infra:signal
GRÜNBERLIN

Splunk im operativen Alltag

Mehr als SIEM – serviceorientiertes Monitoring aus Betriebssicht

Jens Mahnke /16.17.03.2026

Wer sind wir und in welchem Umfeld sind wir tätig?

Berliner Landesunternehmen

- 100%ige Tochter der Grün Berlin GmbH
- seit 2023 rekommunalisiert

Kooperationspartner

- Planung, Bau, Modernisierung, Betrieb und Wartung fast 2.200 Lichtsignalanlagen

Verkehrswende-Fokus

- Priorisierung gemäß Mobilitätsgesetz sowie LED-Modernisierung

Wichtige Einrichtung gemäße NIS-2

- Betrieb der kritischen Lichtsignalanlageninfrastruktur
- Digitalisierung mit KI(ML) und V2X

Die Herausforderung sind die Dienstleister-Silos.

- Für die Anbindung einer einzelnen Lichtsignalanlage sind mehrere unabhängige Dienstleister im Einsatz, von denen jeder nur für sein eigenes Segment verantwortlich ist.

Dienstleister 1

- Modem A
- Hersteller A

Dienstleister 2

- Kupferleitung mit ganz vielen Muffen

Dienstleister 3

- Modem B
- Hersteller B

- Das Problem dabei ist, dass jeder nur seinen eigenen Teil sieht, aber niemand die Auswirkungen auf das Gesamtsystem. Die Fehlersuche wird so zu einem Ping-Pong zwischen den Zuständigkeiten.

Ist Splunk wirklich immer gleich SIEM/SOC?

Die meisten kennen Splunk als Security-Plattform. Diese Sichtweise ist zwar richtig, aber unvollständig.

Threat Detection & Incident Response

Log-Aggregation & Security-Analysen

Compliance-Reporting

Ja, aber: Das volle Potenzial liegt im operativen Betrieb und geht weit über SIEM/SOC hinaus.

Unsere Lösung: End-to-End-Monitoring

- *Splunk dient als gemeinsame Datenbasis für die Bereiche Security und Operations. Anstatt Einzelsysteme für Monitoring, Protokollierung und Security zu implementieren und zu betreuen, nutzen wir eine umfassende Lösung.*

Service-Modelle

- ***LSA** = Steuergerät + Verkehrsrechner + Leitstelle*
- ***IaaS** = Hardware + Virtualisierung*
- *N**etz** = Firewall + Switch + Modem + Leased Line (Kupfer oder Glasfaser) + Mobilfunk*
- *Es gibt keine isolierten Metriken, sondern ganzheitliche Service-Objekte mit Abhängigkeiten.*

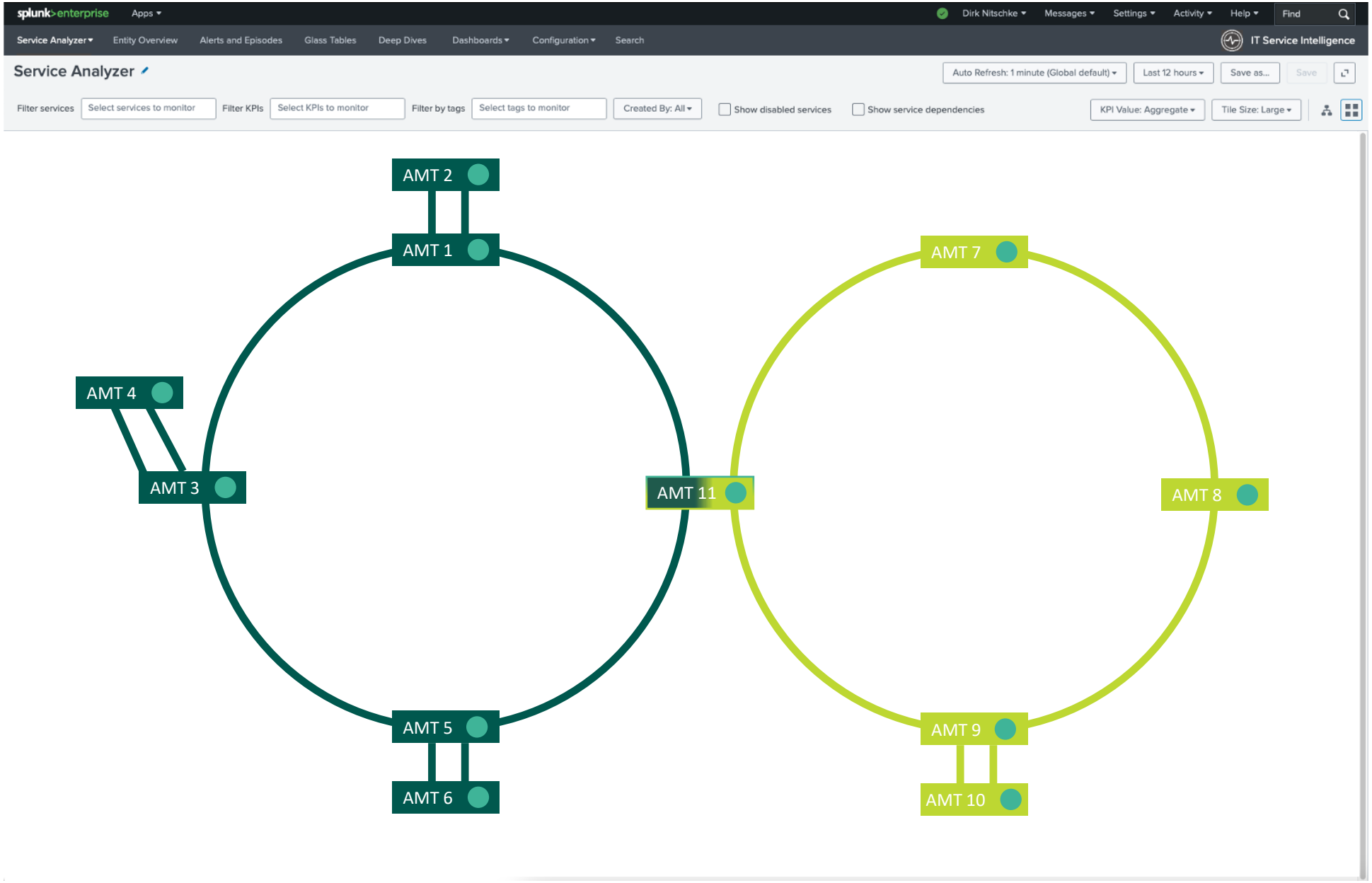
Zentrales Lagebild

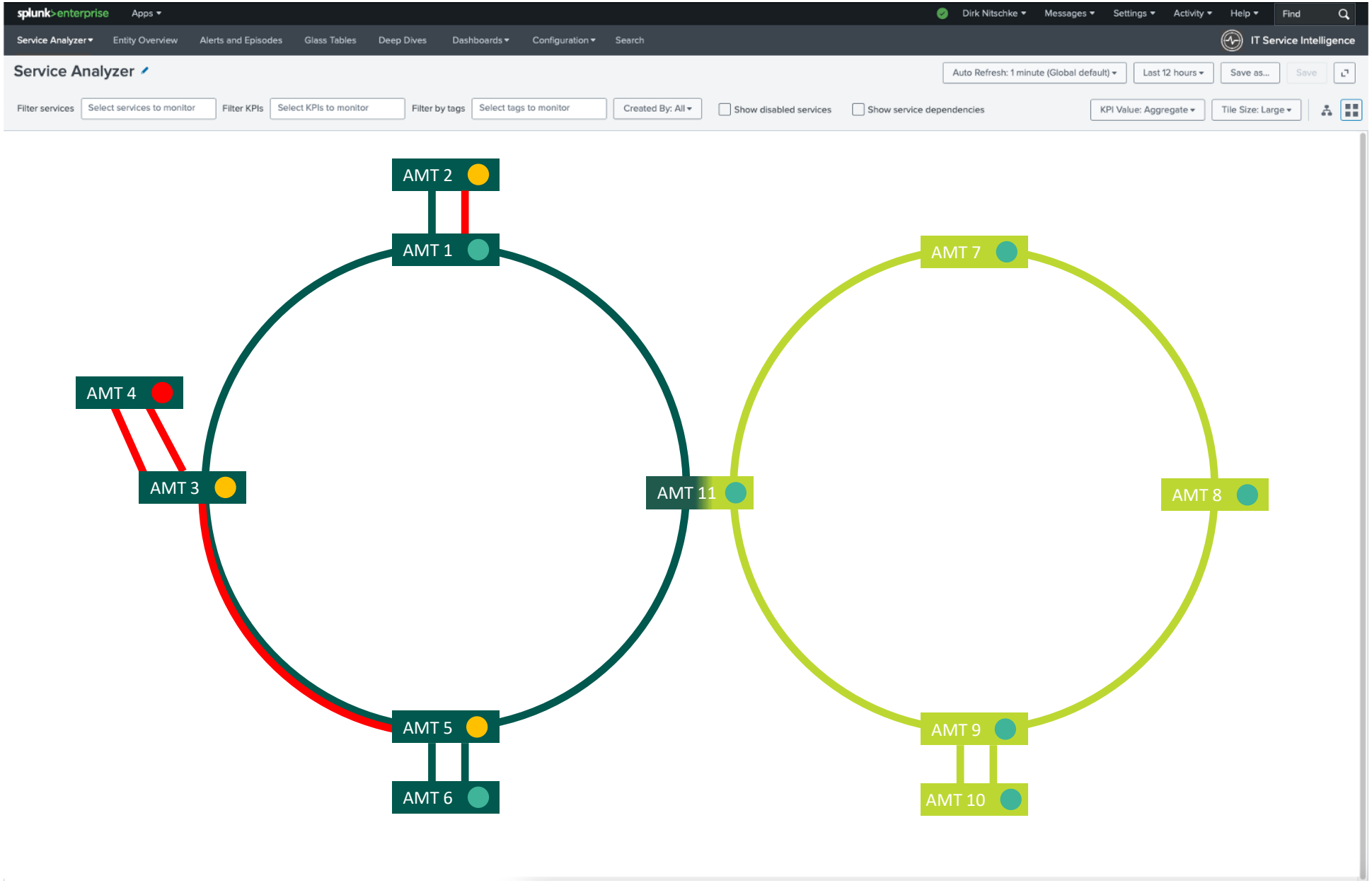
- *Es entsteht ein einheitliches Lagebild für uns intern mit gefilterten, rollengerechten Sichten für jeden Dienstleister.*

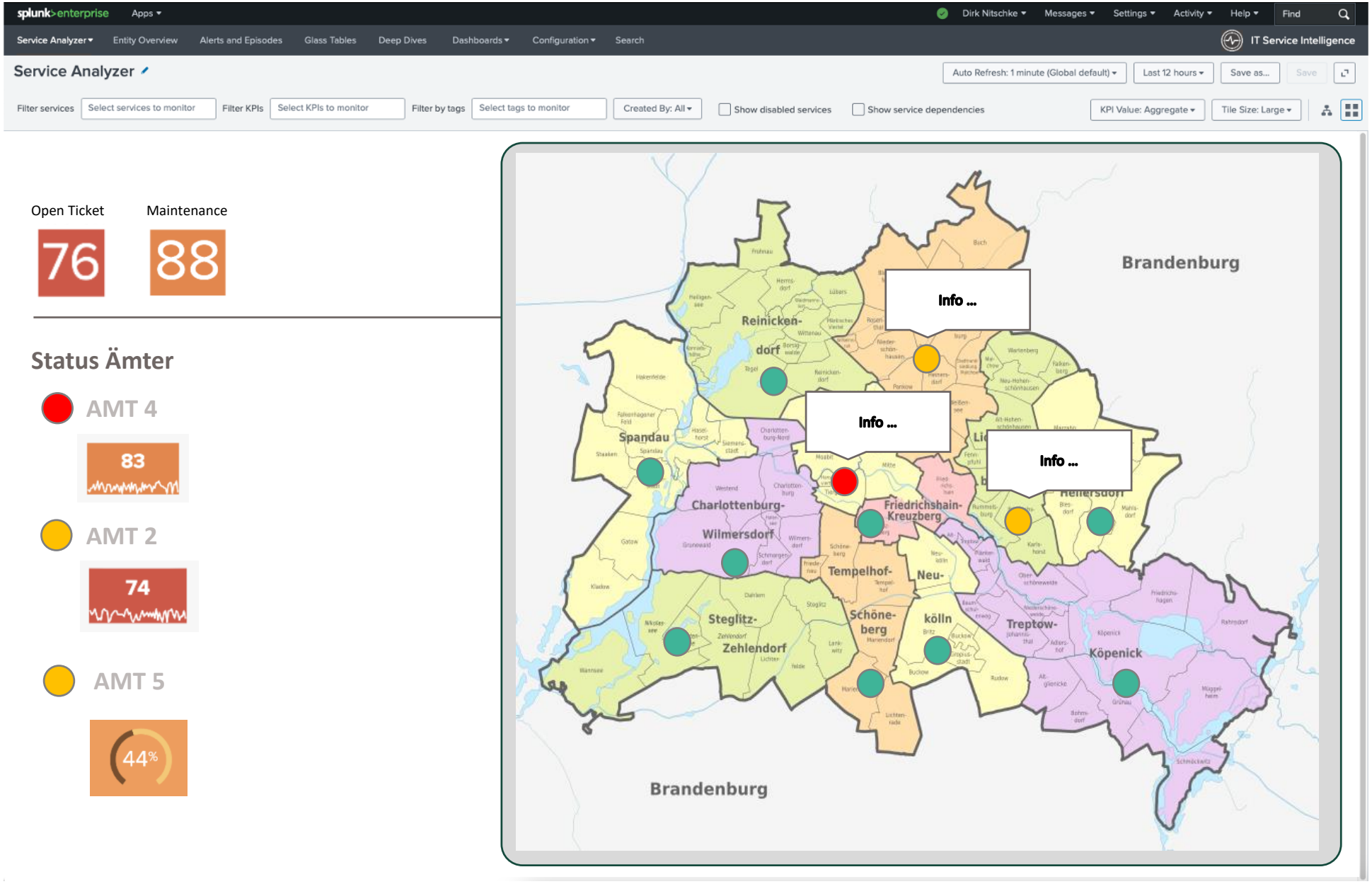
Abhängigkeiten werden sichtbar

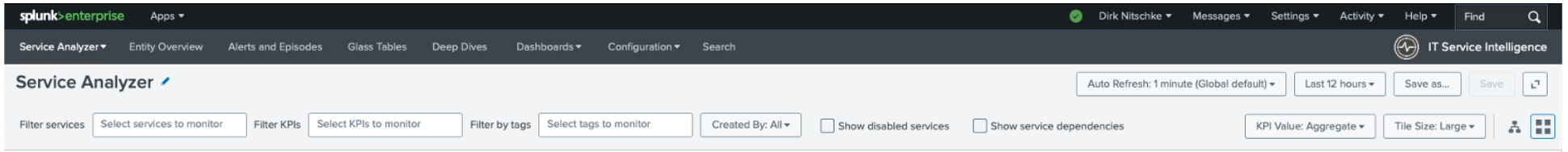
- *Kausalketten über alle Silos hinweg – vom Modem bis zur Leitstelle – in einem Dashboard dargestellt.*

Was sieht die Leitstelle der Verkehrssteuerung derzeit


splunk>enterprise
Apps
Dirk Nitschke
Messages
Settings
Activity
Help
Find
Service Analyzer
Entity Overview
Alerts and Episodes
Glass Tables
Deep Dives
Dashboards
Configuration
Search
IT Service Intelligence
Service Analyzer
Auto Refresh: 1 minute (Global default)
Last 12 hours
Save as...
Save
Filter services
Select services to monitor
Filter KPIs
Select KPIs to monitor
Filter by tags
Select tags to monitor
Created By: All
Show disabled services
Show service dependencies
KPI Value: Aggregate
Tile Size: Large
AMT 2
AMT 1
AMT 4
AMT 3
AMT 11
AMT 7
AMT 8
AMT 5
AMT 6
AMT 9
AMT 10

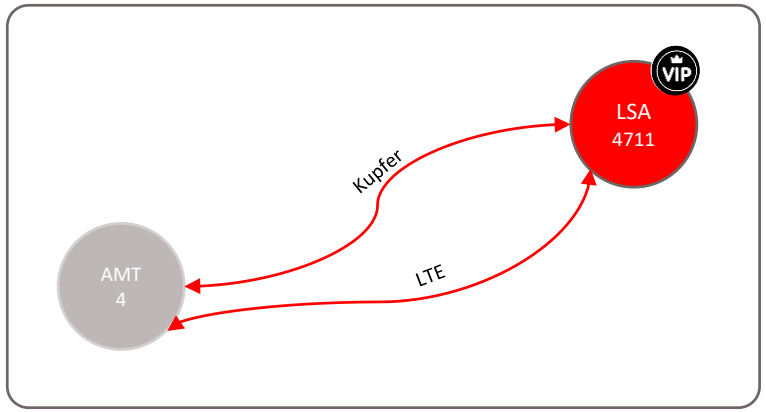

splunk>enterprise
Apps
Dirk Nitschke
Messages
Settings
Activity
Help
Find
Service Analyzer
Entity Overview
Alerts and Episodes
Glass Tables
Deep Dives
Dashboards
Configuration
Search
IT Service Intelligence
Service Analyzer
Auto Refresh: 1 minute (Global default)
Last 12 hours
Save as...
Save
Filter services
Select services to monitor
Filter KPIs
Select KPIs to monitor
Filter by tags
Select tags to monitor
Created By: All
Show disabled services
Show service dependencies
KPI Value: Aggregate
Tile Size: Large
AMT 2
AMT 1
AMT 4
AMT 3
AMT 11
AMT 7
AMT 8
AMT 5
AMT 6
AMT 9
AMT 10


splunk>enterprise
Apps
Dirk Nitschke
Messages
Settings
Activity
Help
Find
Service Analyzer
Entity Overview
Alerts and Episodes
Glass Tables
Deep Dives
Dashboards
Configuration
Search
IT Service Intelligence
Service Analyzer
Auto Refresh: 1 minute (Global default)
Last 12 hours
Save as...
Save
Filter services
Select services to monitor
Filter KPIs
Select KPIs to monitor
Filter by tags
Select tags to monitor
Created By: All
Show disabled services
Show service dependencies
KPI Value: Aggregate
Tile Size: Large
Open Ticket
76
Maintenance
88
Status Ämter
AMT 4
83
AMT 2
74
AMT 5
44%
Info ...
Info ...
Info ...
Brandenburg
Reinicken-
dorf
Spandau
Charlottenburg-
Wilmersdorf
Friedrichshain-
Kreuzberg
Tempelhof-
Neu-
Steglitz-
Zehlendorf
Schöne-
berg
kölln
Treptow-
Köpenick
Brandenburg

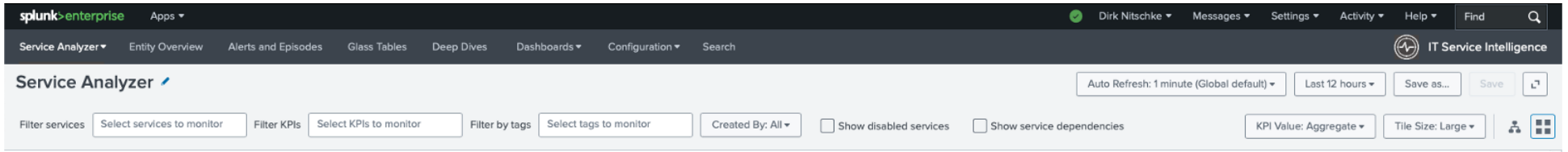


AMT 4 – LSA-4711 Status – Ausfall des Service

Status	LSA	Indicator	Time
Ausfall des Service	LSA 4711 – VIP	Service Netzanschluss	2024-12-31 – 23:23:00
Performance	LSA 4712	Latenzen	2024-12-31 – 22:23:01
Störung	LSA 4713	Service Netzanschluss	2024-12-31 – 22:23:01

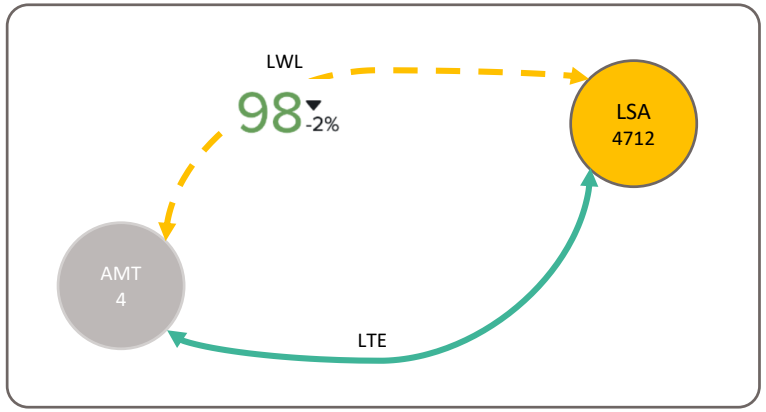


Ticket ID	LSA	Status	Time	Assigned to
A001 – Prio 1	LSA 4711 – VIP	In Progress	2024-12-31 – 23:23:00	Firma Z
D234 – Prio 2	LSA 4712	Testing	2024-12-31 – 22:23:01	Firma Y
G678 – Prio 2	LSA 4713	Waiting for Replay	2024-12-31 – 22:23:01	Firma H



AMT 4 – LSA-4712 Status – Paketverluste

Status	LSA	Indicator	Time
Ausfall des Service	LSA 4711 – VIP	Service Netzanschluss	2024-12-31 – 23:23:00
Performance	LSA 4712	Latenzen	2024-12-31 – 22:23:01
Störung	LSA 4713	Service Netzanschluss	2024-12-31 – 22:23:01



Ticket ID	LSA	Status	Time	Assigned to
A001 – Prio 1	LSA 4711 – VIP	In Progress	2024-12-31 – 23:23:00	Firma Z
D234 – Prio 2	LSA 4712	Testing	2024-12-31 – 22:23:01	Firma Y
G678 – Prio 2	LSA 4713	Waiting for Replay	2024-12-31 – 22:23:01	Firma H

splunk>enterprise Apps ▾ | Dirk Nitschke ▾ | Messages ▾ | Settings ▾ | Activity ▾ | Help ▾ | Find

Service Analyzer ▾ | Entity Overview | Alerts and Episodes | Glass Tables | Deep Dives | Dashboards ▾ | Configuration ▾ | Search | IT Service Intelligence

Service Analyzer

Auto Refresh: 1 minute (Global default) ▾ | Last 12 hours ▾ | Save as... | Save

Filter services: Select services to monitor | Filter KPIs: Select KPIs to monitor | Filter by tags: Select tags to monitor | Created By: All ▾ | Show disabled services | Show service dependencies | KPI Value: Aggregate ▾ | Tile Size: Large ▾

Lichtsignalanlagen Infrastruktur

93	83	Open Tickets	P1 Tickets
Overall Health Score	Predictive Health Score	196	8

96 LSA-Konnektivität

94	Glasfaser
99	Kupfer
73	Mobile Funk

IDoc Failures: 1,000 / 800 / 698 / 400 / 200 / 0

Failed RFC: 380

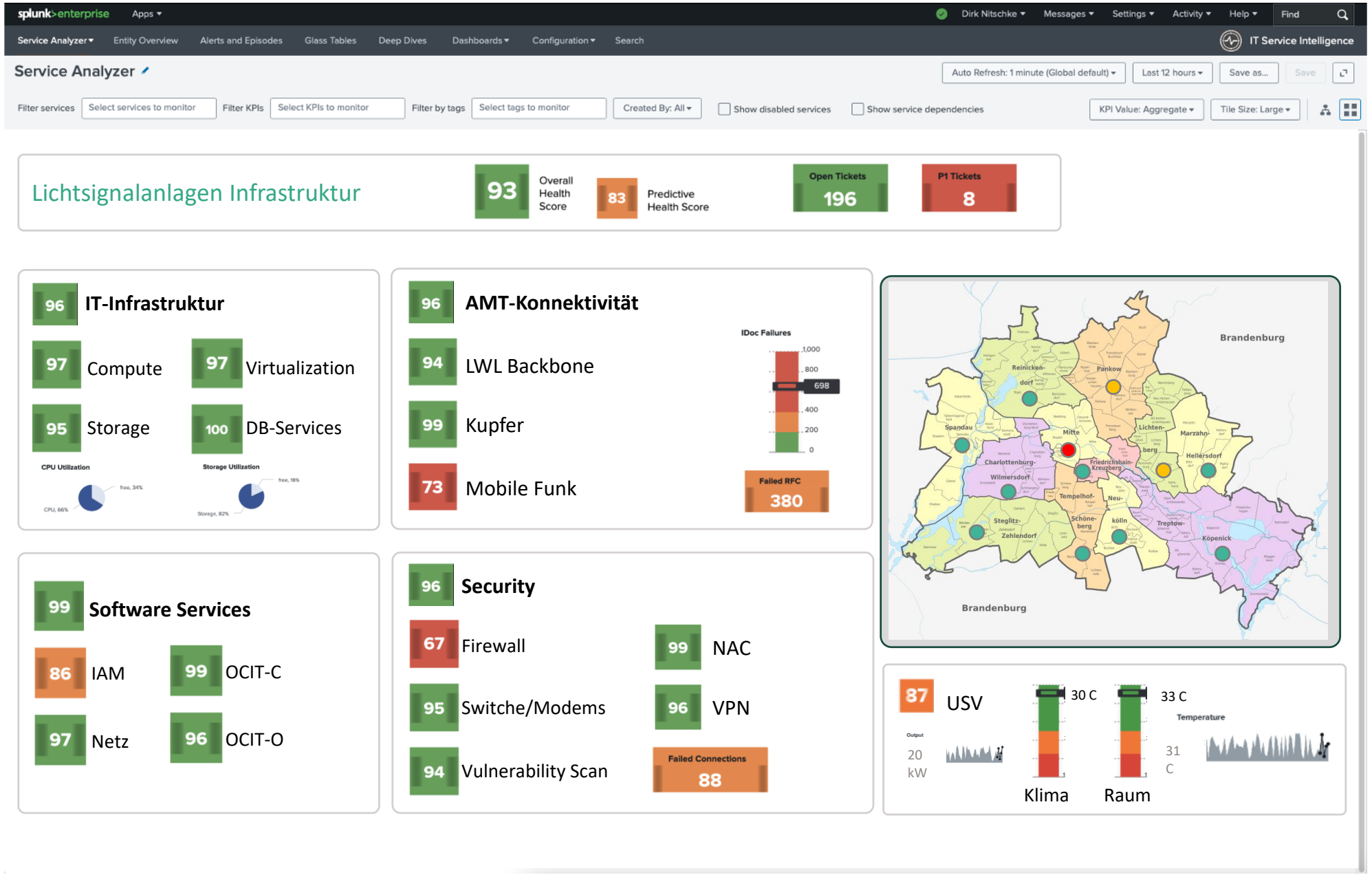
99 Software Services

86	IAM
97	Netz
99	OCIT

96 Security

67	Firewall	99	NAC
95	Switch/Modems	96	VPN
94	Vulnerability Scan	Failed Connections	88

Temperature: 30.4C


splunk>enterprise
Apps
Dirk Nitschke
Messages
Settings
Activity
Help
Find
Service Analyzer
Entity Overview
Alerts and Episodes
Glass Tables
Deep Dives
Dashboards
Configuration
Search
IT Service Intelligence
Service Analyzer
Auto Refresh: 1 minute (Global default)
Last 12 hours
Save as...
Save
Filter services
Select services to monitor
Filter KPIs
Select KPIs to monitor
Filter by tags
Select tags to monitor
Created By: All
Show disabled services
Show service dependencies
KPI Value: Aggregate
Tile Size: Large
Lichtsignalanlagen Infrastruktur
93
Overall Health Score
83
Predictive Health Score
Open Tickets
196
P1 Tickets
8
96
IT-Infrastruktur
97
Compute
97
Virtualization
95
Storage
100
DB-Services
CPU Utilization
Storage Utilization
96
AMT-Konnektivität
94
LWL Backbone
99
Kupfer
73
Mobile Funk
IDoc Failures
1,000
800
698
400
200
0
Failed RFC
380
Brandenburg
Brandenburg
99
Software Services
86
IAM
99
OCIT-C
97
Netz
96
OCIT-O
96
Security
67
Firewall
99
NAC
95
Switche/Modems
96
VPN
94
Vulnerability Scan
Failed Connections
88
87
USV
Output
20
kW
30 C
33 C
Temperature
31
C
Klima
Raum

Was monitoren wir (1/2)

Service Health

- Status aller Verkehrssteuerungservices: Up/Down/Degraded – in Echtzeit.

KPIs

- Verfügbarkeit pro LSA-Knotenpunkt, Verkehrsrechner etc. sowie IP-SLAs der Switches und Firewalls

Syslog & Eventlogs

- Switches, Firewalls, Virtualisierungsserver, Datenbanken, Linux-Server, Webanwendungen, Bedienrechner, NTP-Server und Multiplexer

Performance

- Latenz Steuergerät–Zentrale, Verbindungsabbrüche
- IP-SLAs der Switches und Firewalls

Incidents

- Bei Ausfall oder Schwellwertüberschreitung erfolgt eine automatische Ticket-Generierung

SNMP-Daten

- Klimaanlagen und USV-Anlagen sowie Netzkomponenten bilden die Grundlage für Verfügbarkeits- und Fehleranalysen

Was monitoren wir (2/2)

SLA-Tracking

- *Die vertraglich zugesicherte Verfügbarkeit ist lückenlos dokumentiert*

Trendanalysen

- *Frühzeitige Erkennung von Degradierungen einzelner LSA-Knoten, Verkehrsrechner oder Leitungsverbindungen im Zeitverlauf*

Supplier-Monitoring

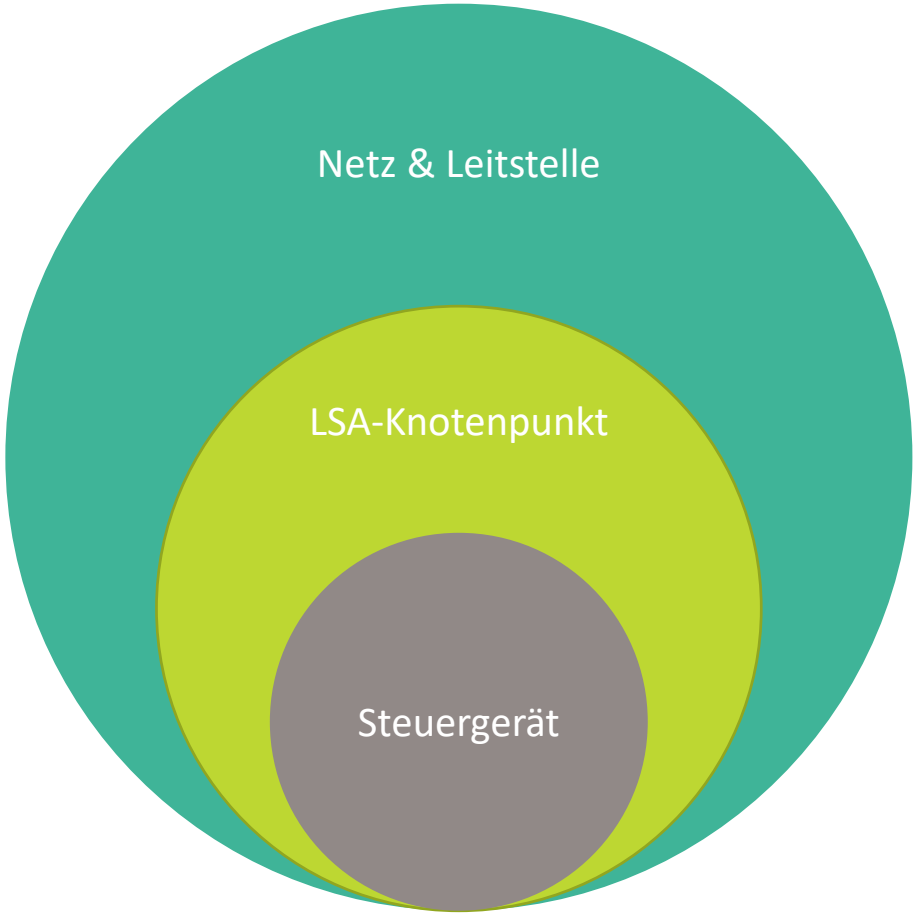
- *Echtzeit-Status der Performance der Dienstleister*

Kapazitäten

- *Die Auslastung und Bandbreite im Netzwerk oder auf den IaaS-Plattformen bilden die Grundlage für Investitionsentscheidungen*

Technische Umsetzung

- Architektur-Bausteine
  1. **Splunk ITSI**
     Service-Modellierung – LSA als vollständiges Service-Objekt mit Health Score
  2. **Datenquellen**
     Syslog, SNMP, Ticket-System, DB-Queries
  3. **Automatisierung**
     Anomaly Detection & automatisches Ticket-Routing bei definierten Ereignissen



Bonus: Nachhaltigkeit und Energie

- *Wenn ohnehin alle Betriebsdaten in Splunk fließen, lässt sich das Energiemonitoring nahtlos integrieren, ohne dass eine zusätzliche Infrastruktur erforderlich ist.*

Energie & Klima

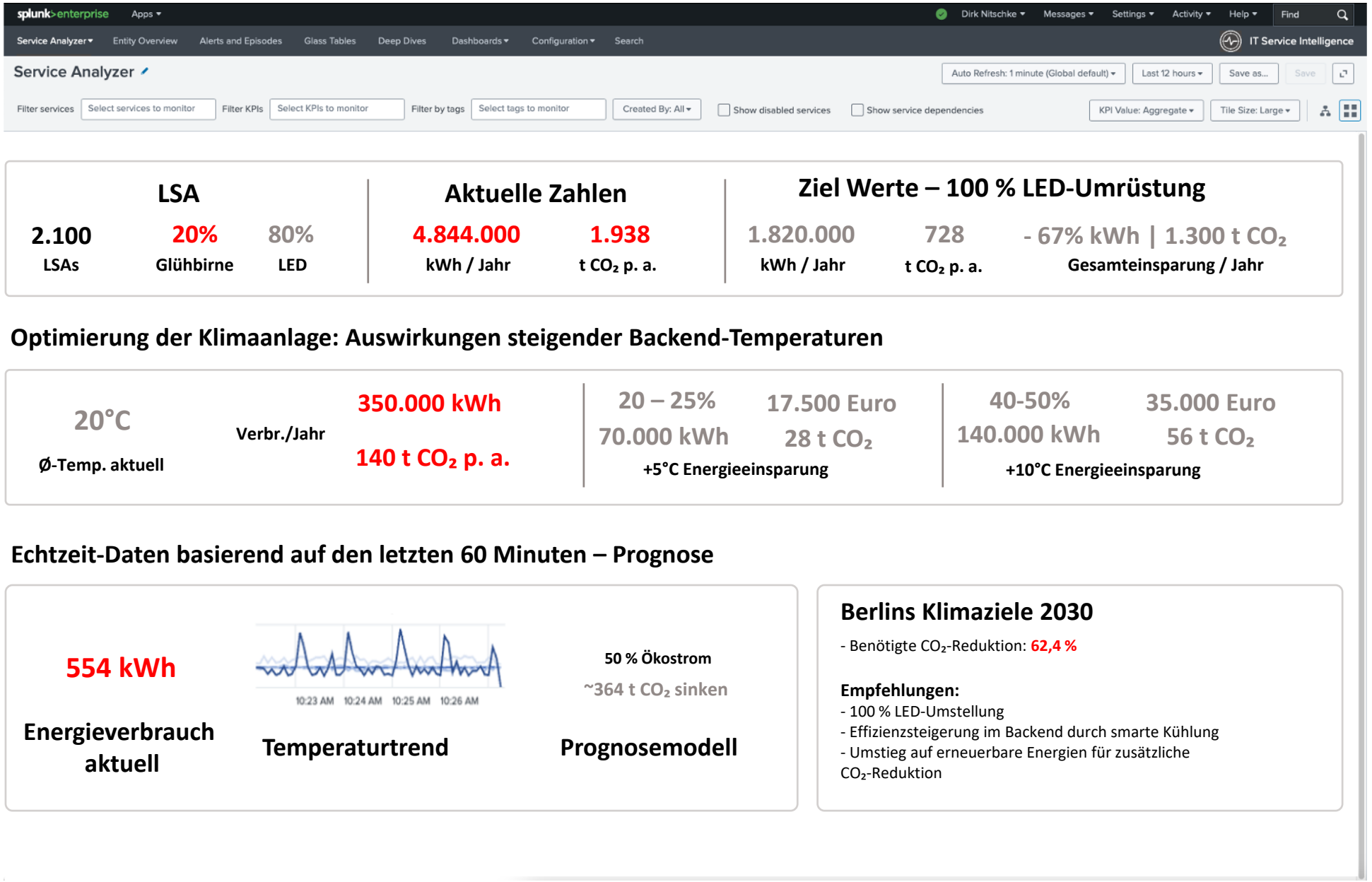
- ***Die einzelnen Standorte werden hinsichtlich Temperatur, Energieverbrauch und CO2-Emissionen analysiert.***
- *Es gibt keine isolierten Metriken, sondern ganzheitliche Service-Objekte mit Abhängigkeiten.*

Prognosemodelle

- *Die Einsparungspotenziale durch die Umstellung auf LED und die optimierte Kühlung sollen quantifizierbar gemacht werden.*

Klimaziele 2030

- *Beitrag zu Berlins Klimazielen messbar – Reporting für Politik und Stakeholder.*


splunk>enterprise
Apps
Dirk Nitschke
Messages
Settings
Activity
Help
Find
Service Analyzer
Entity Overview
Alerts and Episodes
Glass Tables
Deep Dives
Dashboards
Configuration
Search
IT Service Intelligence
Service Analyzer
Auto Refresh: 1 minute (Global default)
Last 12 hours
Save as...
Save
Filter services
Select services to monitor
Filter KPIs
Select KPIs to monitor
Filter by tags
Select tags to monitor
Created By: All
Show disabled services
Show service dependencies
KPI Value: Aggregate
Tile Size: Large
LSA
2.100
LSAs
20%
Glühbirne
80%
LED
Aktuelle Zahlen
4.844.000
kWh / Jahr
1.938
t CO₂ p. a.
Ziel Werte – 100 % LED-Umrüstung
1.820.000
kWh / Jahr
728
t CO₂ p. a.
- 67% kWh | 1.300 t CO₂
Gesamteinsparung / Jahr
Optimierung der Klimaanlage: Auswirkungen steigender Backend-Temperaturen
20°C
Ø-Temp. aktuell
Verbr./Jahr
350.000 kWh
140 t CO₂ p. a.
20 – 25%
70.000 kWh
17.500 Euro
28 t CO₂
+5°C Energieeinsparung
40-50%
140.000 kWh
35.000 Euro
56 t CO₂
+10°C Energieeinsparung
Echtzeit-Daten basierend auf den letzten 60 Minuten – Prognose
554 kWh
Energieverbrauch aktuell
10:23 AM
10:24 AM
10:25 AM
10:26 AM
Temperaturtrend
50 % Ökostrom
~364 t CO₂ sinken
Prognosemodell
Berlins Klimaziele 2030
- Benötigte CO₂-Reduktion: 62,4 %
Empfehlungen:
- 100 % LED-Umstellung
- Effizienzsteigerung im Backend durch smarte Kühlung
- Umstieg auf erneuerbare Energien für zusätzliche CO₂-Reduktion

Lessons Learned

1

Start simple

- Wenige KPIs, aber die richtigen. Lieber drei aussagekräftige Metriken als zwanzig, die niemand liest.

2

Service-Modell ist King

- Das Dashboard-Design sollte kontinuierlich auf Basis von echtem User-Feedback verbessert werden.

3

Team-Alignment

- Betrieb, Security, Dienstleister und Betriebsrat sollten frühzeitig einbezogen werden.
- Akzeptanz entsteht durch Mitgestaltung.

4

Iterativ vorgehen

- *Die Auslastung und Bandbreite im Netzwerk oder auf den IaaS-Plattformen bilden die Grundlage für Investitionsentscheidungen*

infra:signal
GRÜNBERLIN

Vielen Dank!