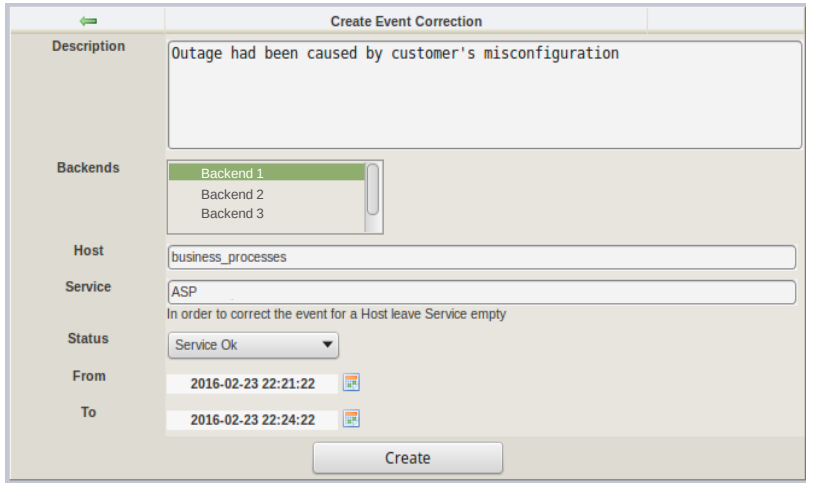
Beispiel: Downtimes können mit Informationen ergänzt werden. Wenn eine Störung nicht vom Service-Anbieter verursacht wurde, kann diese von der Berechnung der Einhaltung der SLAs ausgeschlossen werden.

Beispiel: Downtimes innerhalb der vorgesehenen Wartungsfenster können ebenfalls gekennzeichnet und nachträglich von der Berechnung der Einhaltung der SLAs ausgeschlossen werden.

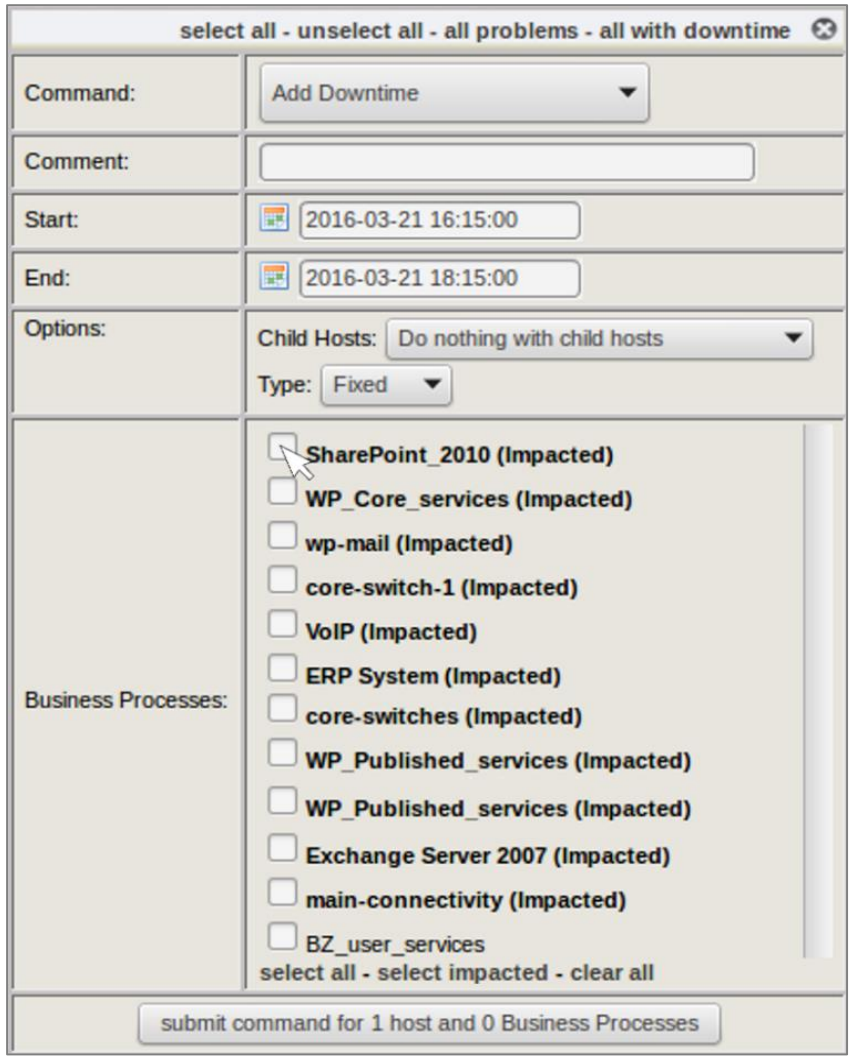
CRITICAL	Unscheduled	0d 0h 3m 0s	0.208%	0.208%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 3m 0s	0.208%	0.208%

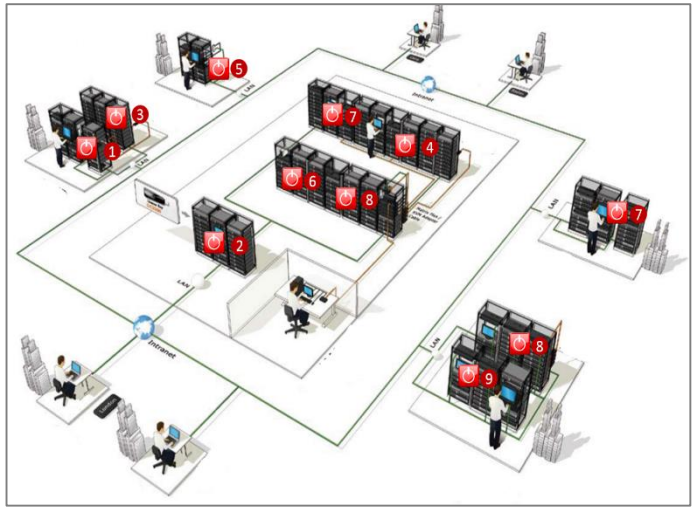
Event Start Time	Event End Time	Event Duration	Event/State Type	Event/State Information	Correct
2016-02-23 22:21:22	2016-02-23 22:24:22	0d 0h 3m 0s	SERVICE CRITICAL (HARD)	Business Process CRITICAL: ASP Tunap [pbzaspkx001:Disk Space: CRITICAL]	[correct]
2016-02-23 22:24:22	2016-02-24 00:00:00	0d 1h 35m 38s	SERVICE OK (HARD)	Business Process OK: ASP Tunap	[correct]
2016-02-24 00:00:00	2016-02-24 12:12:26	0d 12h 12m 26s+	SERVICE OK (HARD)	Business Process OK: ASP Tunap	[correct]

- Die nachträgliche Korrektur von Monitoring-Events unterstützt somit die Exaktheit der Berichterstattung in Bezug auf die SLA-Einhaltung.
- Diese Funktionalität wird auch bei der automatisierten Report-Versendung gewährleistet, wobei definiert werden kann ob die vorgenommenen Anpassungen berücksichtigt werden sollen oder nicht.



Verbesserung der Einplanung von Wartungsfenstern





Neben einer erheblichen Zeitersparnis hat diese Übertragung den Vorteil, dass auf einen Blick ersichtlich wird welche Prozesse aktuell nicht verfügbar sind und welcher Host oder Service dem Downtime zu Grunde liegt.

Konfiguration eines Business Prozesses, welcher als Auslöser für den Shutdown-Prozess fungiert

↓

Auswahl der Hosts, welche heruntergefahren werden sollen

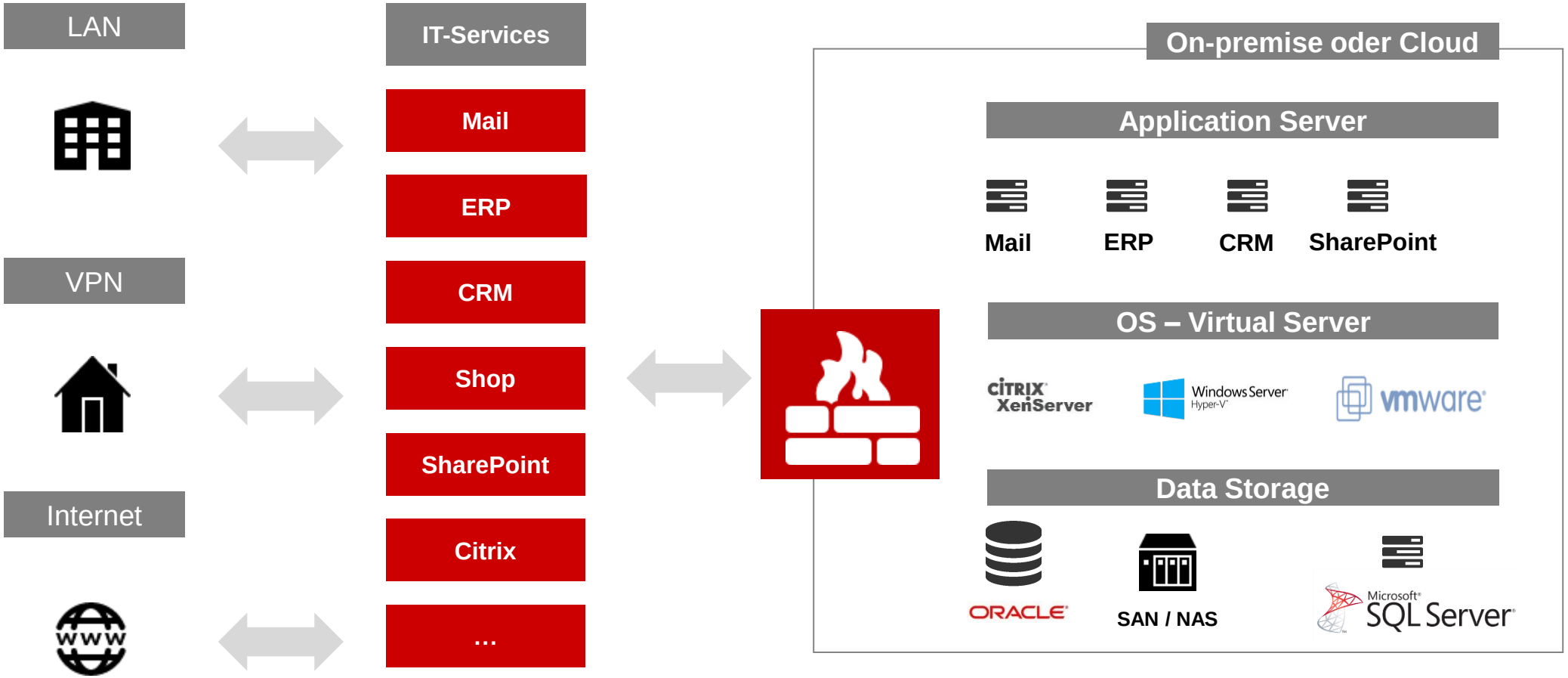
↓

Definition der Toleranzzeit vor Auslösen des Shutdowns

↓

Manuelle Bestätigung des Shutdowns (Optional)

Beispiel eines Service-Katalogs



Service Level Management

Darstellung des Einhaltungsgrades der SLAs als Tachometer

Aggregierte Darstellung aller Service Level

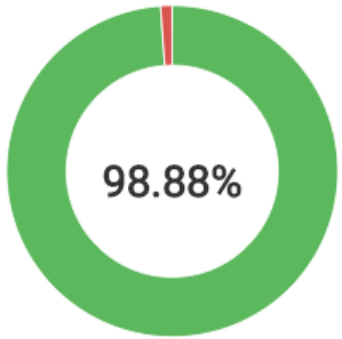
Tägliche Statistiken

SLA-Statistiken für einzelne Hosts und Service-Gruppen

Zeitleiste und interaktive Dashboards

SLA Reporting in NetEye

Availability SharePoint app and db servers (24x7)



Status report of 14.5.2015
Acutal period from **1.0.2015 0:0** to **1.0.2016 0:0** (1 month).
You arrived at 98.881% availability, with an SLA of 98.5%.

Status	Availability	SLA	
✓	98.88	98.50	98.881%

Availabiltiy of this year

Host	Service	SLA	Jan 2016	Feb 2016	Mar 2016	Apr 2016	May 2016	Jun 2016	Jul 2016	Aug 2016	Sep 2016	Oct 2016	Nov 2016	Dec 2016	12 Month
business_processes_detail	SharePoint app and db servers	98.50%	✓ 99.36%	✓ 98.91%	✗ 98.40%	✓ 99.02%	✗ 98.50%	?	?	?	?	?	?	?	✓ 98.84%

Availabiltiy of last year

Host	Service	SLA	Jan 2015	Feb 2015	Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015	Oct 2015	Nov 2015	Dec 2015	12 Month
business_processes_detail	SharePoint app and db servers	98.50%	✓ 99.05%	✓ 98.60%	✗ 98.40%	✓ 98.74%	✓ 98.88%	✓ 98.54%	✓ 99.15%	✗ 98.48%	✓ 98.81%	✓ 98.79%	✗ 98.47%	✓ 98.78%	✓ 98.72%

Log Management

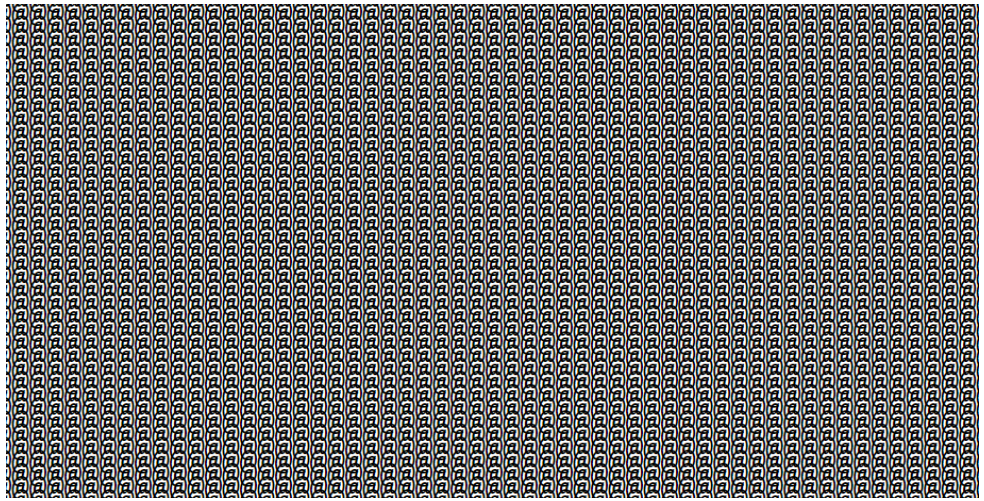
Herausforderungen in der Praxis

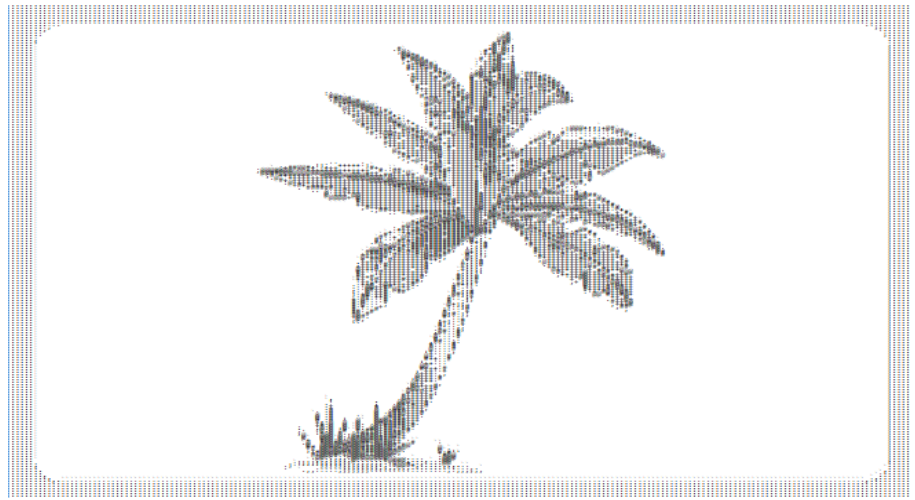
Die Komponenten Ihrer IT-Landschaft protokollieren sicherheitsrelevante Ereignisse und liefern somit eine riesige Menge nützlicher Daten.

Allerdings liegen die erfassten Logeinträge auf verschiedenen Komponenten und in unterschiedlichen Formaten vor und sind meist nicht aussagefähig genug, um auf konkrete Vorfälle schließen zu lassen. Noch dazu ist es bei mehreren Millionen Log-Zeilen pro Tag kaum möglich, die Übersicht zu bewahren.

Wie können diese Herausforderungen in Angriff genommen werden?

Mit dem NetEye Log Management unterstützen wir Sie, die sicherheitsrelevanten Informationen herauszufiltern und in den richtigen Kontext zu setzen – so können Sie sicherheitsrelevanten Events in Echtzeit erkennen und Sicherheitsvorfällen detailliert analysieren.





Security Information and Event Management (SIEM)

Gartner definiert SIEM als:

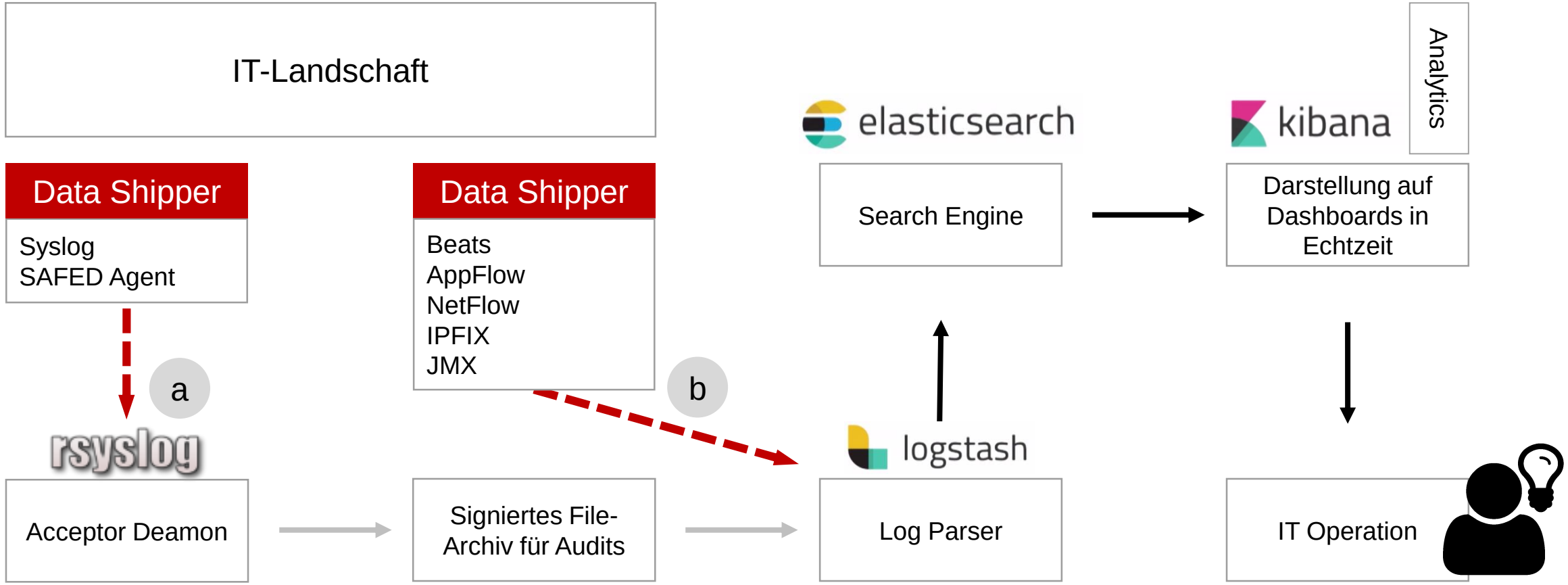
Security information and event management (SIEM) technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. It also supports compliance reporting and incident investigation through analysis of historical data from these sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources.

Security Information Management
Zentrale Sammlung und Langzeitspeicherung von Log-Daten für Trendanalysen

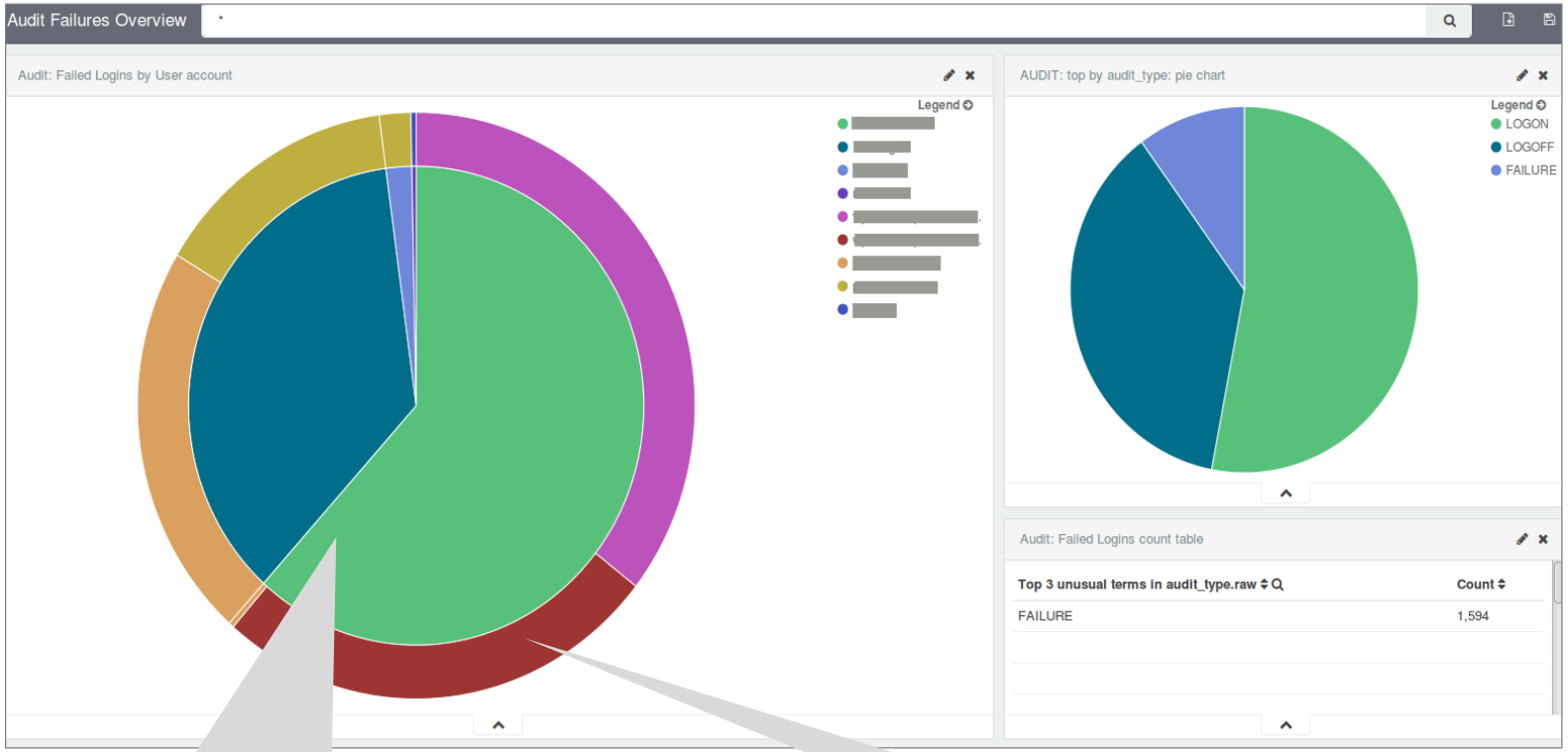
Security Event Management
Echtzeit Monitoring, Korrelierung von Events, Benachrichtigungen Visualisierungen

Lösungsansatz: NetEye Log Management

Heterogene Logs werden in ein **zentralisiertes, analytisches System** geladen, um über die Darstellung in live Dashboards, Analysen von Mustern und Anomalien zu ermöglichen.



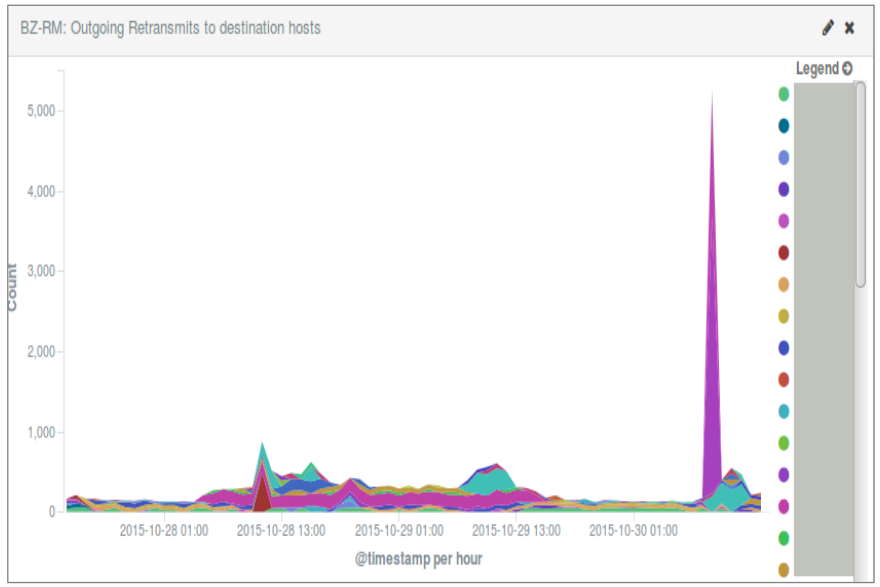
Daten werden zu Informationen



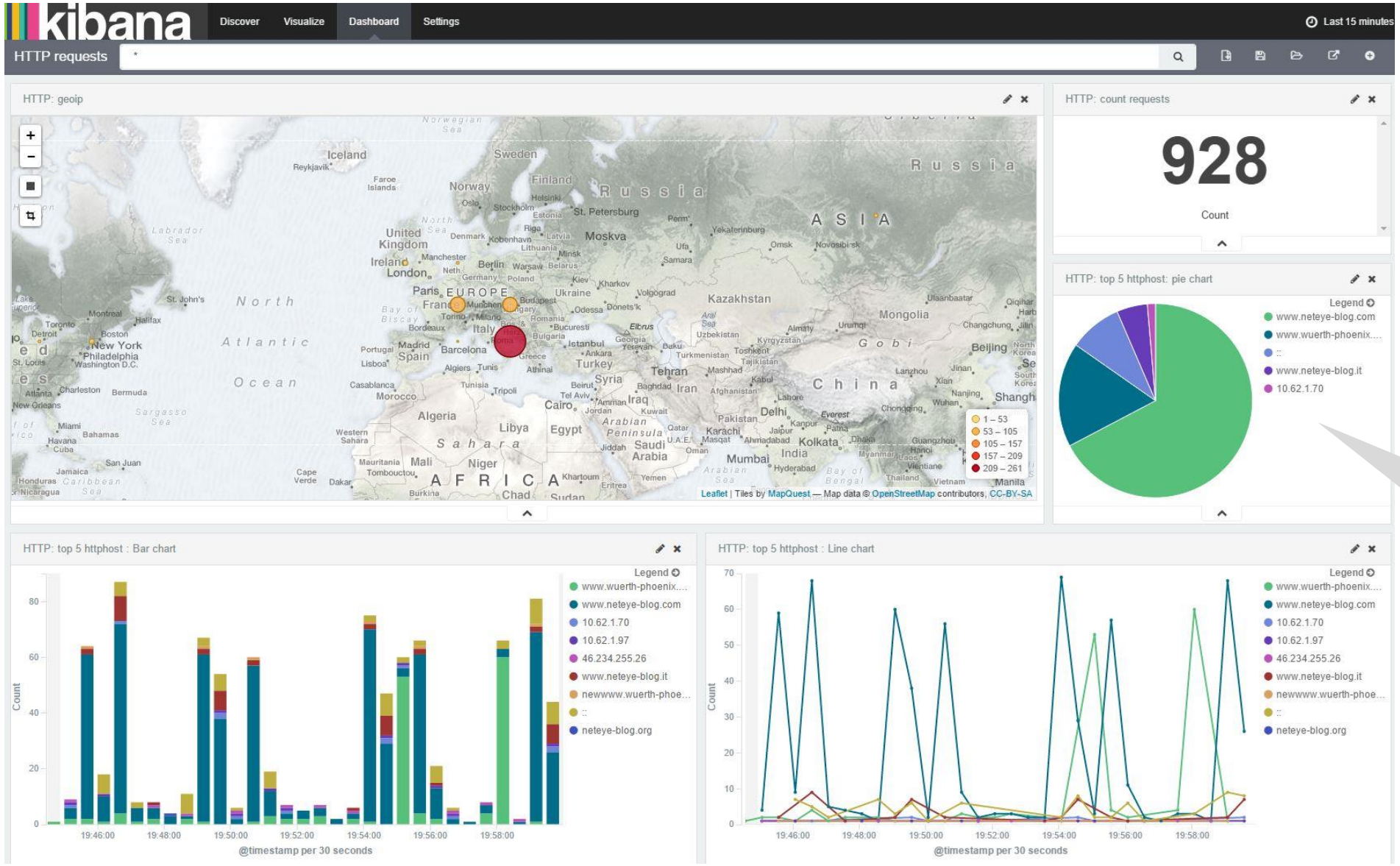
Drill Down der Hosts, auf welchen Login-Versuche vorgenommen wurden, die jedoch fehlgeschlagen sind.

Informationen zu den Benutzern welche den fehlgeschlagenen Logins verursacht haben.

Log-Analyse und Event-Korrelierung im neuen Log Management



NetEye Log Management: Anwendungsbeispiel Dashboards



Übersicht zu den Zugriffen auf die Webserver

Event Management: Auf Log-Ereignisse reagieren

URSPRUNG

Konfiguration der Senderkomponenten

paloalto NETWORKS, APACHE, STONESOFT, CISCO, SURICATA, OSSEC, SNORT, nBox, SAP, Microsoft, CITRIX NetScaler, Linux, ORACLE WebLogic, WebSphere, JBoss by Red Hat, +

TYPOLOGIE

Verschiedene Event-Typologien:

- LOG
- SMS
- E-Mail
- SNMP Trap
- …

REGELWERK

Definition und Konfiguration der Regeln für die verschiedenen Event-Typologien (Security Information & Event Management)

Rule Matching Engine

AKTIONEN

Definition verschiedener Aktionen:

- SNMP Trap
- Event Console
- SMS
- E-Mail
- Command
- Nagios
- Ignore
- …

Elastic Stack als Basis des Log Managements

Über 50.000.000 Produkt-Downloads

Die United Services Automobile Association analysiert täglich 3 - 4 Milliarden Events

Über 35.000 Open Source Product Commitments

Namhafte Kunden wie:

Otto, Xing, Audi, Orange, DHL, TomTom, Adidas, Teradata

Namhafte Kunden wie:

Facebook, Nasa, ebay, cisco, Goldman Sachs, SwissLife

Über 51.000 Community-Mitglieder weltweit

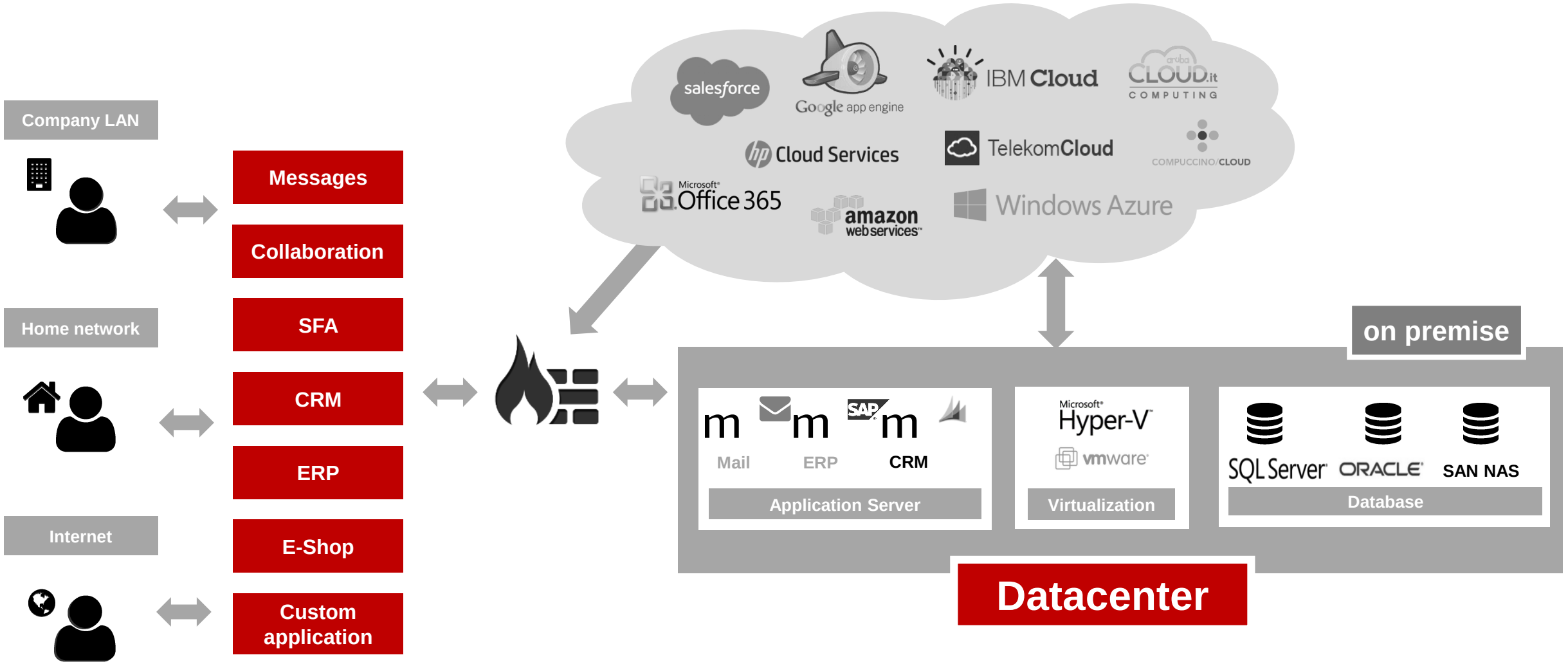
1.800 Teilnehmer auf der Elastic{ON}[16]

Vorteile des NetEye Log Managements

- Erweiterung des klassischen Monitorings
- Übersicht über alle Ereignisse der IT-Landschaft in Echtzeit
- Erkennung von Anomalien
- Hervorheben von Mustern
- Datenbasis für Audits

Real User Experience

Die wachsende Komplexität in der Verwaltung der IT-Dienste



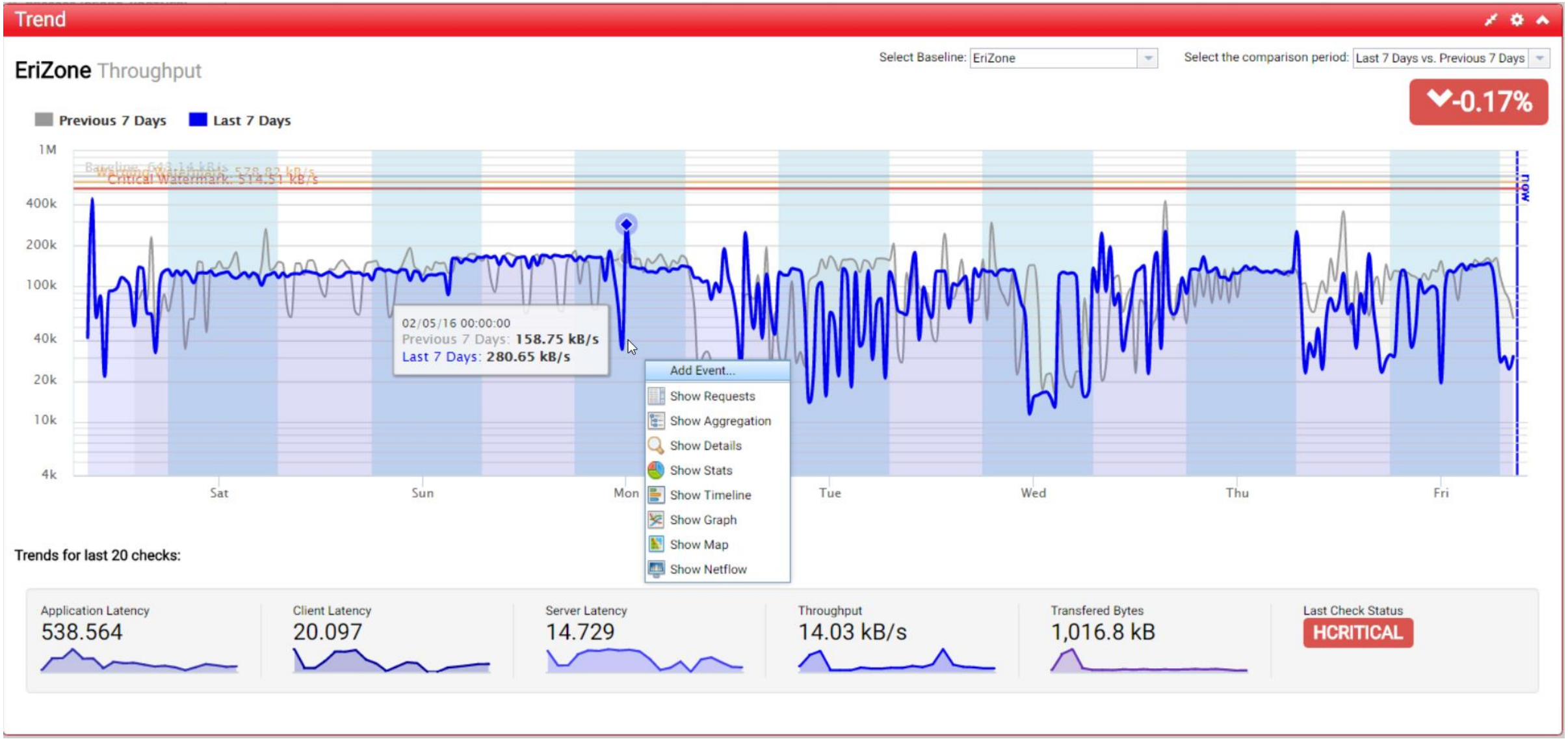
Erhöhte Komplexität in der Verwaltung von Netzwerken

Die massive Anwendung von Virtualisierungen, Cloud und mobiler Geräte hat die Komplexität der Verwaltung von Netzwerken erhöht.

Forrester Research: "31% der Leistungseinschränkungen benötigen mehr als einen Monat um gelöst zu werden oder werden gar nie gelöst."

6 Schritte einer Performance Monitoring Strategie

RUE Dashboard für EriZone

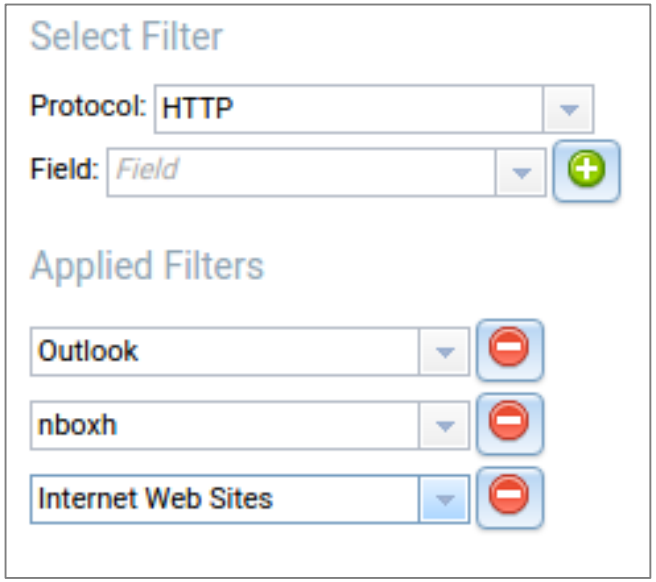


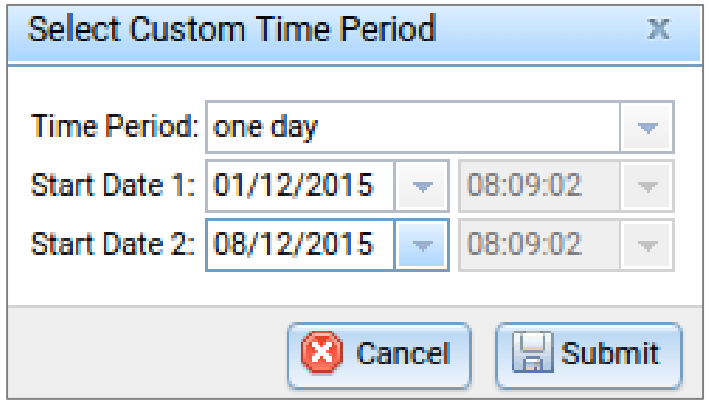
Gezieltere Analysen durch die Definition individueller Filter

In RUE werden aus den gesammelten Daten Leistungsindikatoren (KPIs) errechnet.

Diese Indikatoren, können aggregiert werden, um aussagekräftige Information abzuleiten.

Die Verwendung individueller Filter ermöglicht die gezielte Bewertung, um zutreffende Aussagen in Bezug auf die Netzwerk- und Application Performance treffen zu können.





Zur Verfolgung der Performance-Entwicklung über einen längeren Zeitraum und zur Abbildung von Leistungsveränderungen, ist es notwendig die erfassten Werte zweier Zeitspannen grafisch gegenüberzustellen.

Um diese Vergleichsmöglichkeiten zu erweitern können die Vergleichsperioden ab RUE 1.9 individuell eingestellt werden.

NetEye Real User Experience 1.9

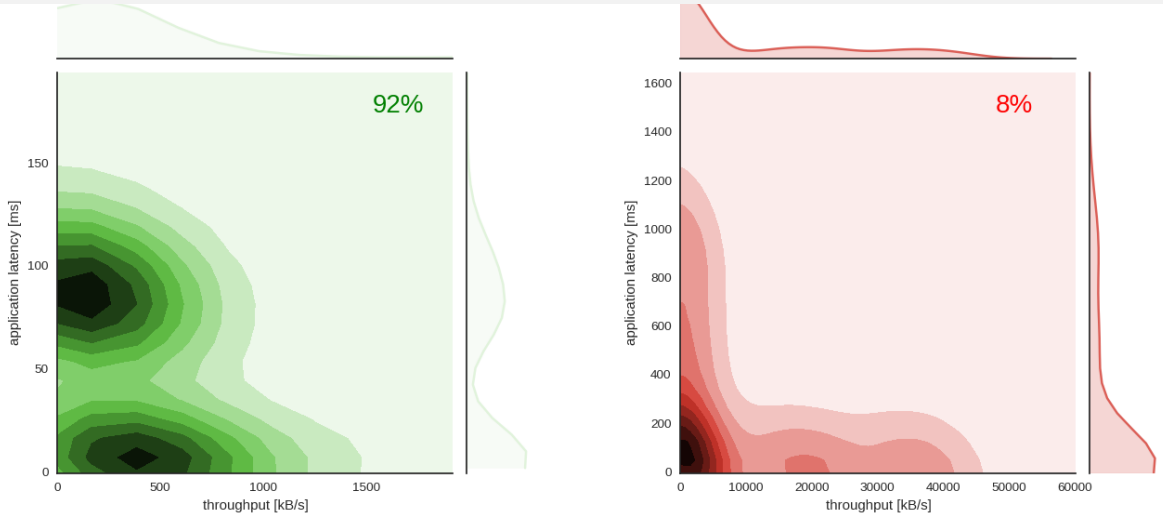
Neue KPIs
Explicit Congestion Notification
Inflight Bytes

Neues Konfigurationspanel für die Netzwerk-Sonde, sowie Wiederherstellung früherer Konfigurationen

Machine Learning Plots zur Darstellung der RUE Trends

Density Plots

Density Plots eines Tages; 92% sind dichter Standardtraffic (linke Grafik in grün), 8% werden als weniger dichter Traffic (rechte Grafik in rot) detektiert.



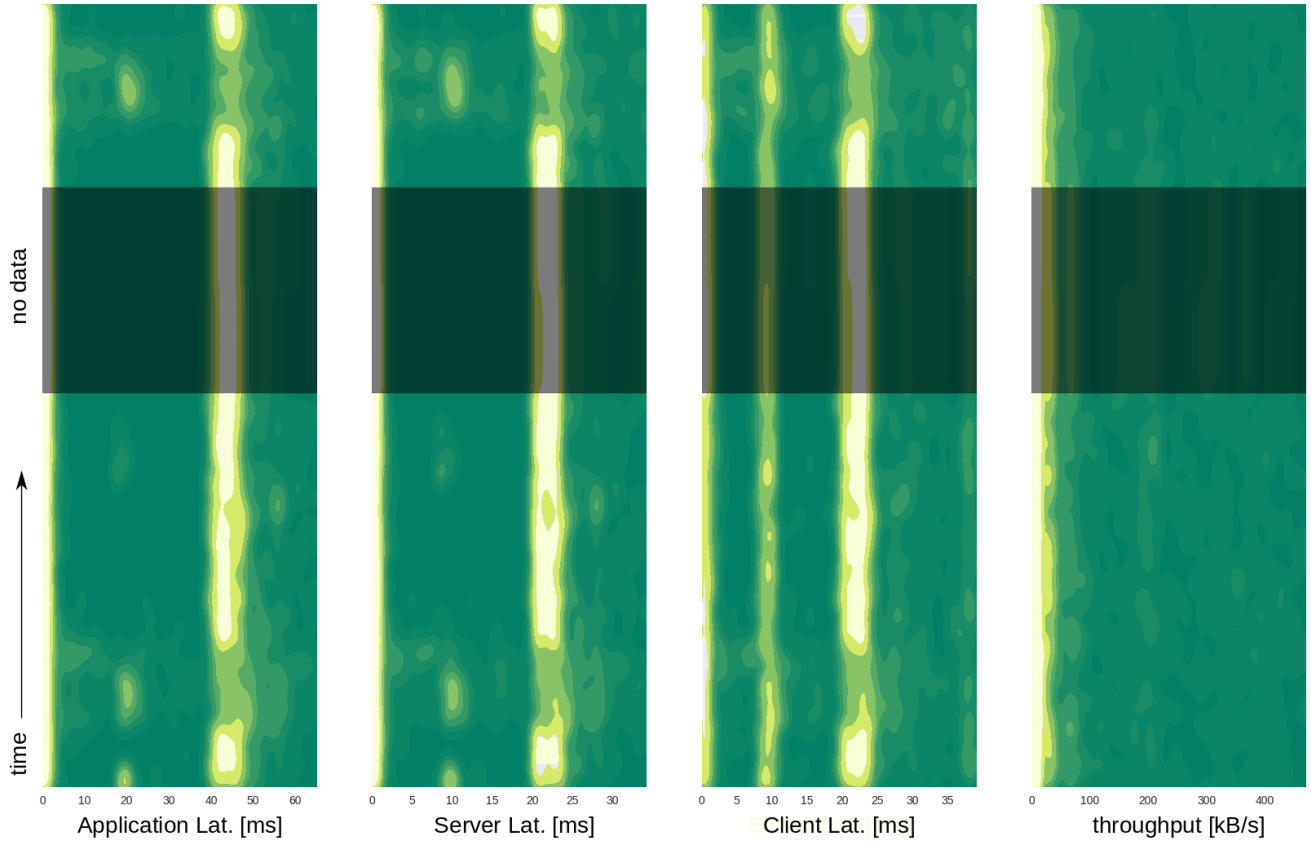
Es ist sehr wahrscheinlich, am zu untersuchenden Tag, Anfragen mit einer Applikationslatenz von ca. 90 ms und einem Durchsatz von 150 kB/s zu finden, alternativ treten Anfragen mit einer Applikationslatenz von 10 ms und einem Durchsatz von ca. 400 kB/s auf. Die Wahrscheinlichkeitsverteilung der Applikationslatenz hat zwei Maxima. Es gibt auch Anfragen mit viel extremeren Werten was Durchsatz bzw. Applikationslatenz betrifft, aber diese extremeren Werte machen am zu untersuchenden Tag maximal 8% des totalen Traffics aus.

Data Trends

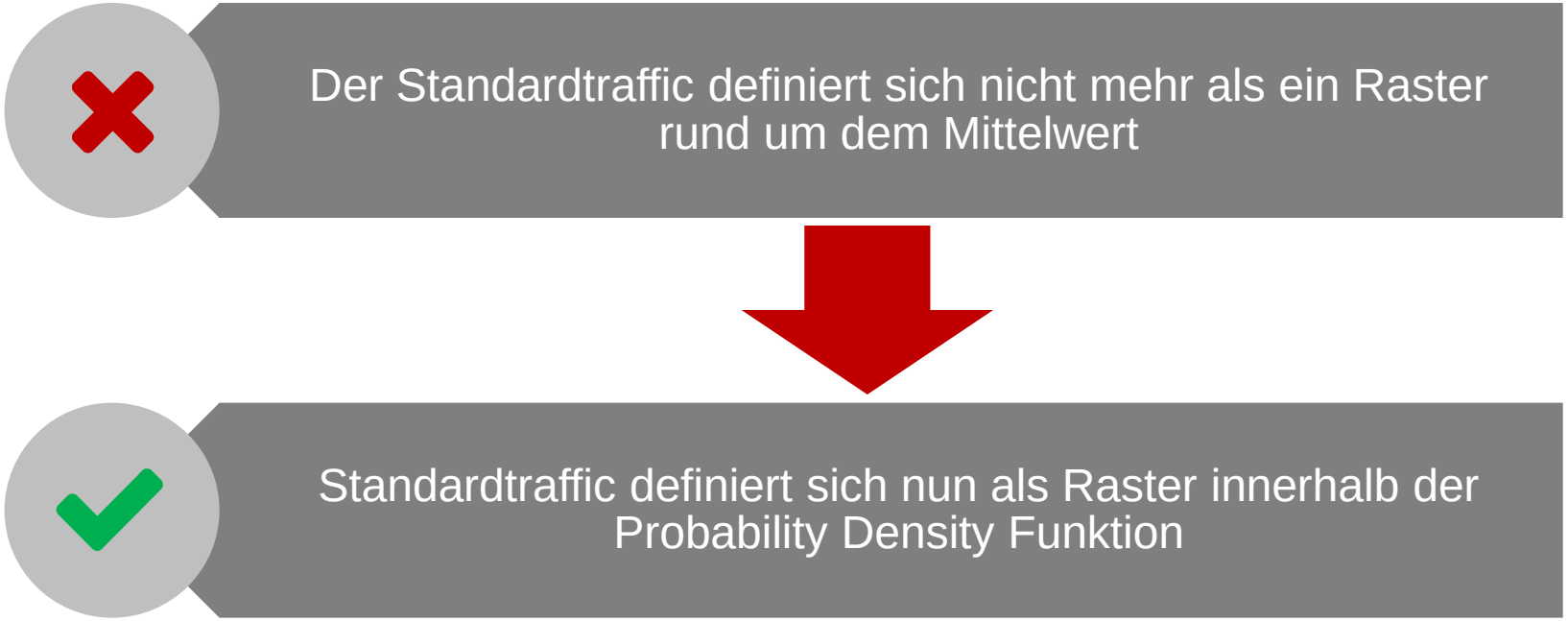
Performance Trends: Traffic ist an den zu analysierenden Tagen annähernd konstant (Applikationslatenz: 42 ms, Serverlatenz 22 ms, Clientlatenz 22 ms, Durchsatz< 25 kB/s).

Neben den sehr häufigen Werten treten bei allen Latenzen auch Werte von annähernd 0 ms auf. Im Fall der Clientlatenz koexistiert Traffic mit ca. 10 ms neben dem bereits beschriebenen.

Es handelt sich allerdings um weniger Anfragen als bei denen die um die 22 ms liegen. Von einem kurzen Zeitraum liegen keine Daten vor, der Bereich wurde grau überlagert.

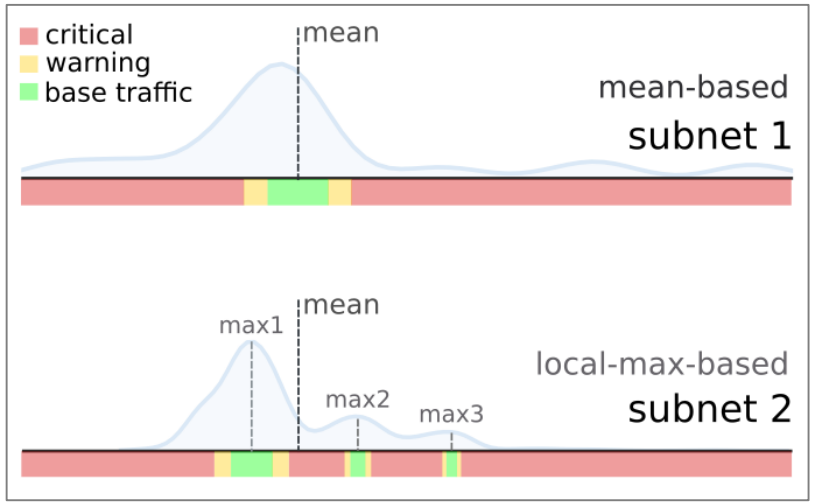


Neue Definition des Standardtraffics



Ergebnis: effektiver Alarm für die Lösung

Density plots - Throughput



Id	Name	Avg Throughput	Avg Load time (ms)	Avg App Lat (ms)	Avg Server Lat (ms)	Avg Client Lat (ms)	Avg Requests/min	Requests	Impacted clients	Attempt	Last Check	Status
	No filter applied											
4	Outlook	0.0B/s	138,887,1...	694.032	2.584	93,329,37...	15.8	79	28/28	193	16/06/15 11:41:00	HCRITICAL
5	Main Web	266.4k/s	163.010	41.086	16.396	54.221	53.6	268	13/13	65535	16/06/15 11:41:00	HCRITICAL
6	Trendmicro Update	124.3k/s	358.039	187.647	11.314	1.970	37.4	187	11/11	211	16/06/15 11:41:00	HCRITICAL
8	Fime App	309.1k/s	218.446	63.942	15.723	32.507	220.6	1,103	7/7	24	16/06/15 11:41:00	HCRITICAL
12	Skype	0.0B/s	13,627,95...	76.470	4.167	11,027,75...	142.0	710	24/24	189	16/06/15 11:41:00	HCRITICAL
13	NetEye Updates	44.4k/s	82.603	1.755	0.117	40.424	16.0	80	5/5	1637	16/06/15 11:41:00	HCRITICAL
14	CIS	0.0B/s	106,240,2...	66.827	10,910,50...	72,563,11...	32.8	164	2/2	792	16/06/15 11:41:00	HCRITICAL

Effektive Alamierung

USERGOUP 2016

Neuheiten rund um EriZone, dem Ticketing-System zur Implementierung von ITIL-Prozessen

Georg Kostner

Ludwigsburg, 12. Mai 2016

ITIL Prozesse

Service Design

- Service Catalogue Management
- Service Level Management
- Capacity Management
- Availability Management
- IT Service Continuity Management
- IT Security Management
- Supplier Management

Service Transition

- Change Management
- Change Evaluation
- Service Asset and Configuration Management
- Knowledge Management

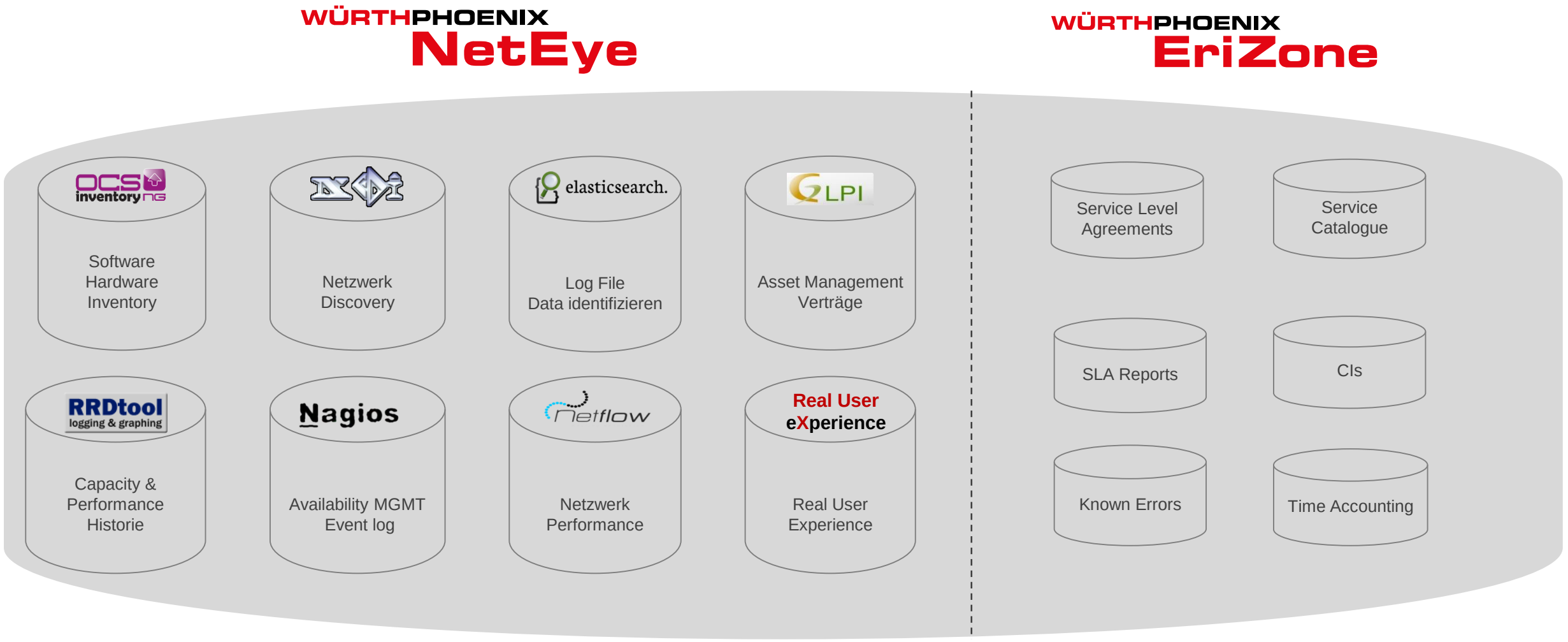
Service Operation

- Event Management
- Request Fulfillment
- Access Management
- Incident Management
- Problem Management

WÜRTHPHOENIX NetEye

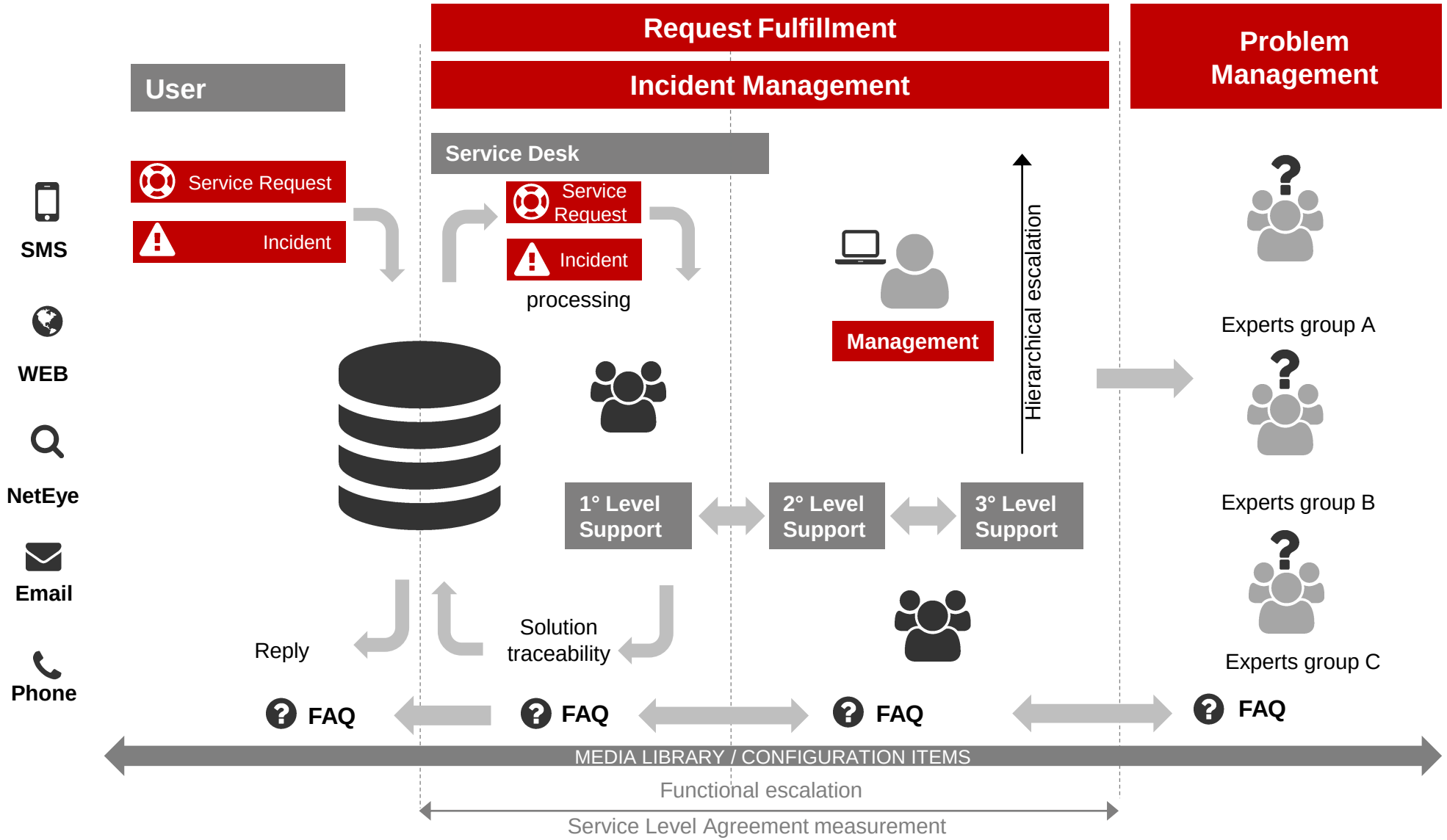
WÜRTHPHOENIX EriZone

Datenbanken

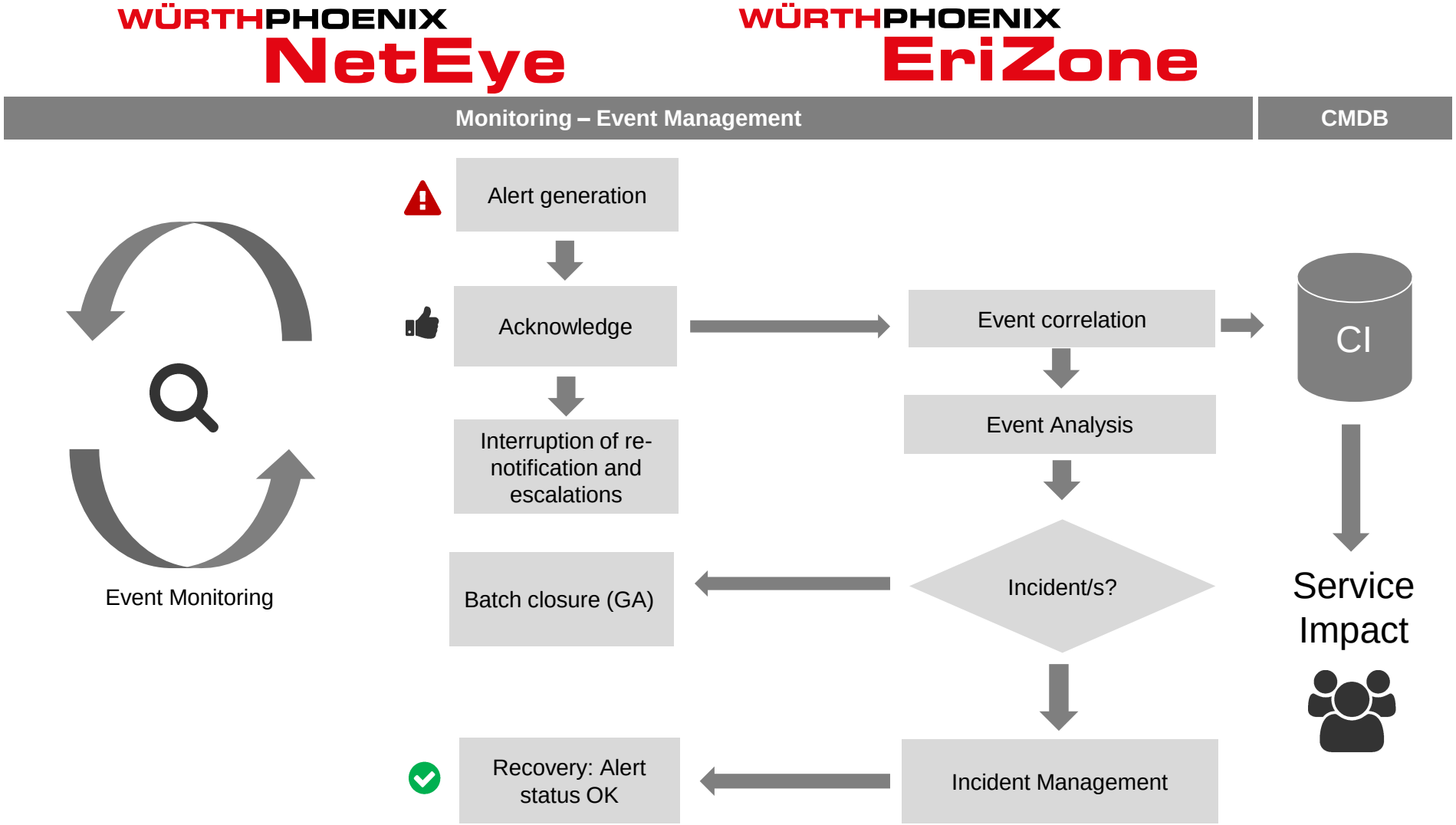


ZUVERLÄSSIGKEIT TROUBLESHOOTING PERFORMANCE SERVICE MANAGEMENT

Zentralisierte Verwaltung aller Anfragen mit EriZone



Integration NetEye-EriZone



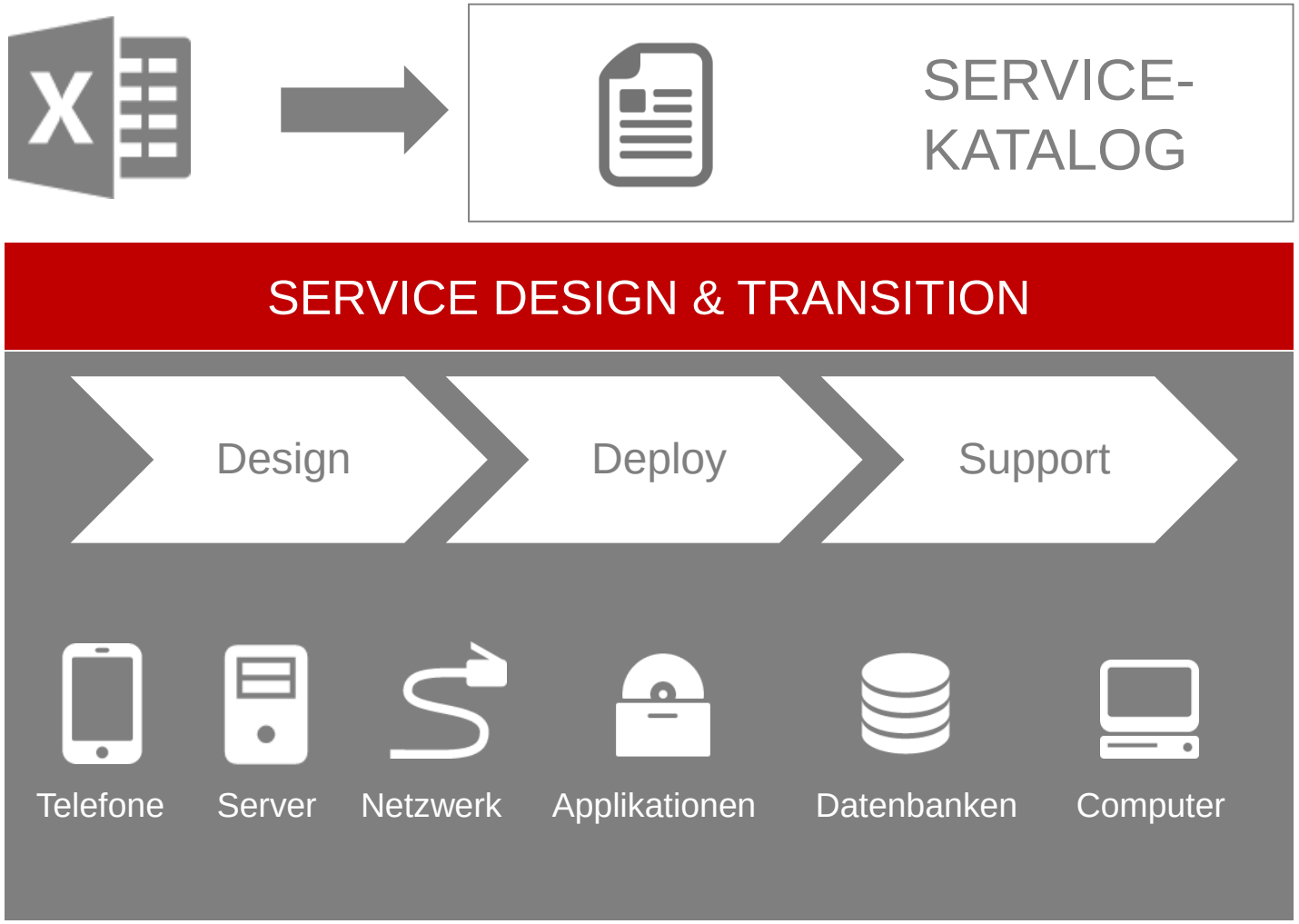
Unser Vorgehensmodell

1. **SERVICE STRATEGY**
   Identifizierung der Dienste
2. **SERVICE DESIGN & TRANSITION**
   Projektierung und Implementierung der Dienste
3. **SERVICE TRANSITION & OPERATION**
   Verwaltung und Instandhaltung der Dienste
4. **CONTINUAL SERVICE IMPROVEMENT**
   Kontinuierliche Verbesserung der Dienste

Phase 1: Identifizierung der Dienste

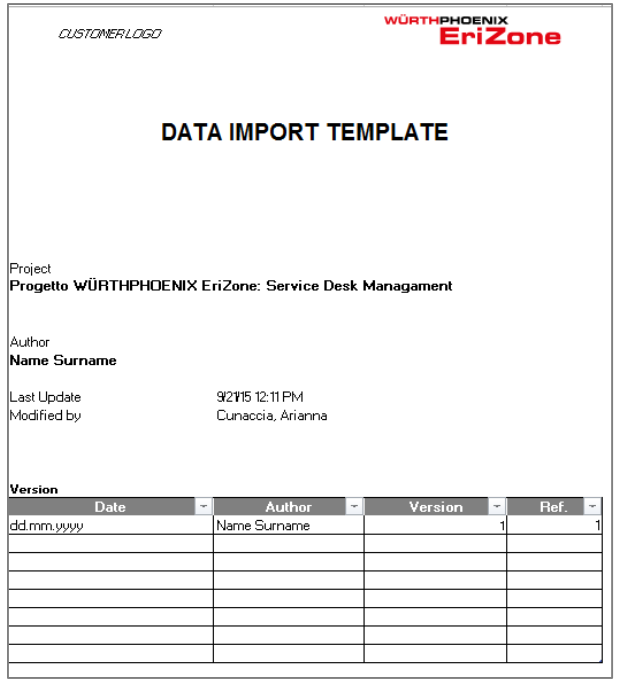
Festlegung der Strategie zur erfolgreichen Betreuung des Kunden, angepasst an die Unternehmensbedürfnisse

Phase 2: Projektierung und Implementierung der Dienste



Definition automatisierter und wiederholbarer Prozesse

Service-Katalog



CUSTOMER LOGO

WÜRTHPHOENIX EriZone

DATA IMPORT TEMPLATE

Project
Progetto WÜRTHPHOENIX EriZone: Service Desk Managament

Author
Name Surname

Last Update 9/2/15 12:11 PM
Modified by Cunaccia, Arianna

Version

Date	Author	Version	Ref.
dd.mm.yyyy	Name Surname	1	1

- Categories
- Services
- Queue – role – groups
- Closure typology
- Service Dispatcher
- Access Management
- CMDB class definition

Service Name Level 3	Final Service Name (Calculated)	Comment	Service Type	Service Criticality	Destination Queue	Default SLA
	[S-001] Sample Service::		Front End	2 low		
	[S-001] Sample Service::Sub Service 2		IT Management	3 normal		
Sub Service 3	[S-001] Sample Service::Sub Service 2::Sub Service 3		IT Operational	4 high		
Sub Service 4	[S-001] Sample Service::Sub Service 2::Sub Service 4		End User Service	2 low		

Phase 3: Verwaltung und Instandhaltung der Dienste

WÜRTHPHOENIX

WÜRTHPHOENIX
EriZone

SERVICE TRANSITION - OPERATION

SERVICE CATALOGUE

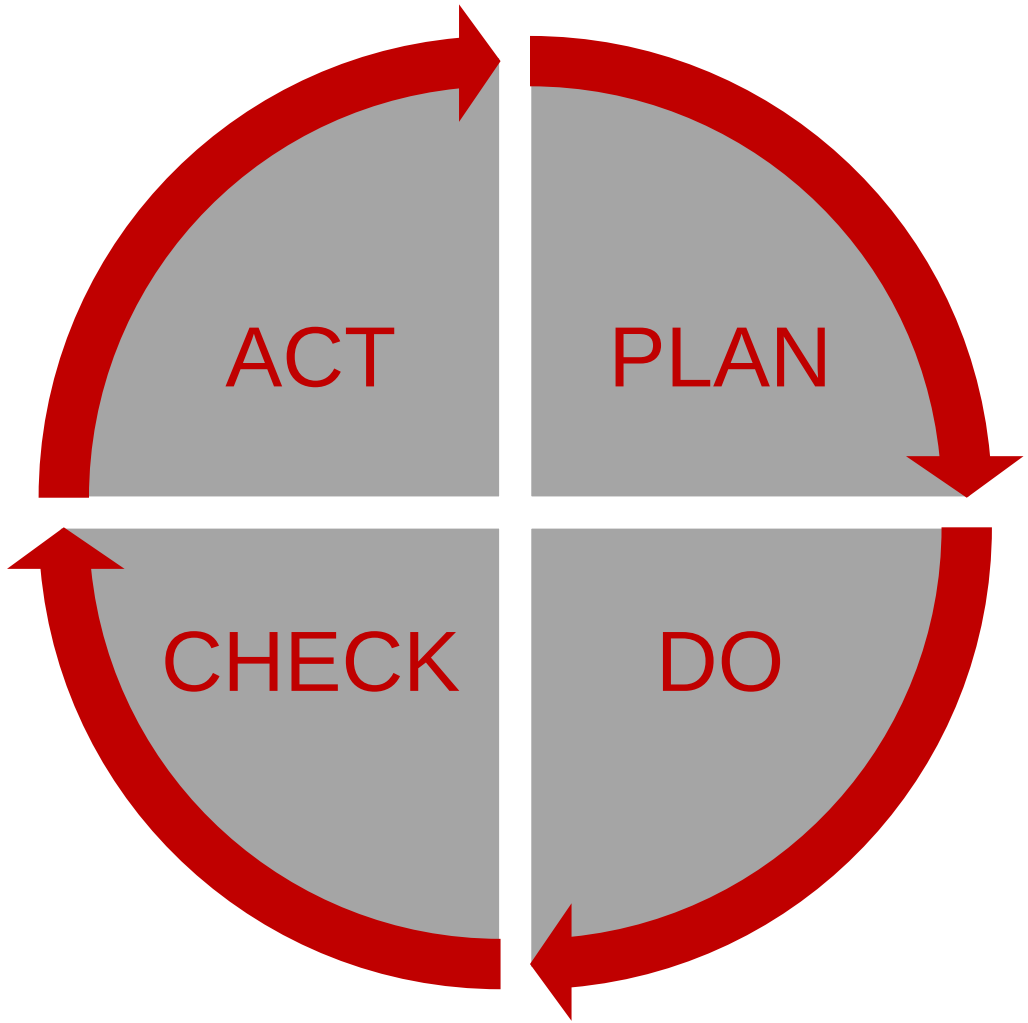
SLA

OLA

Signalisierung Fehler	Incident
Anfrage Assistenz	Service Request
Diagnose Incident	Problem
Anfrage Änderung	Request for Change
Anfrage Zugang	Access
Registrierung Event	Event

Phase 4: Kontinuierliche Verbesserung der Dienste

Aktivitäten zur kontinuierlichen Verbesserung der Prozess-Leistung

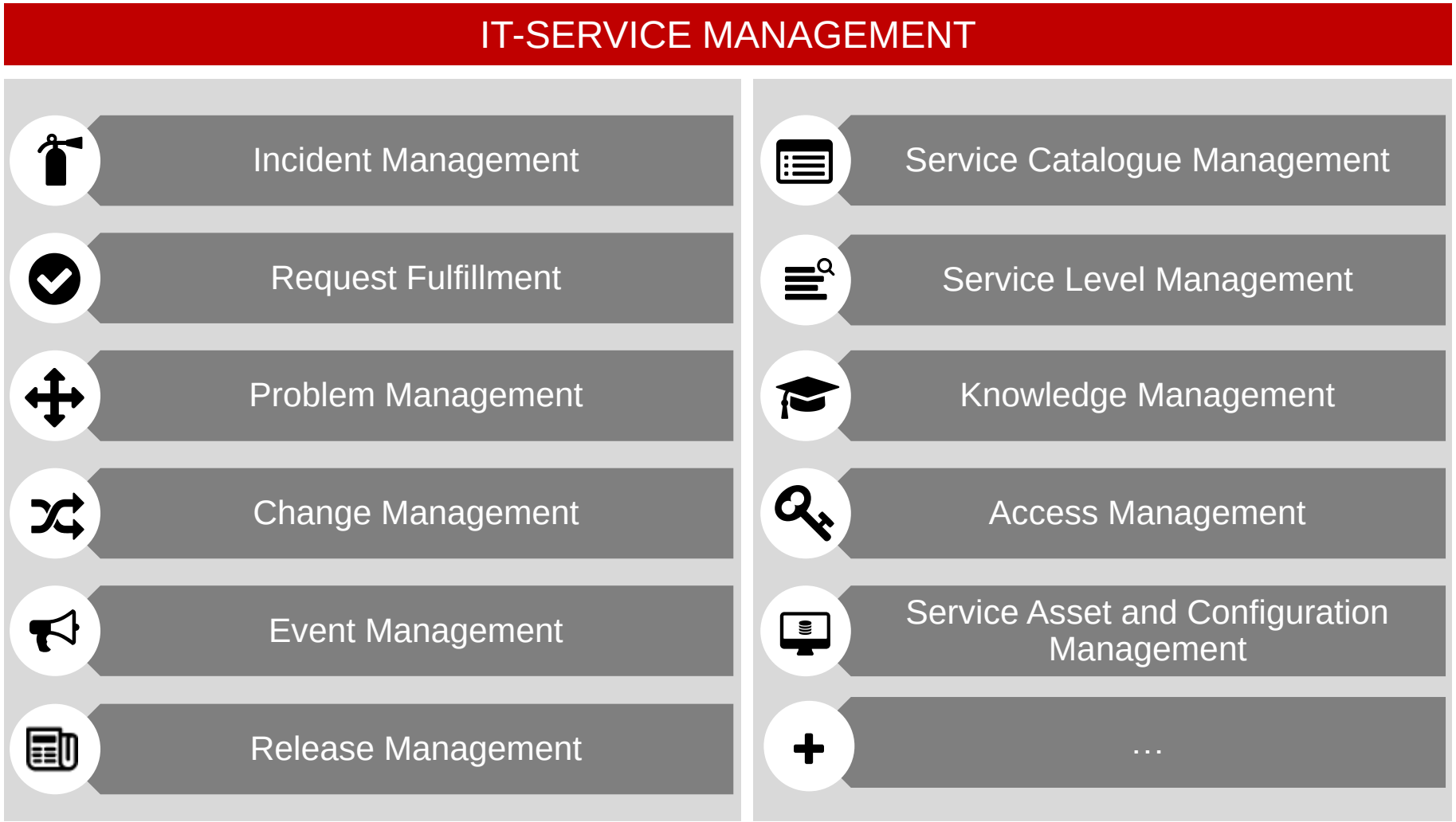


Festlegung der Ziele und Prozesse

Überwachung und Messung der Prozesse und Dienste und entsprechendes Reporting

Implementierung des Prozesses

IT-Service Management mit EriZone



Service Management in unterschiedlichen Unternehmensbereichen

IT

HR

Finanzwesen

Operation

Einkauf

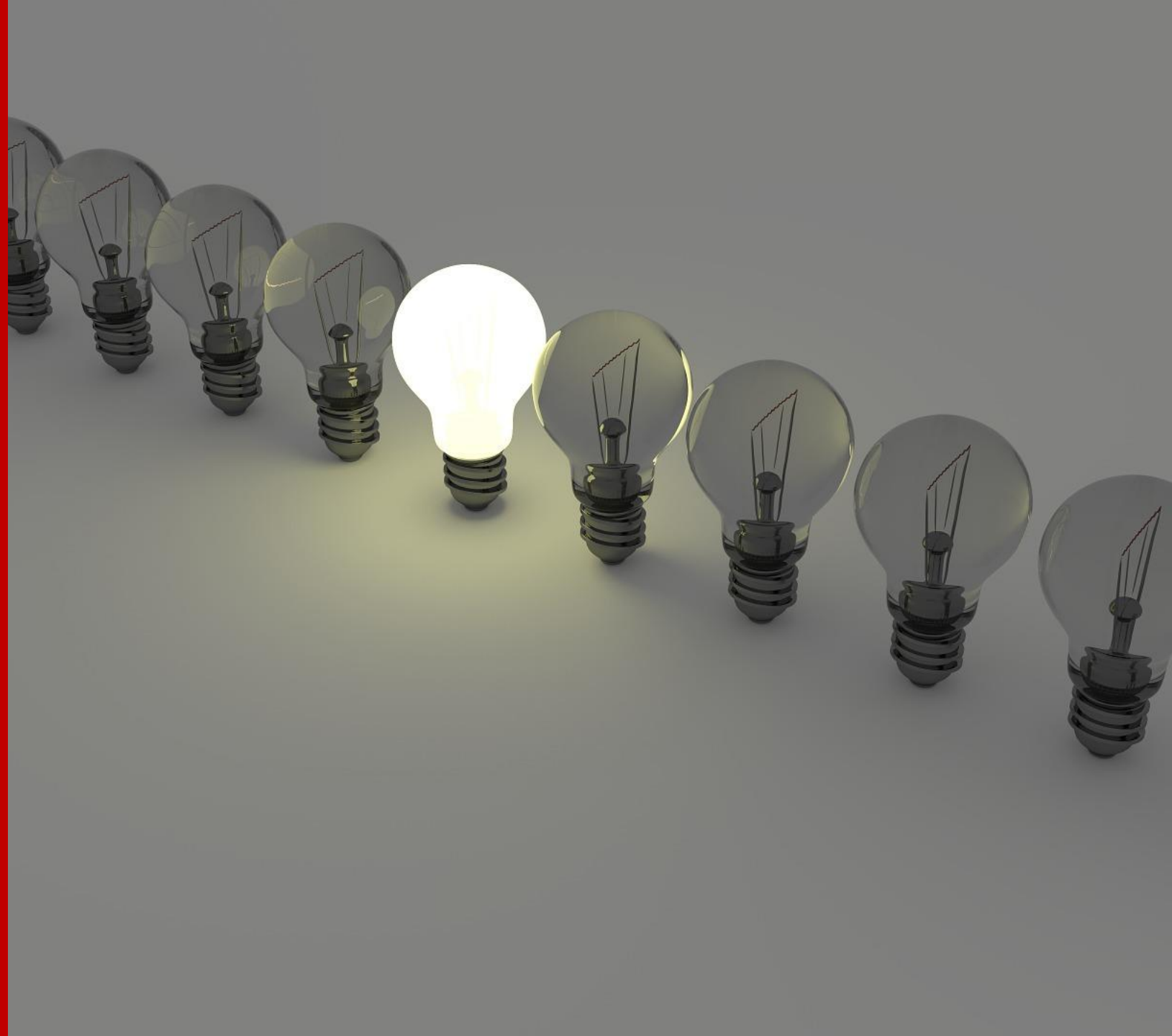
Marketing

Verwaltung

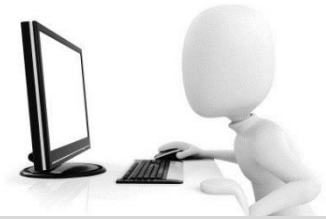
Und weitere…

WÜRTHPHOENIX
EriZone

News rund um EriZone



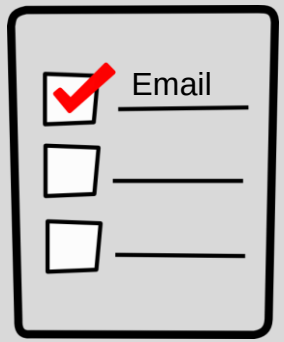
Auslösung der Prozesse basierend auf dem Sprach-Code des Kunden



Sprachcode des Kunden

Dienste nach Kunde filtern

Auswahl des Dienstes



Auswahl Kategorie:
Der Schlüssel ist es den Sprachcode des Kunden zu verwenden

Default Wert

SLA Auswahl

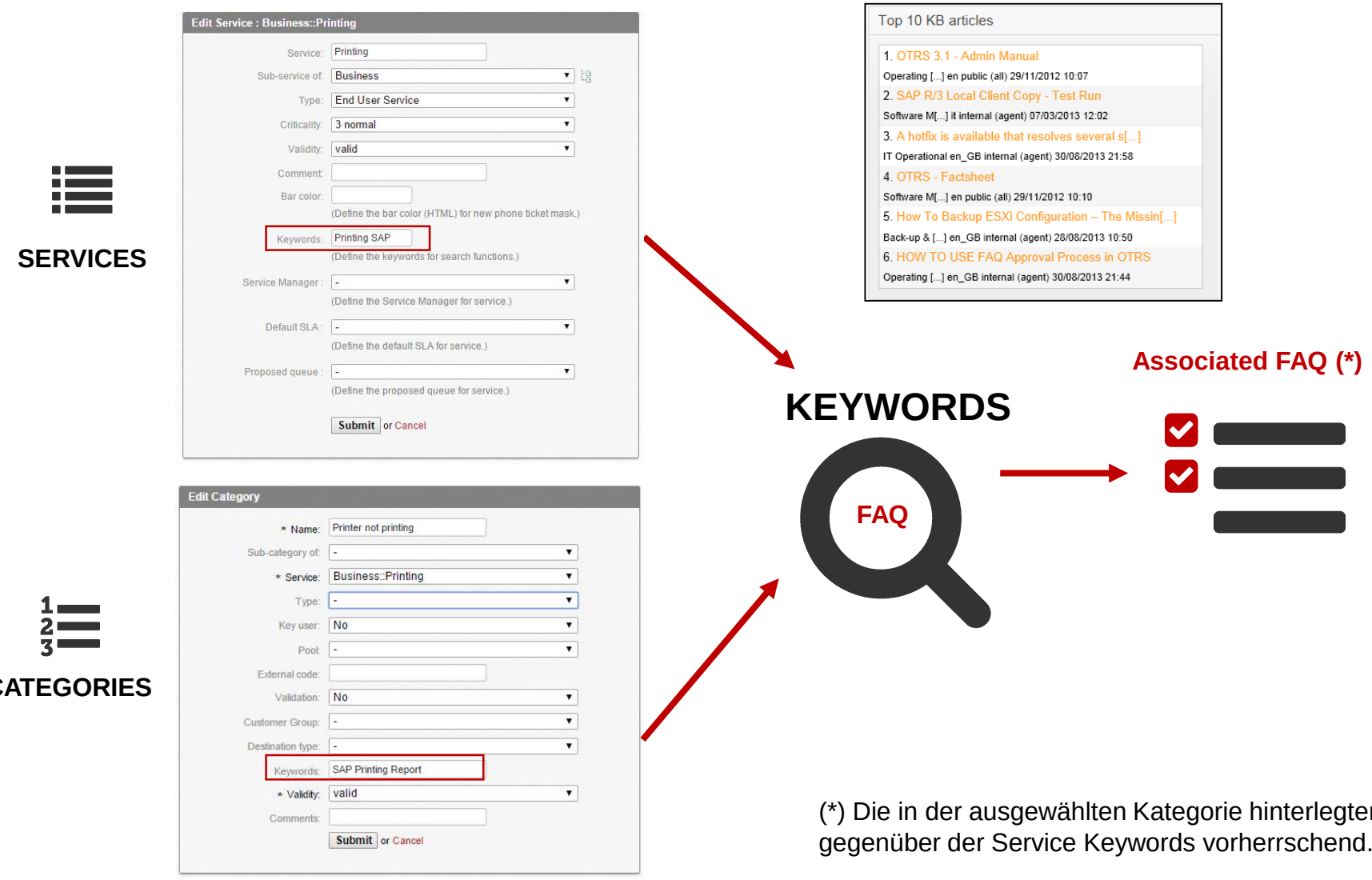
Zuweisung Gruppe

Bestimmungsort

Auswirkung -> Priorität (*)

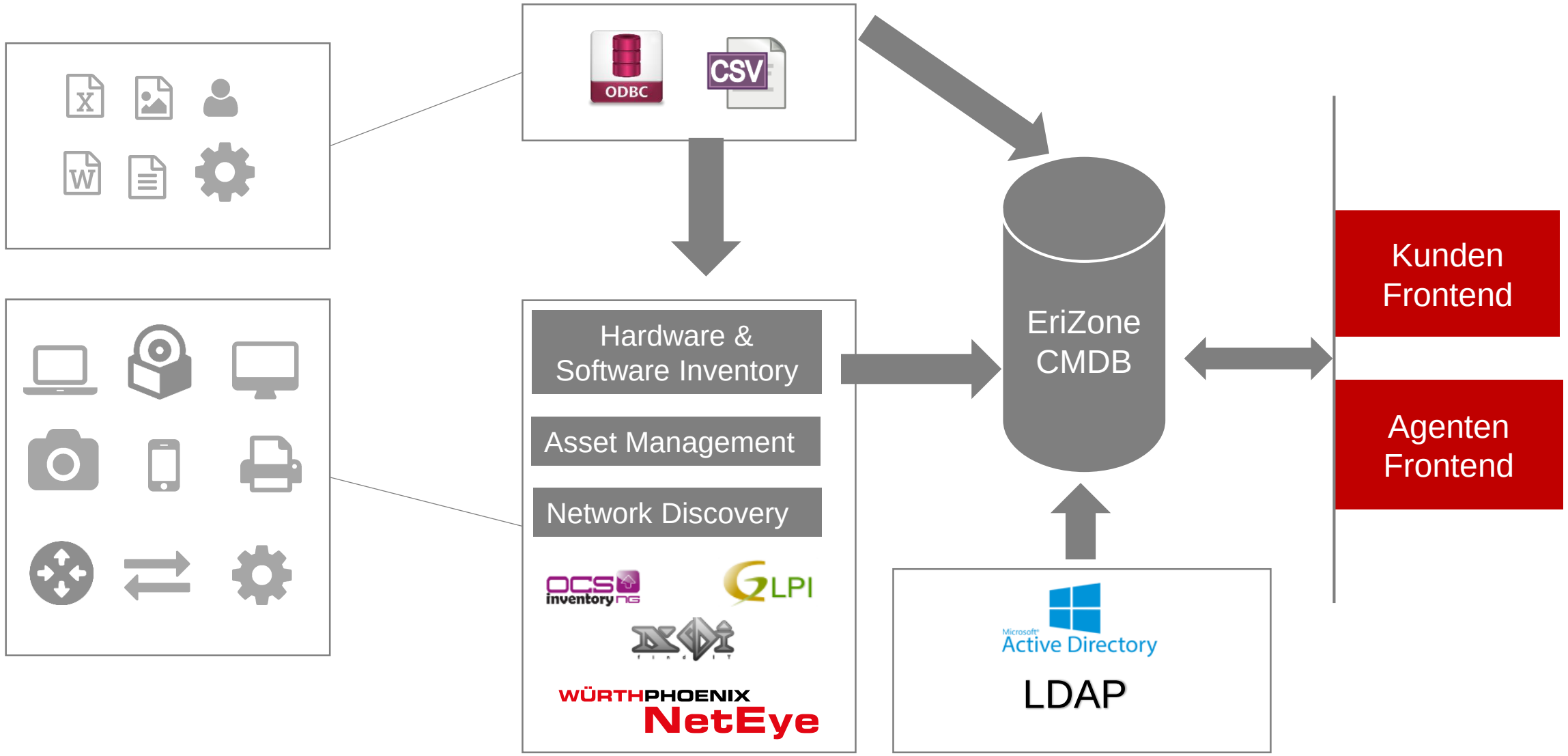
Automatische Auslösung Prozess

Integration von Service-Katalog und Knowledge Management

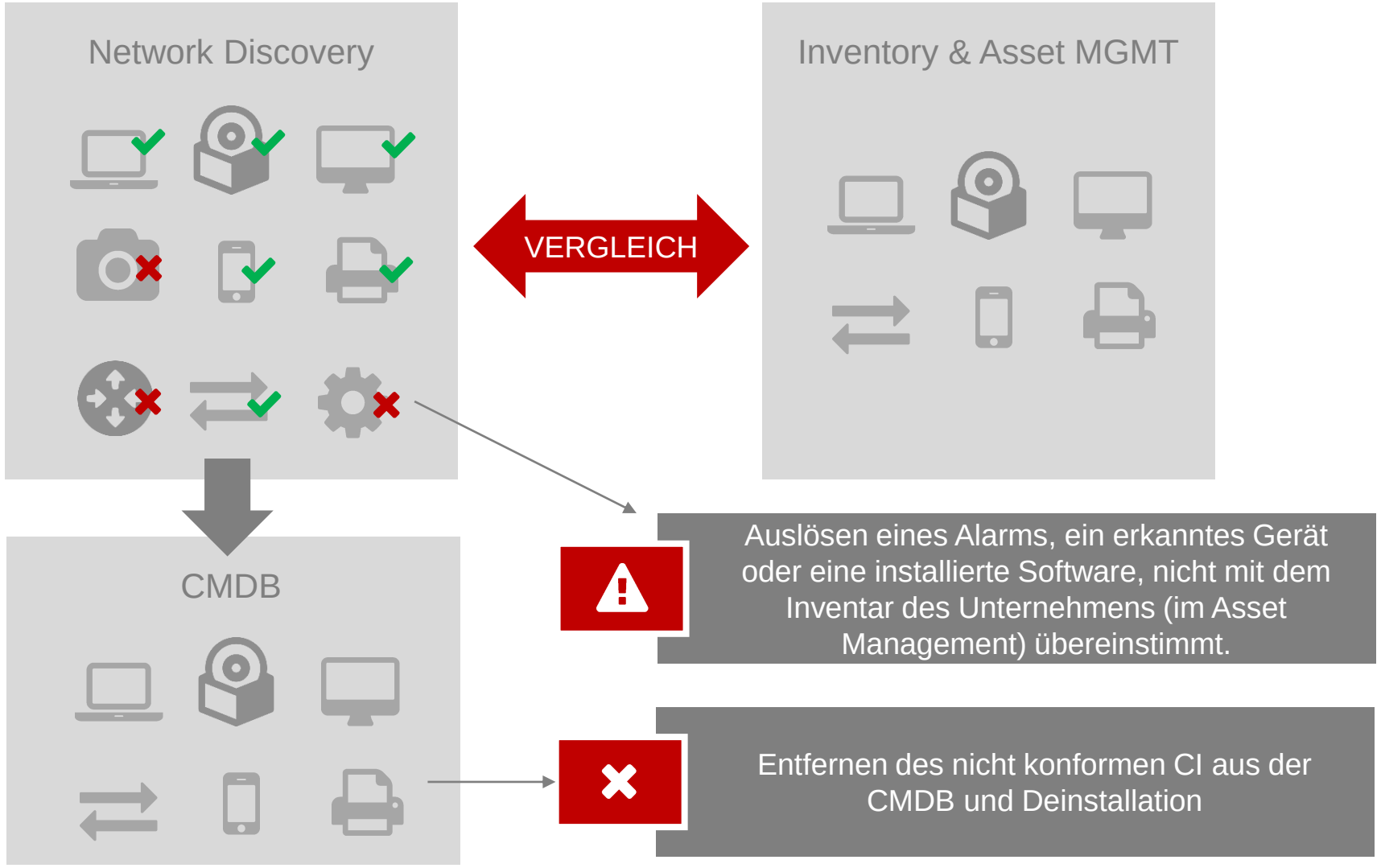


(*) Die in der ausgewählten Kategorie hinterlegten Keywords sind gegenüber der Service Keywords vorherrschend.

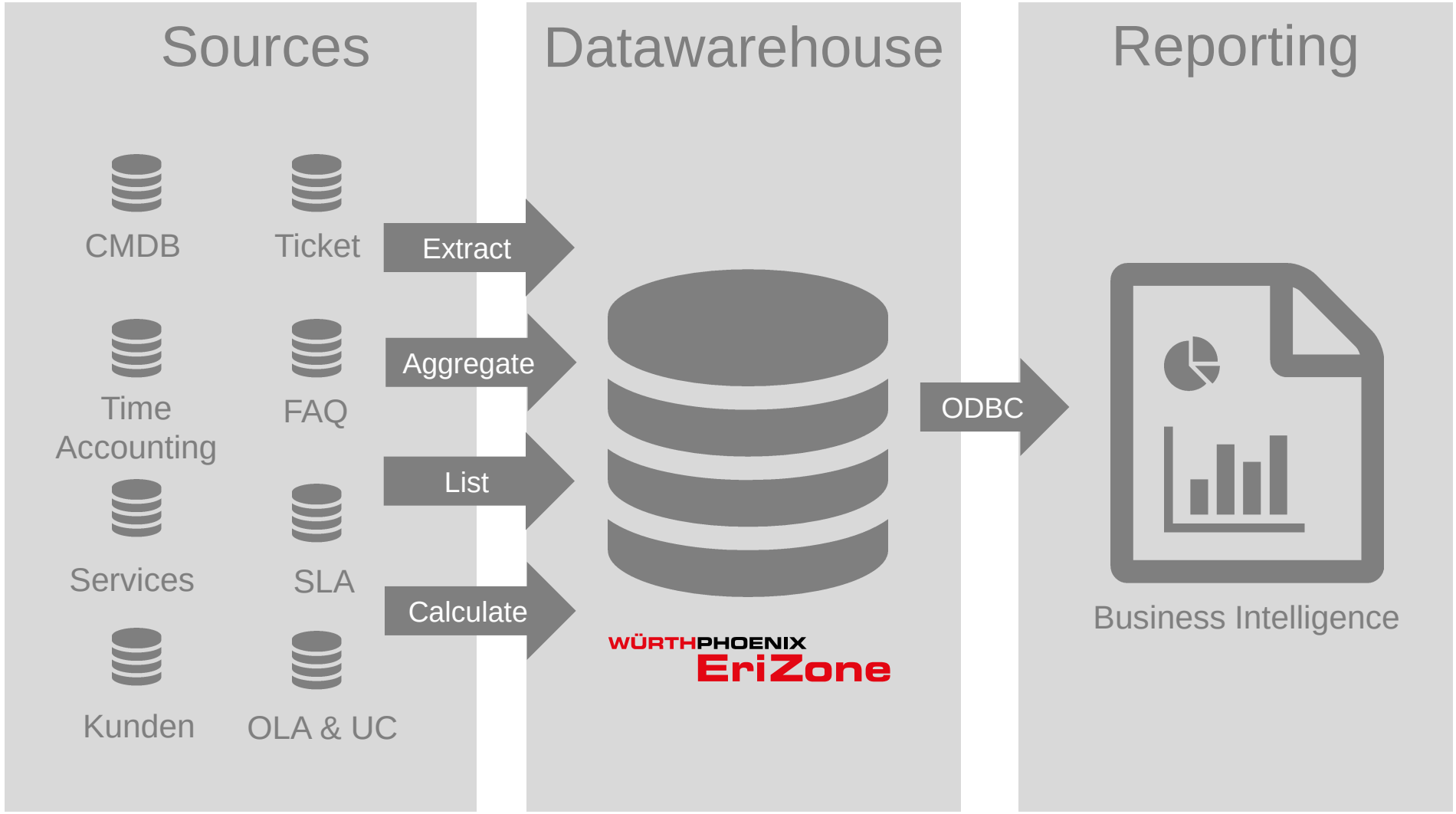
EriZone CMDB



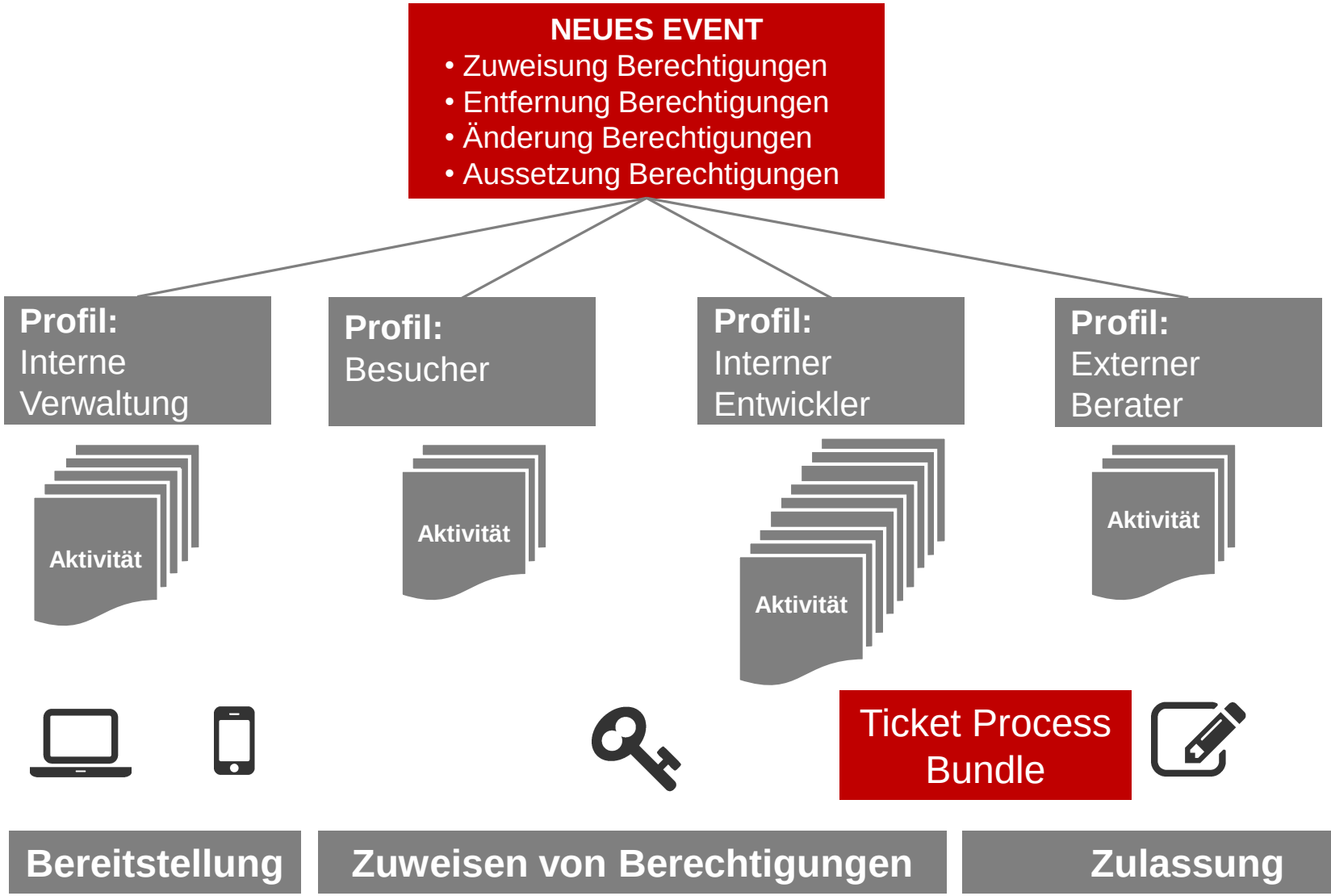
Auditing der Configuration Items



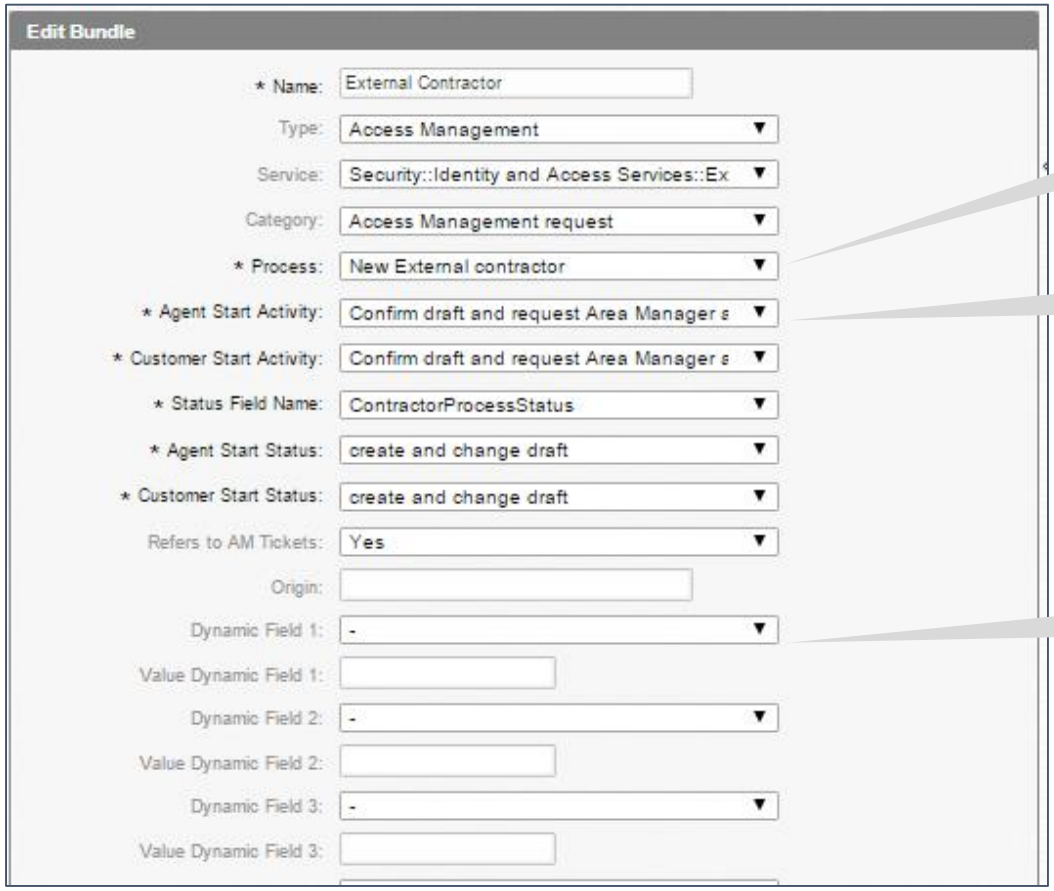
EriZone Datawarehouse



Access Management in EriZone



Konfiguration des Prozess Bundle

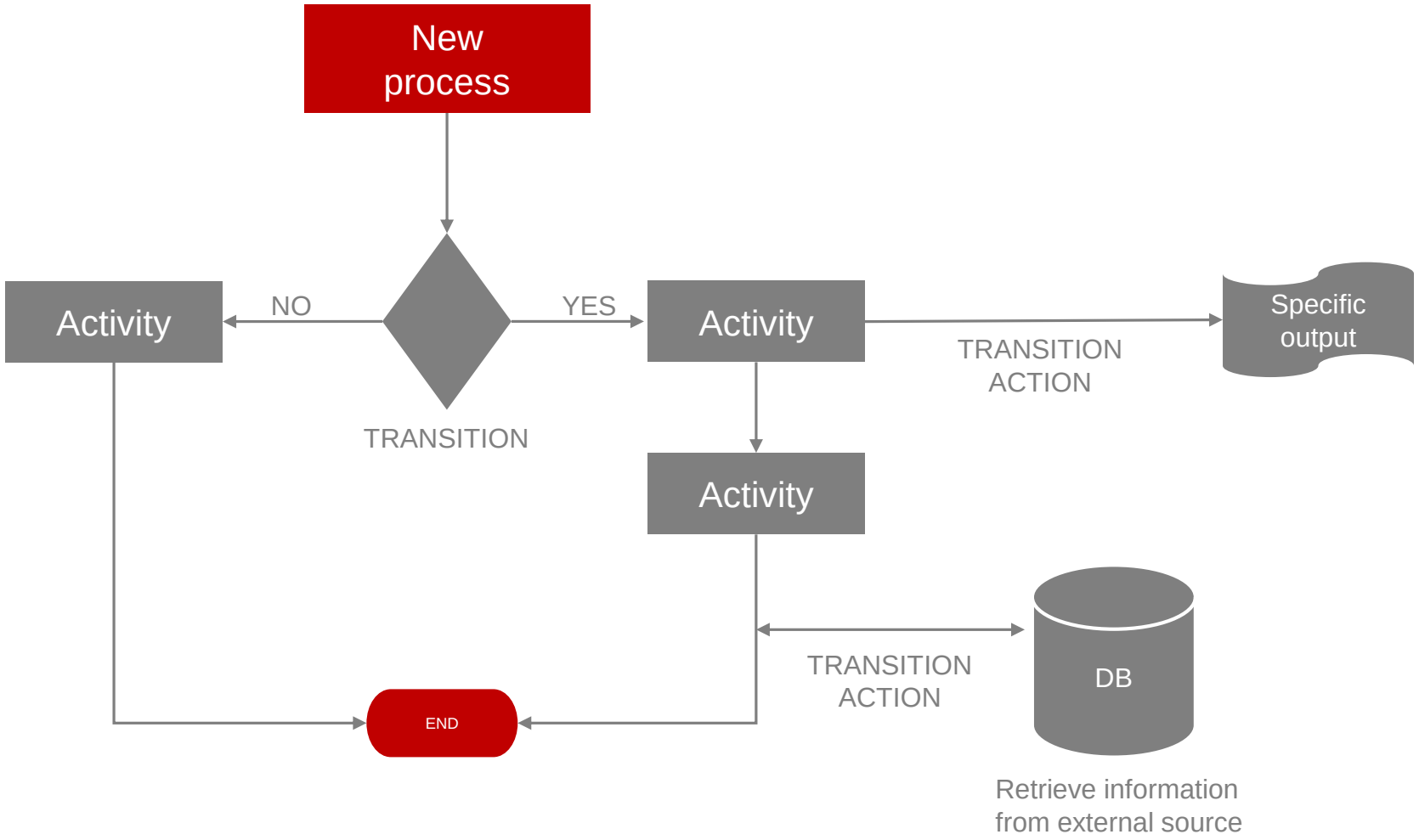


Prozessdefinition

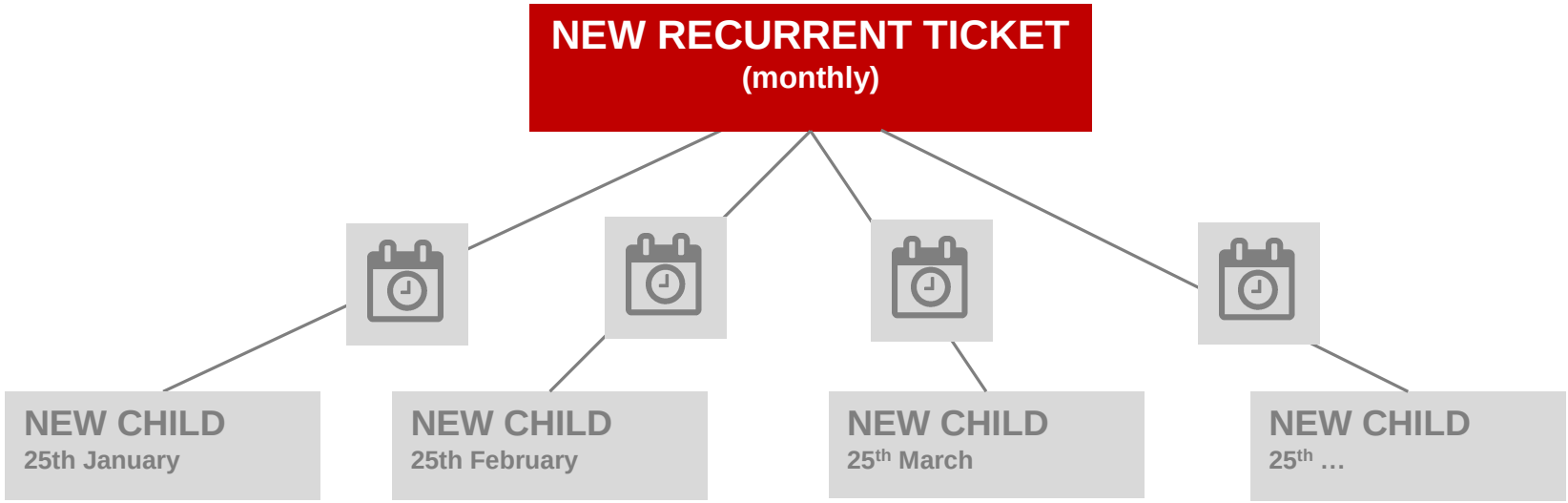
Flow Definition

Dynamic fields Initialisierung

Prozess Management

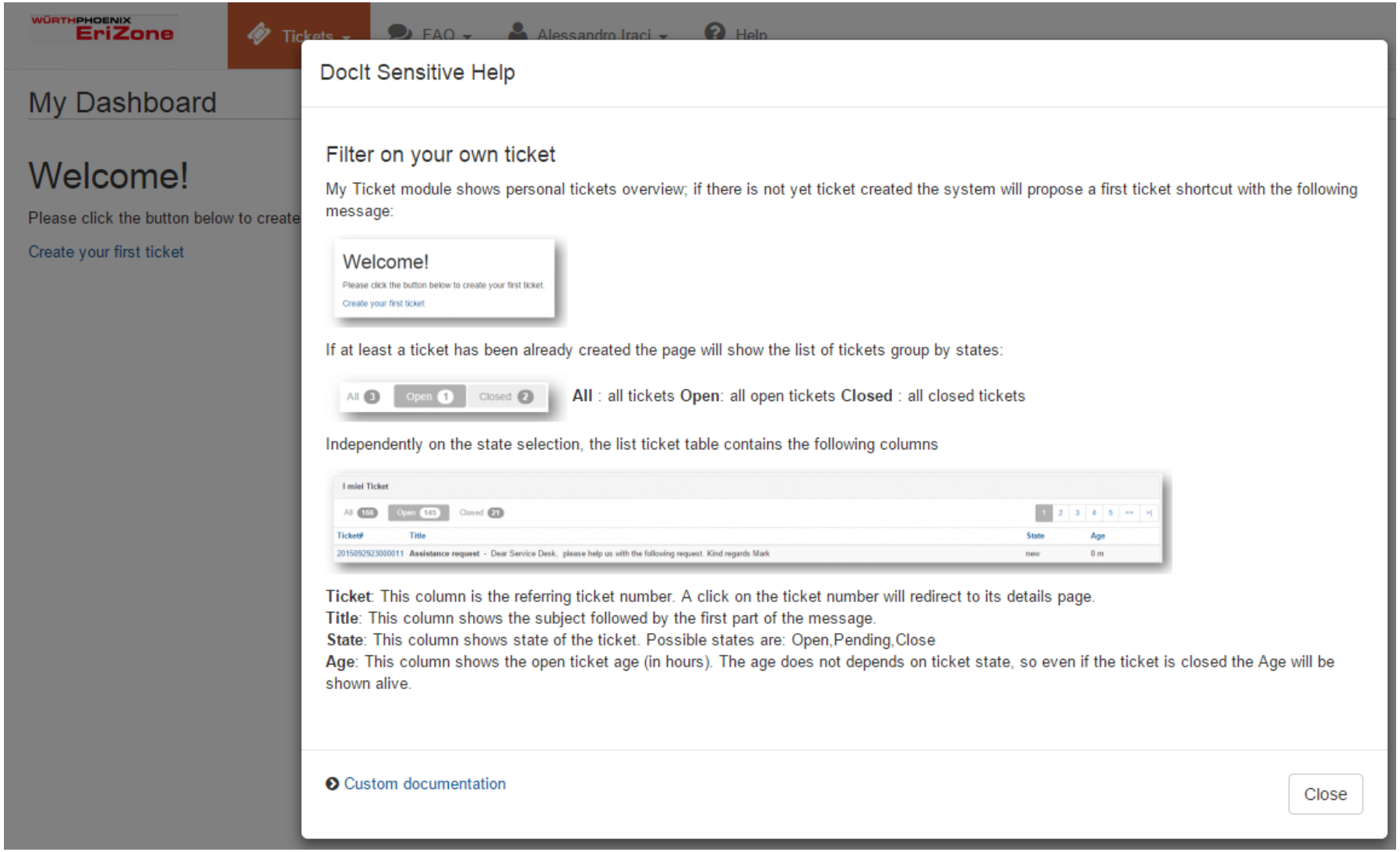


Wiederkehrende Tickets



Wiederkehrende Tickets: täglich, wöchentlich, monatlich, jährlich und einmalig

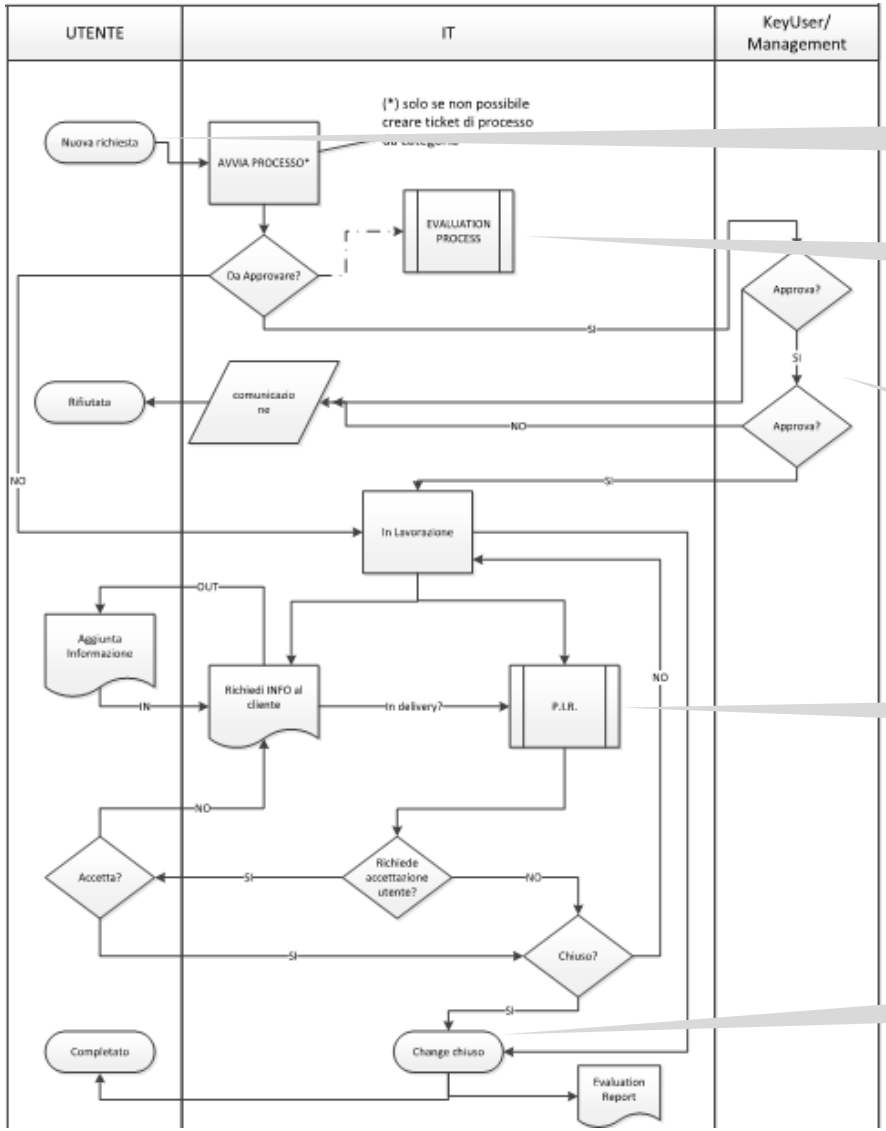
Für iedes Ereignis wird ein Child Ticket zur Nachvollziebarkeit und Historie erzeugt


WÜRTHPHOENIX EriZone
Tickets
FAQ
Alessandro Iraci
Help
My Dashboard
Welcome!
Please click the button below to create
Create your first ticket
DocIt Sensitive Help
Filter on your own ticket
My Ticket module shows personal tickets overview; if there is not yet ticket created the system will propose a first ticket shortcut with the following message:
Welcome!
Please click the button below to create your first ticket.
Create your first ticket
If at least a ticket has been already created the page will show the list of tickets group by states:
All 3
Open 1
Closed 2
All : all tickets Open: all open tickets Closed : all closed tickets
Independently on the state selection, the list ticket table contains the following columns
I miei Ticket
All 166
Open 145
Closed 21
Ticket#
Title
State
Age
2015092923000011 Assistance request - Dear Service Desk, please help us with the following request. Kind regards Mark
new
0 m
Ticket: This column is the referring ticket number. A click on the ticket number will redirect to its details page.
Title: This column shows the subject followed by the first part of the message.
State: This column shows state of the ticket. Possible states are: Open,Pending,Close
Age: This column shows the open ticket age (in hours). The age does not depends on ticket state, so even if the ticket is closed the Age will be shown alive.
Custom documentation
Close

EriZone 3.6 mit dem Change - Evaluierungsprozess

- Planung und Kontrolle der Changes
- Change und Release Planung
- Kommunikationen
- Entscheidung und Autorisierung eines Changes
- Sicherstellung eines Korrektur-Plans
- Messung und Kontrolle
- Management Reporting
- Verstehend der Auswirkungen eines Changes
- Kontinuierliche Verbesserung

Beispiel eines Change Prozesses



REQUEST FOR CHANGE

EVALUATION PROCESS

APPROVAL

POST IMPLEMENTATION REVIEW

CLOSED CHANGE

Neue Module in EriZone 3.6

Budgeting

Budget information in terms of operating and capital expenses

Evaluation

- Evaluation Performance
- Evaluation Risk management
- Evaluation Test
- Evaluation Recommendation
- Evaluation Report

Major Features

Wiederkehrende Tickets (täglich, wöchentlich, monatlich, jährlich)	Tägliche Zeiterfassung Agenten-Journal	Neue Transaktions – Aktionen für das Prozess Management	SLA Auswahl basierend auf den zu erwartenden Auswirkungen
Weitergabe interner und externer Notizen von Child- zu Parent-Ticket	Neue Spalten im Datawarehouse	Unmanaged ticket report auf Basis des Unternehmenskalender und Berechtigungen	Script Load für das Access Management
Übersicht zu den Access Management Aktivitäten im Kunden-Frontend	**VERSION 3.6**	Vereinfachte Deployment scripts → test (sync for productive systems)	Screenshot Copy & Paste Unterstützung IE – Edge – Firefox - Chrome
Online Hilfe	Änderung interner Artikel	«My service» Modul-Integration	**NEW**

Nächste Schritte

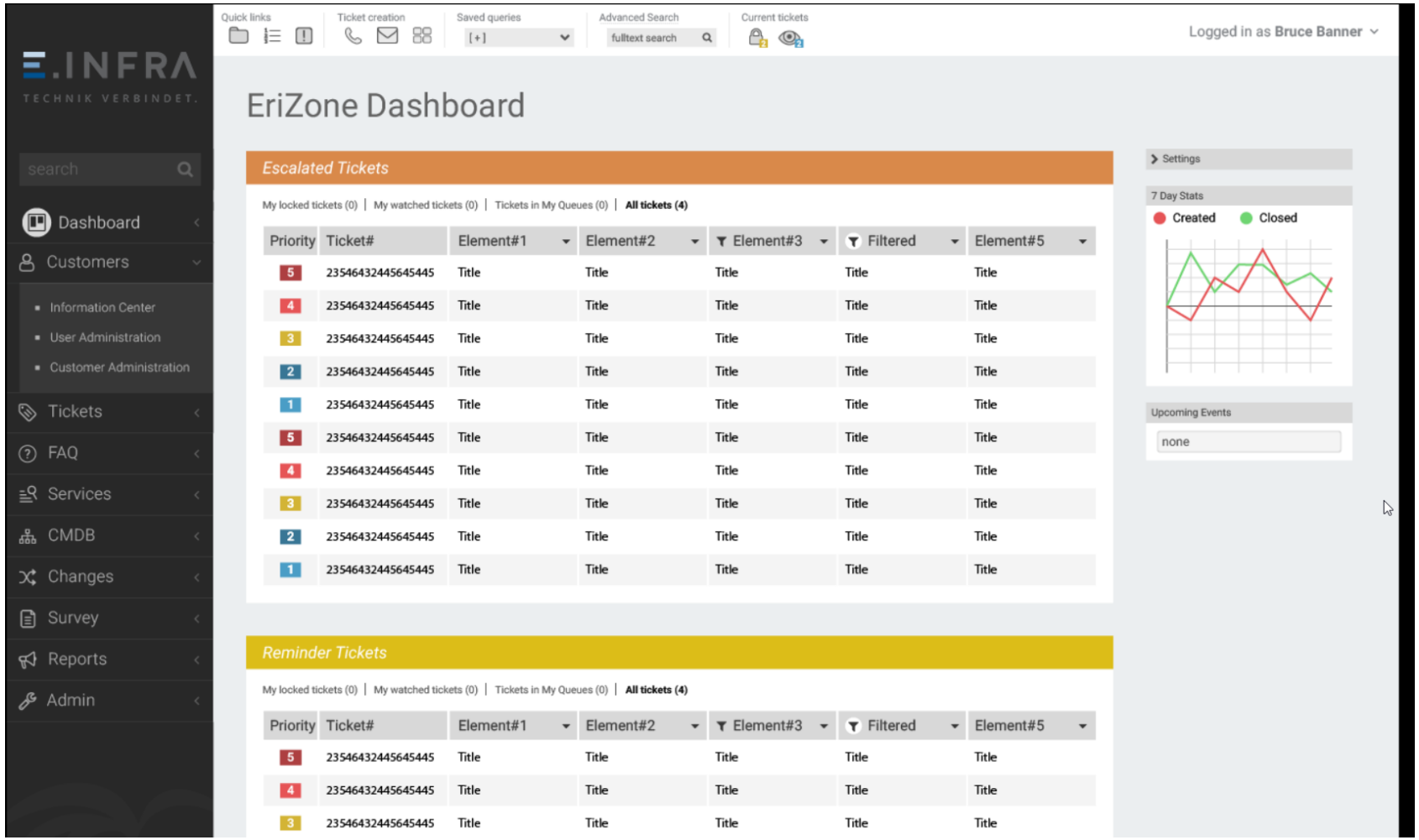
2017

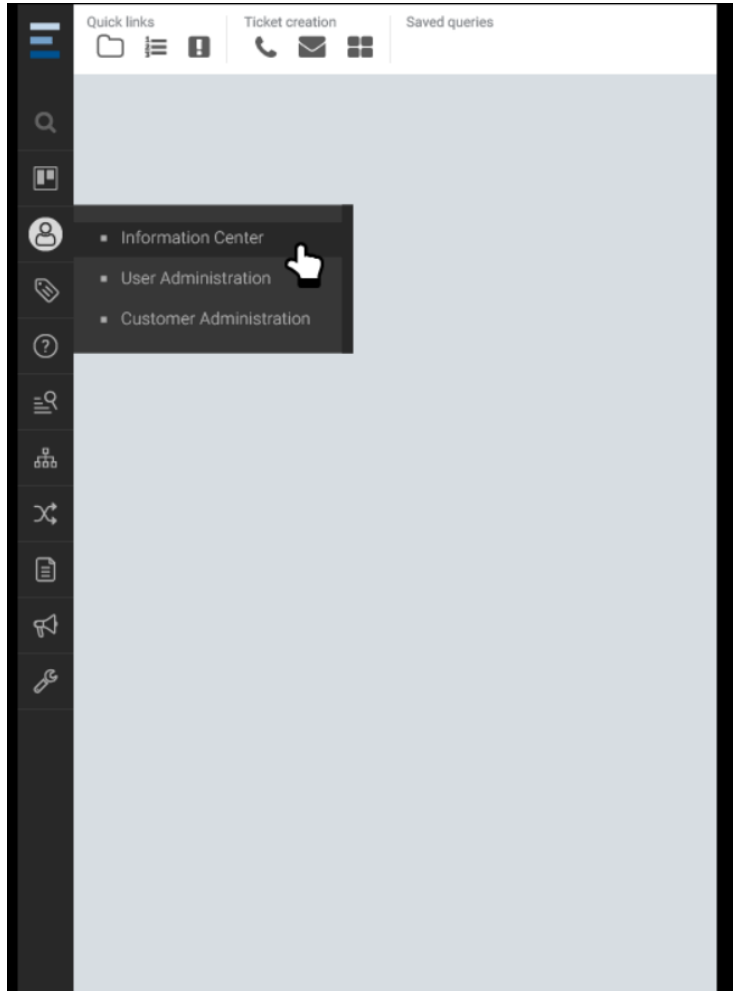
ISO 27001

Produkt Zertifizierung ITIL v3 2011 - Axelos

EriZone v. 5
(OTRS 5)

EriZone 5: Erste Eindrücke





Q&A

Danke!

Georg.Kostner@wuerth-phoenix.com