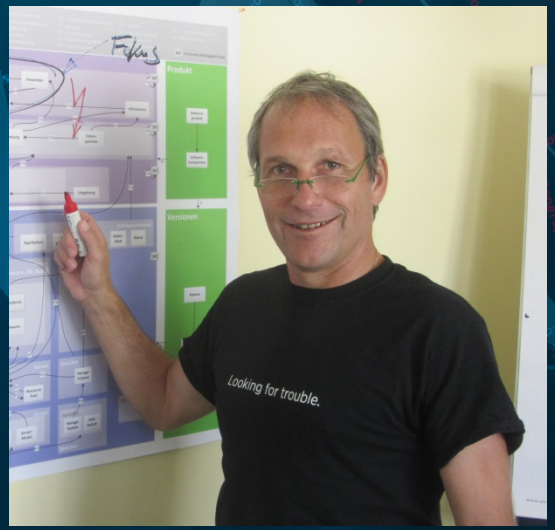
Copyright © 2015 Splunk Inc.

.conf2015

Reducing Incidents and Enhancing Services with Operational Intelligence



Andreas Jahnke

Manager Monitoring, DATEV

andreas.jahnke@datev.de

splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Referenced customers for ITSI product participated in a limited release software program that included items at no charge.

The Company

The Company

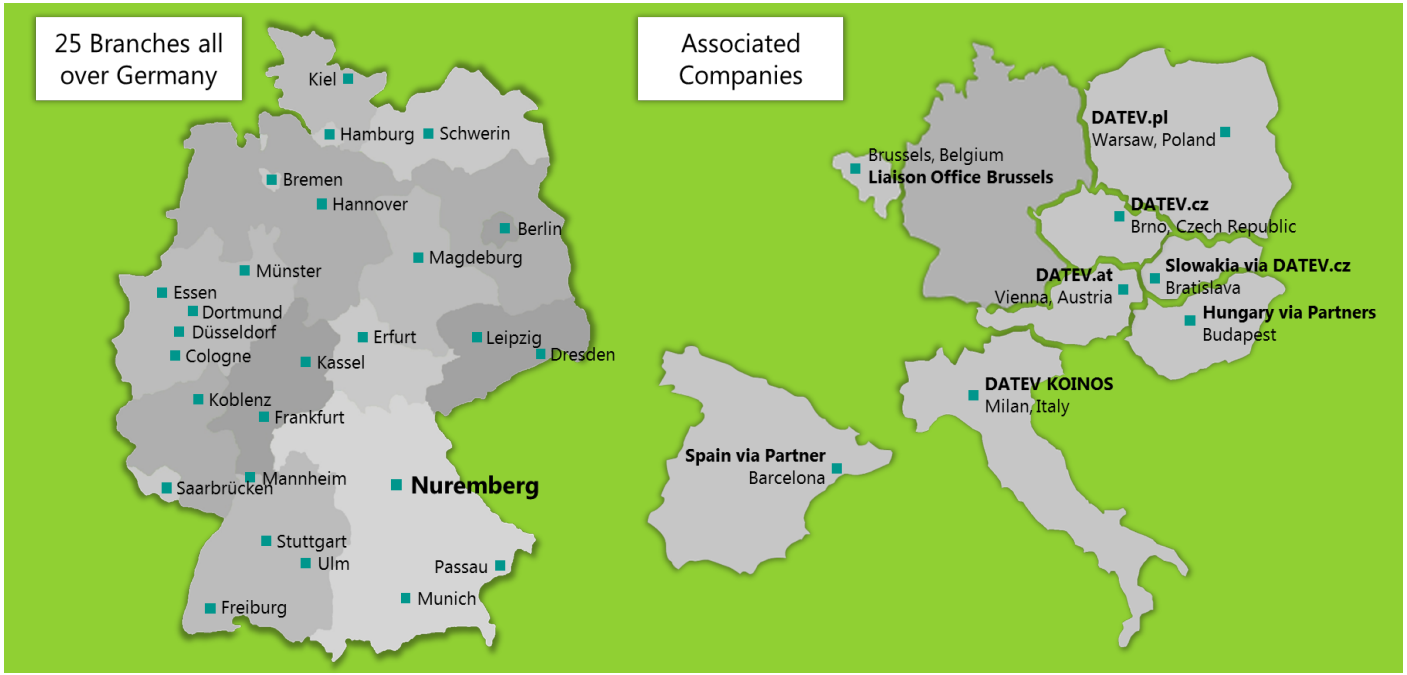
DATEV eG
Headquarters: Nuremberg
Foundation: 1966

Professional EDP service organization in Europe for:

- tax consultants
- lawyers
- attested auditors
- certified public accountants

The Company

Branches in Germany, liaison offices in Berlin, Brussels, and associated companies



DATEV: Mission and Members

Our Purpose

- Economical promotion of our members (40,393 in 2014)
- That means: Supporting all services carried out by our members on behalf of their clients

Our Members

- tax consultants
- lawyers
- certified public accountants
- attested auditors
- tax consulting companies
- auditing companies
- lawyer companies

DATEV – Member – Client

DATEV‘s Customers: Members and their clients

Range of Products

Software

e.g.

- Accounting
- Audit
- Human Resources
- Business Advice
- Internal Organization

ca. 1m active Financial Accounting and 11.5m Payroll Slips each month

Services

e.g.

- Personal Service
- Electronic Service
- Service Applications

1,138 employees provided with ca. 1.79m service contacts in 2014

Advice/Knowledge

e.g.

- Strategic Advice
- Advice for Start-Ups
- Service Applications
- Further Education
- Literature
- Databases

About 200,000 users attended DATEV seminars in the year 2014

Data Processing Center, Printing and Shipment

Facts and Figures

CPU:
- 52,741 MIPS
- 2 IBM 2827 H66
- 2 IBM 2818-M10/Z03 ICF

Servers:
- 1,602 Unix
- 7,088 Windows

Storage:
- 31.6 PB on disc drives and tape cartridges

Printing:
- 35 laser printers
- 5 colour printers
- 2 inkjet – continuous printers

Shipment:
- 14m envelopes per month

Key Figures

Financial years 2010 - 2014

	Turnover (m Euro)	Employees	Members	Investment (in Euro)
2014	844	6,780	40,393	107.0
2013	803	6,606	40,274	66.0
2012	760	6,411	40,013	61.0
2011	731	6,110	39,771	44.7
2010	699	5,844	39,756	39.5

Splunk at DATEV

Why Splunk?

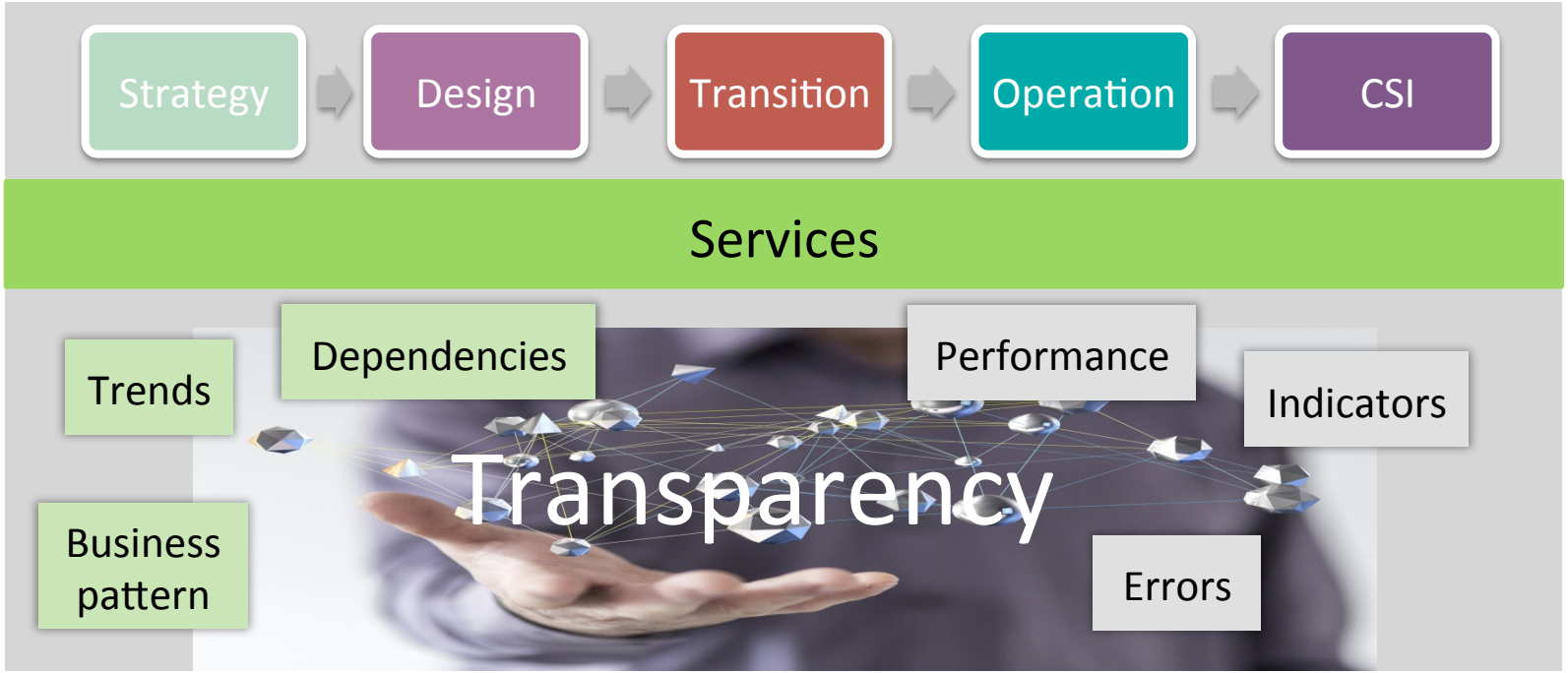
Use cases:

- **Improving services**
  - **Availability, Reliability, Performance & Security**

- **Handling of (major) incidents**
  - **Common view of IT, reducing mean time to repair (MTTR) & mean time to investigate (MTTI)**

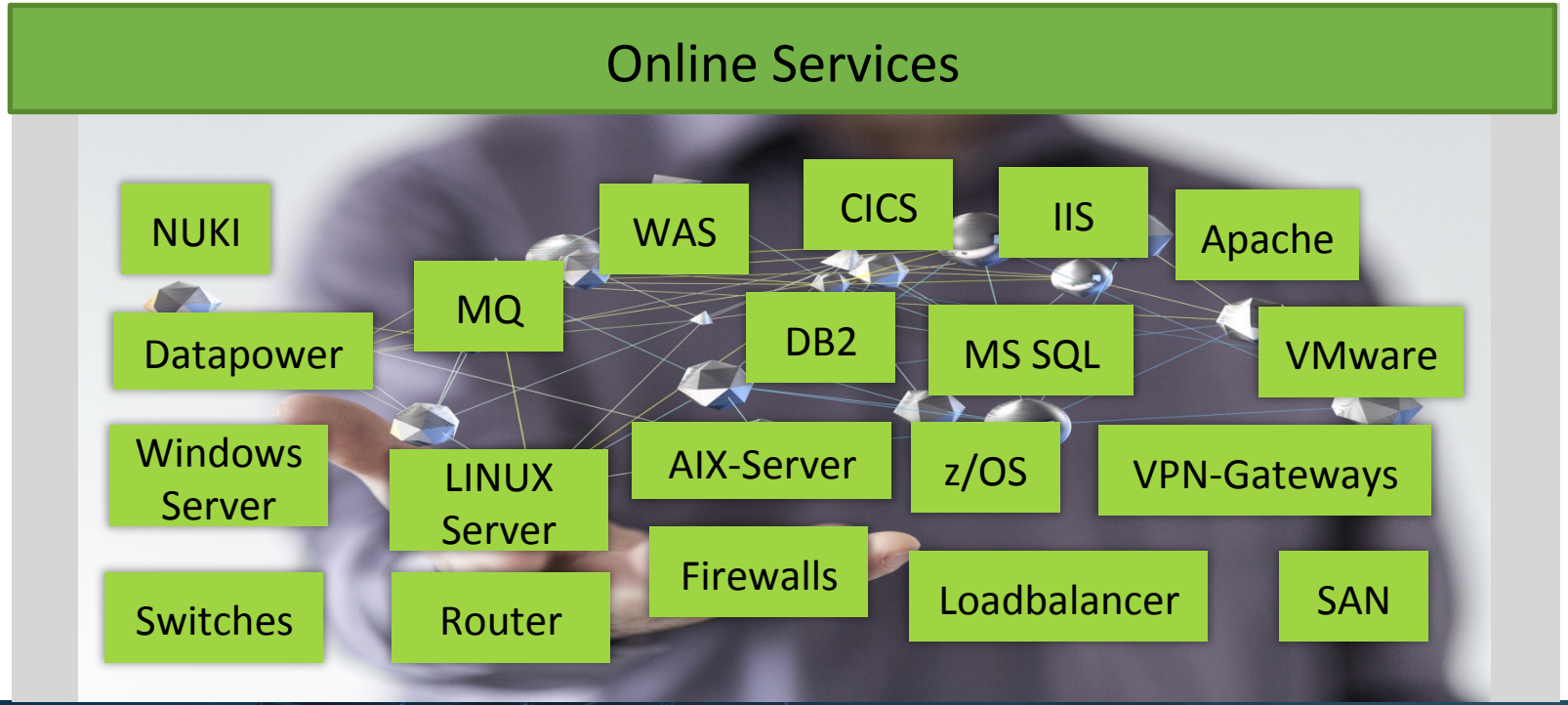
How? Improving Services

Supporting all ITIL stages



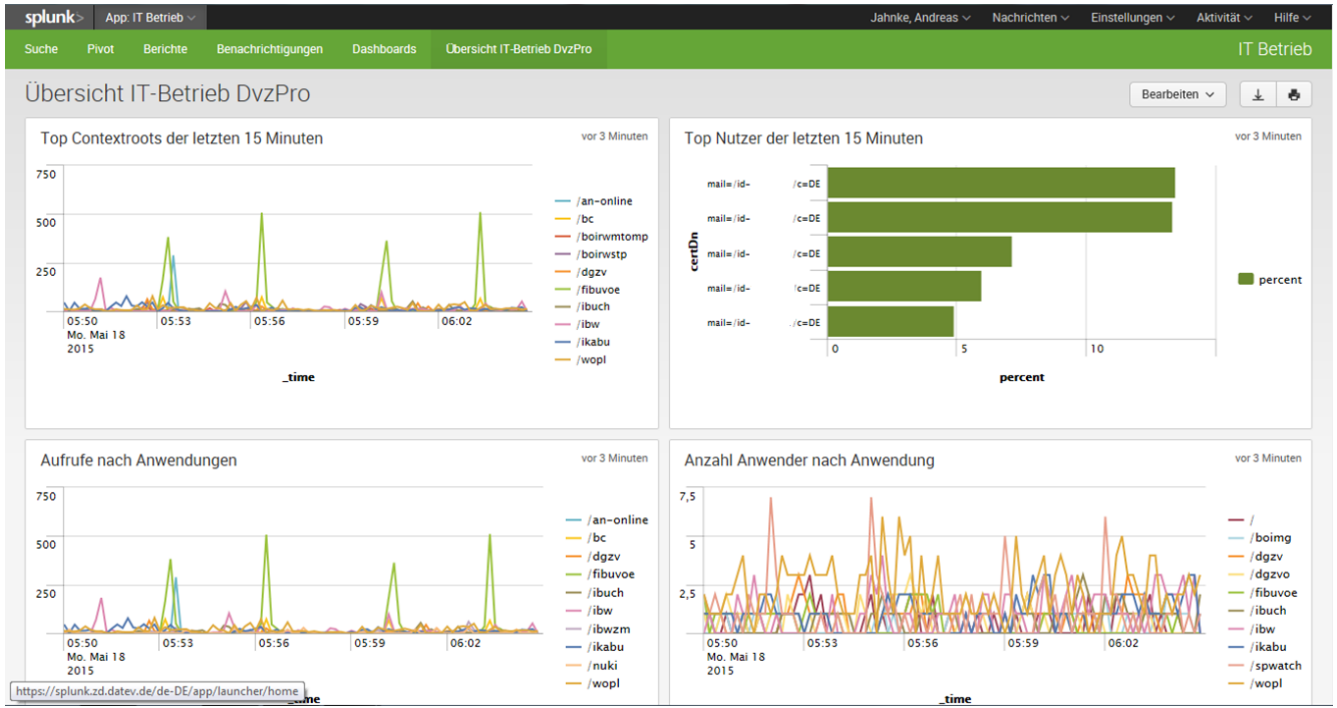
How? Improving Services

Example



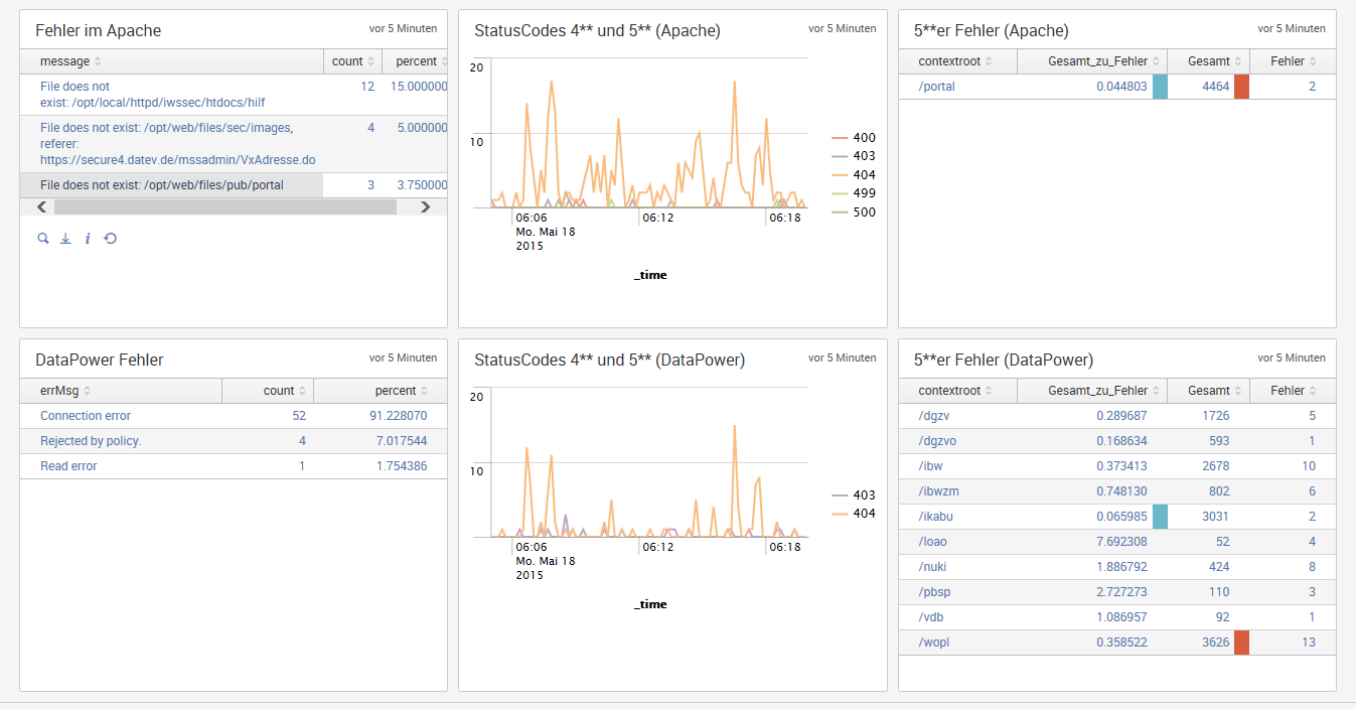
Implementation - Improving Services

Dashboard “Online Services“



Implementation - Improving Services

Dashboard “Online Services“



How? Handling of (Major) Incidents

Creating a task force

- **Main Targets:**
  - **Reducing MTTR**
  - **Reducing investigation expense**
  - **Common view of IT**
  - **Establishing central logfile analysis (Splunk)**
  - **Integration with monitoring & ITSM**

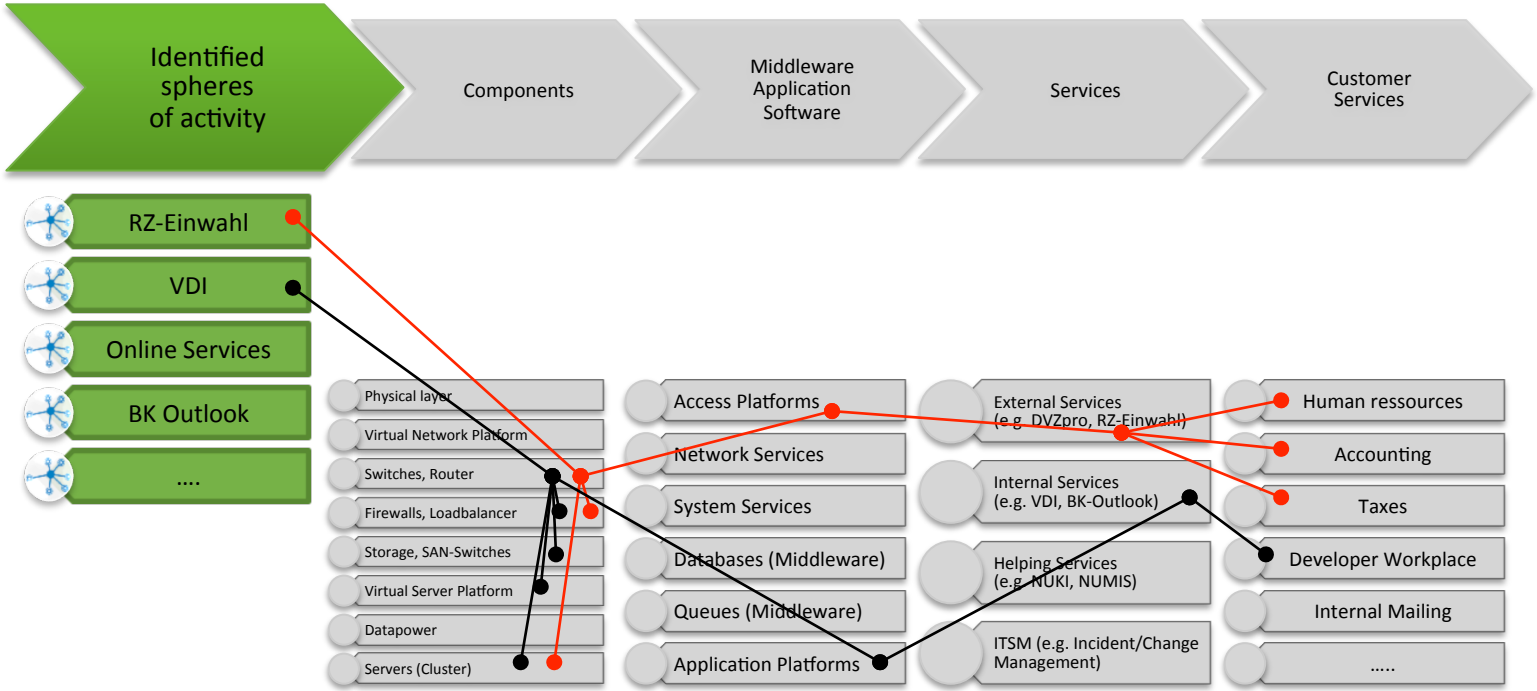
How? Handling of (Major) Incidents

Creating a task force

- **Analyzing** major incidents, problem records & event history
- **Assessment** with service owner, technical & application management, event management
- **Prioritizing** the identified **spheres of activity**

How? Handling of (Major) Incidents

Service-oriented activities of the task force (examples)



How? Handling of (Major) Incidents

Activites of the task force

- **Initial meeting** with all stakeholders
- **Assessment of log data** (classification of confidence, regulations by law, quality, quantity) & **approval**
- **Integration of log data** into central Splunk system
- **Creating requests and dashboards**…..

How? Handling of (Major) Incidents

Activites of the task force

- **Knowledge transfer to stakeholders** in the organisation (analyze techniques, monitoring, handling of Splunk)
- **Creating events & forwarding** to the existing central **Event Management System** (Omnibus) and **Service Monitoring** with **Escalation**

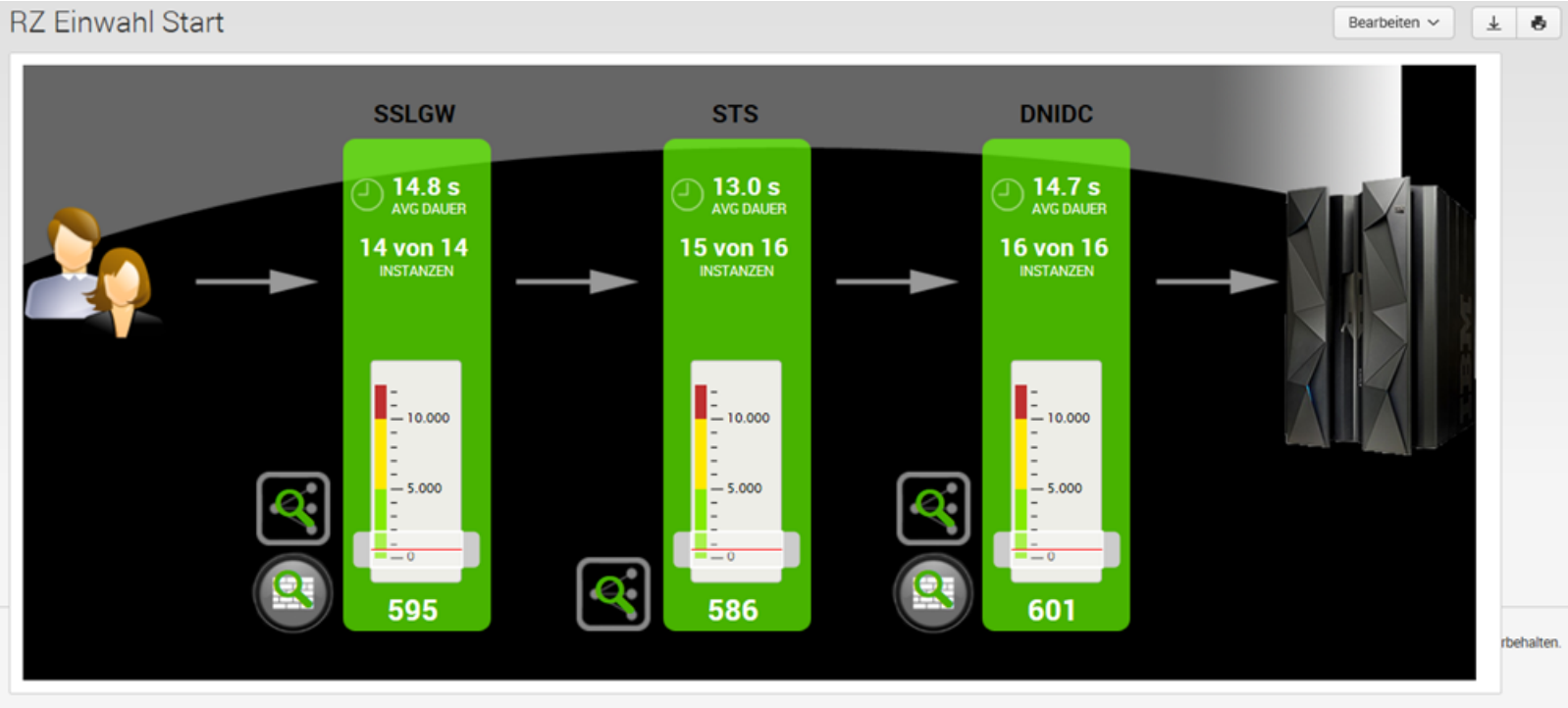
How? Handling of (Major) Incidents

Activites of the task force

- **Indications** for tool consolidation
- **Review** of all activities, agile optimization (lessons learned)
- **Management Reports/reviews per quarter**

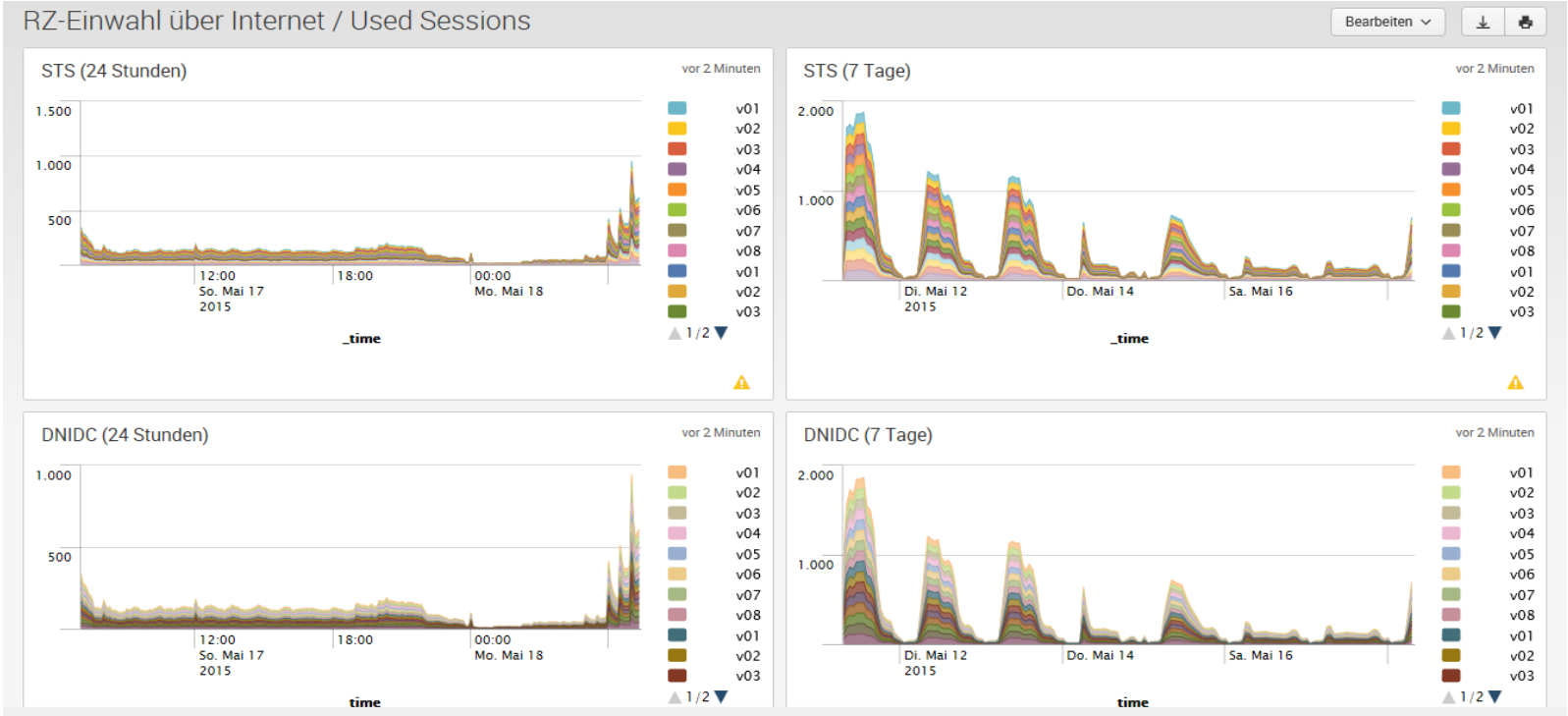
Implementation: Handling of (Major) Incidents

Dashboard “RZ-Einwahl“



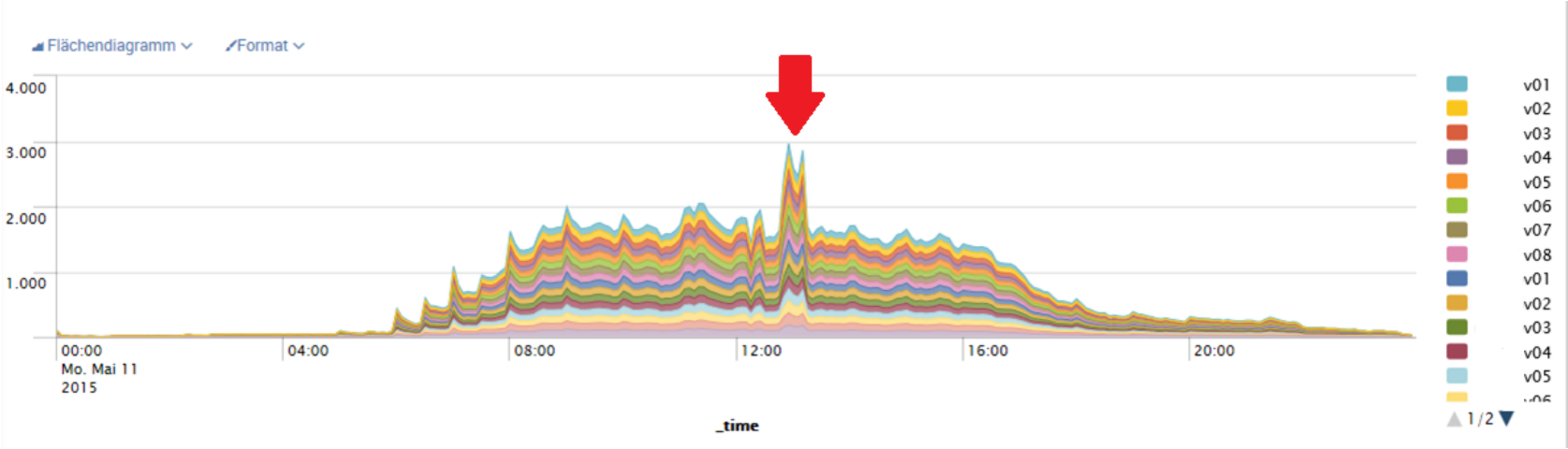
Implementation: Handling of (Major) Incidents

Dashboard “RZ-Einwahl“ (more details)



Implementation: Handling of (Major) Incidents

Dashboard “RZ-Einwahl“ (incident host application)



Benefits & Problems

DATEV

- ↑ **Improves productivity** of development, service, technical & application management (quality testing, troubleshooting)
- ↑ **Improves quality** of online services
- ↓ **Slow implementation & knowledge transfer** because of lack of human resources
- ↓ **Complex user management** with access to log data

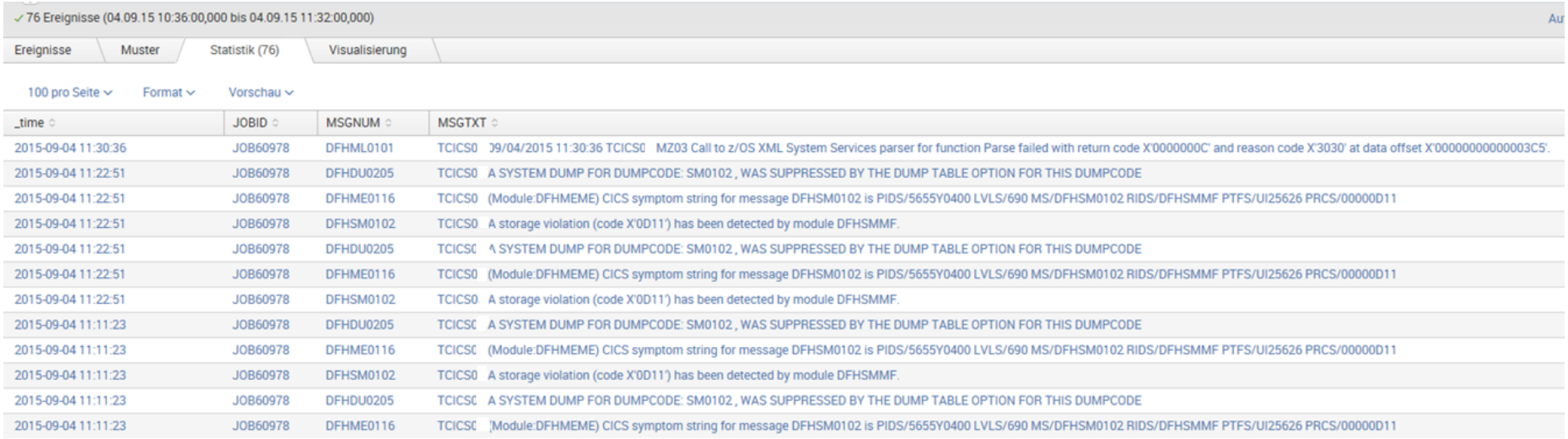
Benefits & Problems

Splunk

- **Easy setup,** central management
- **High performance** (realtime), **scalability & stability**
- **High usability**
- **Flexible organization (with partners)** e. g. new feature requests
- **Integration of z/OS possible & done**
- **No z/OS-forwarder** in the standard portfolio, extra product from Syncsort with additional costs
- **Bugs AIX-forwarder** (solved) and **VMware App** (under progress)

Benefits: Integration of z/OS

Splunk & Syncsort



✓ 76 Ereignisse (04.09.15 10:36:00,000 bis 04.09.15 11:32:00,000)

Ereignisse | Muster | Statistik (76) | Visualisierung

100 pro Seite | Format | Vorschau

_time	JOBID	MSGNUM	MSGTXT
2015-09-04 11:30:36	JOB60978	DFHML0101	TCICS0 09/04/2015 11:30:36 TCICS0 MZ03 Call to z/OS XML System Services parser for function Parse failed with return code X'0000000C' and reason code X'3030' at data offset X'00000000000003C5'.
2015-09-04 11:22:51	JOB60978	DFHDU0205	TCICS0 A SYSTEM DUMP FOR DUMPCODE: SM0102 , WAS SUPPRESSED BY THE DUMP TABLE OPTION FOR THIS DUMPCODE
2015-09-04 11:22:51	JOB60978	DFHME0116	TCICS0 (Module:DFHMEME) CICS symptom string for message DFHSM0102 is PIDS/5655Y0400 LVLS/690 MS/DFHSM0102 RIDS/DFHSMMF PTFS/UI25626 PRCS/00000D11
2015-09-04 11:22:51	JOB60978	DFHSM0102	TCICS0 A storage violation (code X'0D11') has been detected by module DFHSMMF.
2015-09-04 11:22:51	JOB60978	DFHDU0205	TCICS0 A SYSTEM DUMP FOR DUMPCODE: SM0102 , WAS SUPPRESSED BY THE DUMP TABLE OPTION FOR THIS DUMPCODE
2015-09-04 11:22:51	JOB60978	DFHME0116	TCICS0 (Module:DFHMEME) CICS symptom string for message DFHSM0102 is PIDS/5655Y0400 LVLS/690 MS/DFHSM0102 RIDS/DFHSMMF PTFS/UI25626 PRCS/00000D11
2015-09-04 11:22:51	JOB60978	DFHSM0102	TCICS0 A storage violation (code X'0D11') has been detected by module DFHSMMF.
2015-09-04 11:11:23	JOB60978	DFHDU0205	TCICS0 A SYSTEM DUMP FOR DUMPCODE: SM0102 , WAS SUPPRESSED BY THE DUMP TABLE OPTION FOR THIS DUMPCODE
2015-09-04 11:11:23	JOB60978	DFHME0116	TCICS0 (Module:DFHMEME) CICS symptom string for message DFHSM0102 is PIDS/5655Y0400 LVLS/690 MS/DFHSM0102 RIDS/DFHSMMF PTFS/UI25626 PRCS/00000D11
2015-09-04 11:11:23	JOB60978	DFHSM0102	TCICS0 A storage violation (code X'0D11') has been detected by module DFHSMMF.
2015-09-04 11:11:23	JOB60978	DFHDU0205	TCICS0 A SYSTEM DUMP FOR DUMPCODE: SM0102 , WAS SUPPRESSED BY THE DUMP TABLE OPTION FOR THIS DUMPCODE
2015-09-04 11:11:23	JOB60978	DFHME0116	TCICS0 (Module:DFHMEME) CICS symptom string for message DFHSM0102 is PIDS/5655Y0400 LVLS/690 MS/DFHSM0102 RIDS/DFHSMMF PTFS/UI25626 PRCS/00000D11

The Future

DATEV & Splunk / Partner LCS

- **Integration with VMware**
- **Integration with Windows servers**
- **Proof-of-Concept Event Management System**
  (= tool consolidation)
- **Proof-of-Concept SIEM**

THANK YOU

splunk>