



The IT Service Provider Finanz Informatik

Who we are. What we do.

Content

- Overview of the company Finanz Informatik and Requirements
- Architecture
- Use case
- Questions

The company serves a large part of the German retail banking market

Finanz Informatik – Company

Revenue (in mill. €)	1,624
with saving banks	976
with state banks	338
Employees (full-time equivalents)	4,825

Customers

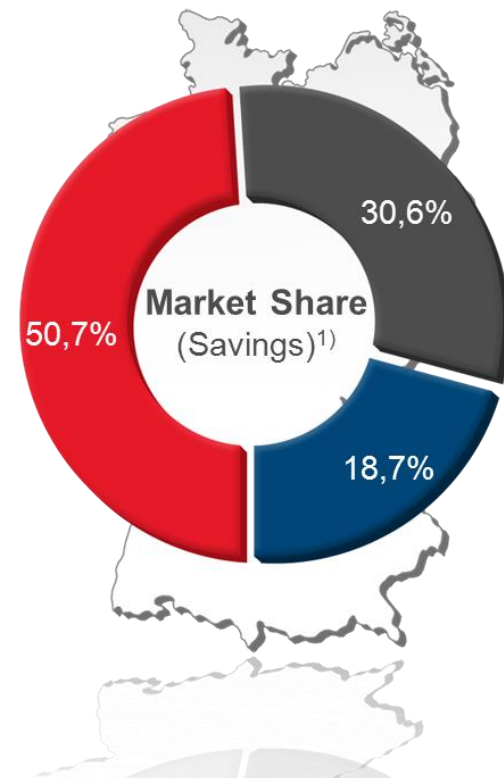
Savings banks	414
State banks + DekaBank	8
State home loan banks	9

Accumulated balance sheet of supported savings banks (in bill. €) (2014) 764

■ Savings Banks Financial Group ■ Credit Unions ■ Private Banks, other

December 30st, 2015

¹⁾ Sources: DSGV, statista (12/31/2014)



Significant scale can be achieved through bundling volume IT services

Supported financial institutions

Branches of supported savings banks	14,676
Bank-specific employees of supported savings banks	189,362

Processing volumes

Supported accounts (in mill.)	123
-------------------------------	-----

End devices

ATMs	24,693
Statement printers	14,155
Other self-service terminals	14,790
Booked entries per annum (in bill.)	11,6

December 31st, 2014



Finanz Informatik is competitively positioned with its comprehensive portfolio



What was our initial situation

.Requirements

Our Requirements for one solution

The Problem



Mainframe UNIX Windows Network

Different Enterprise solutions

Logfile analysis
Separated by platform



The Requirements

- High availability, efficiency and safety
- Cross-Platform correlation
- Multi-Tenancy
- Realtime reporting and alerting

The Solution



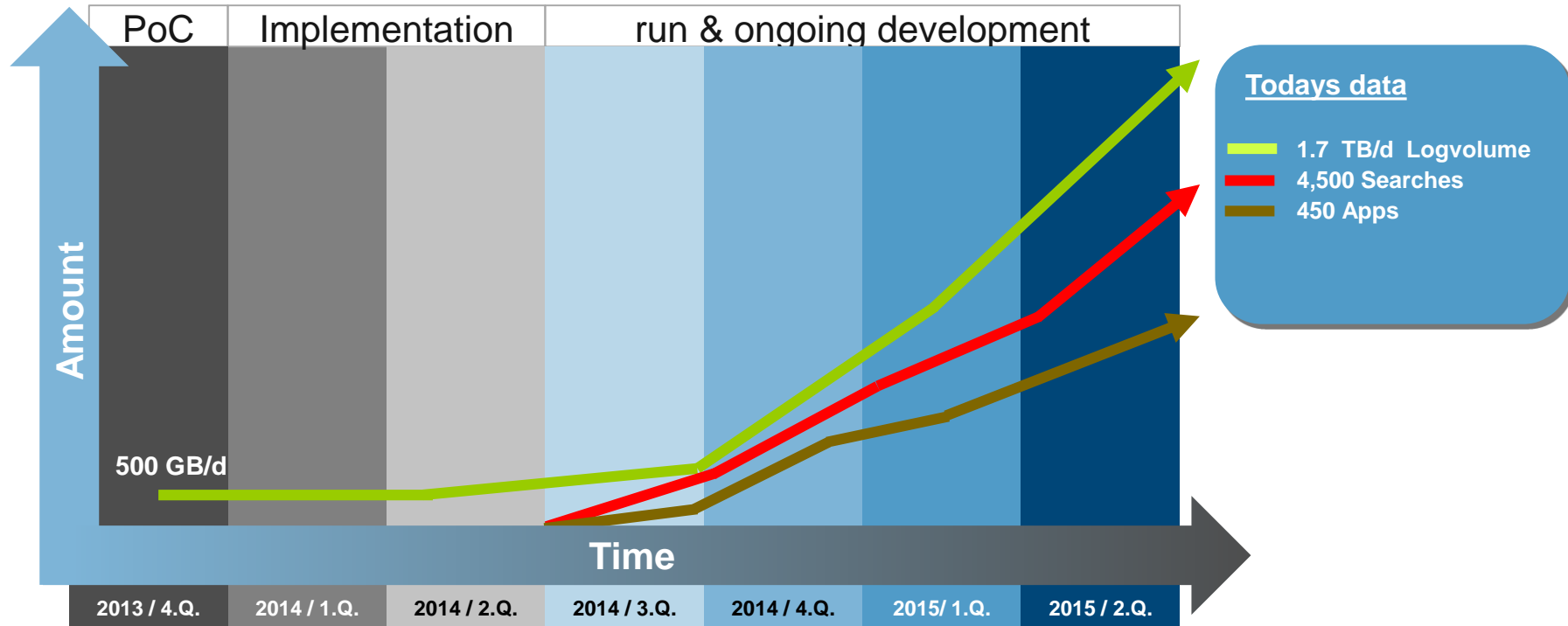
Mainframe UNIX Windows Network

splunk>

Logfile analysis
Cross-platform



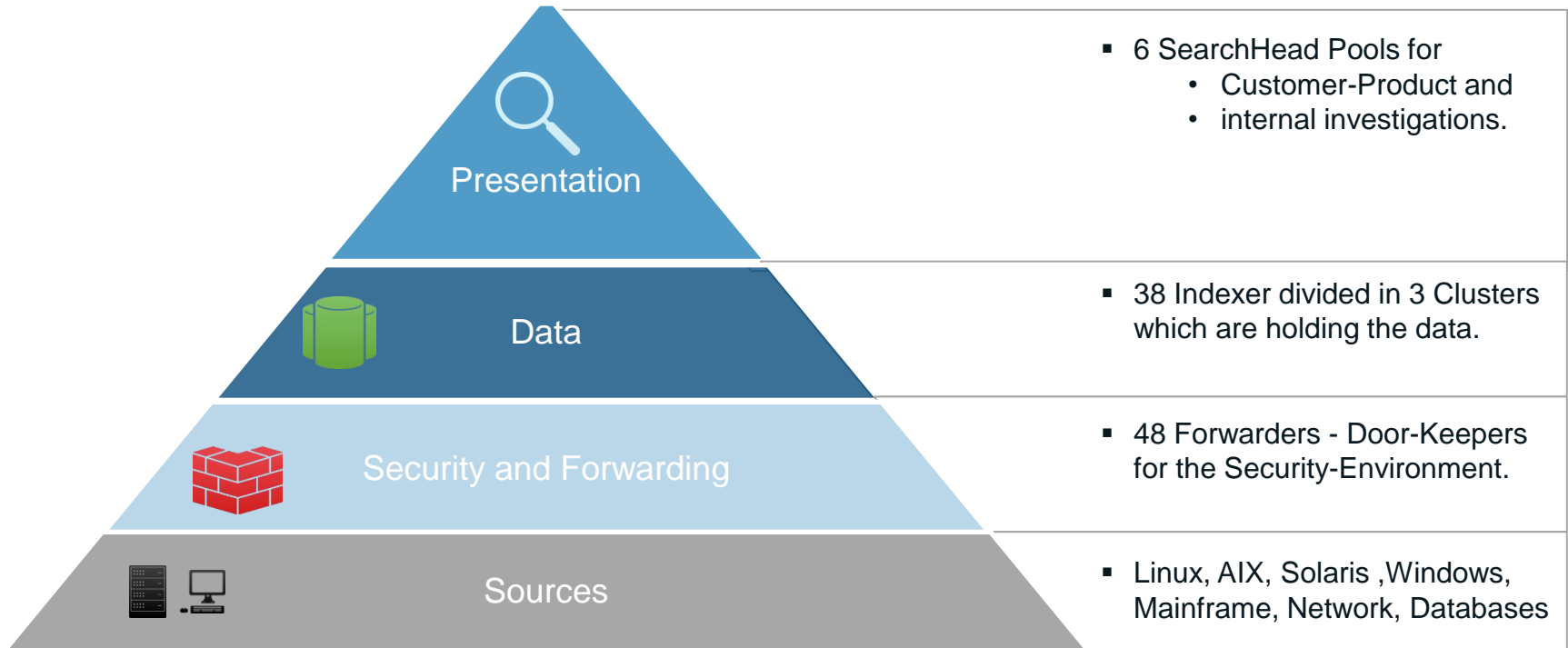
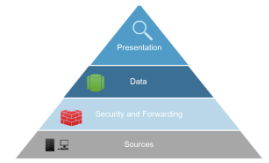
The todays result of our logvolume growth



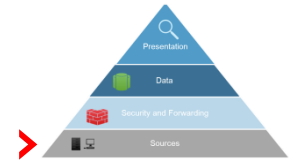
How we implemented the Requirements

.Architecture

FI-Architecture-Pyramid for splunk>

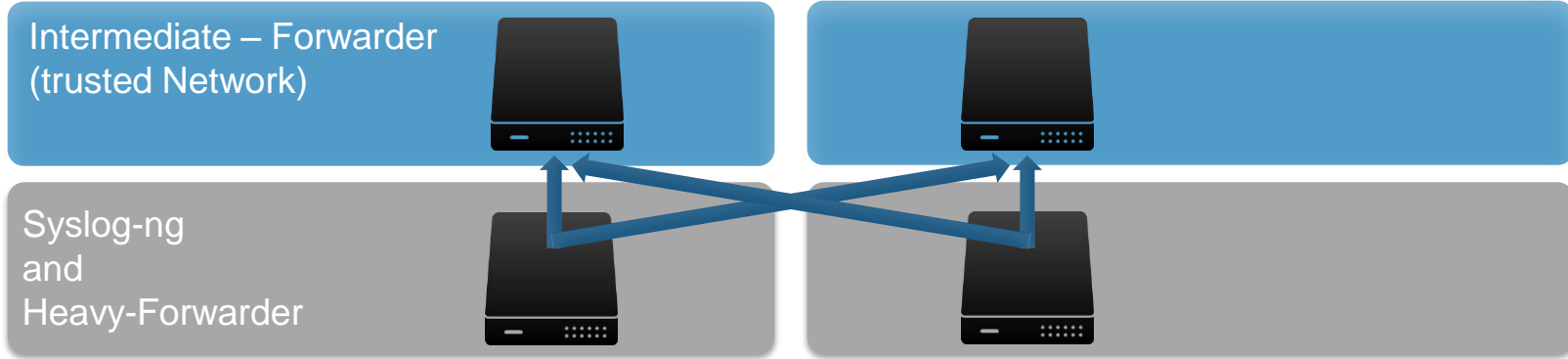


Transport-Layer – Syslogs and Heavy-Forwarders as entry points for the different sources

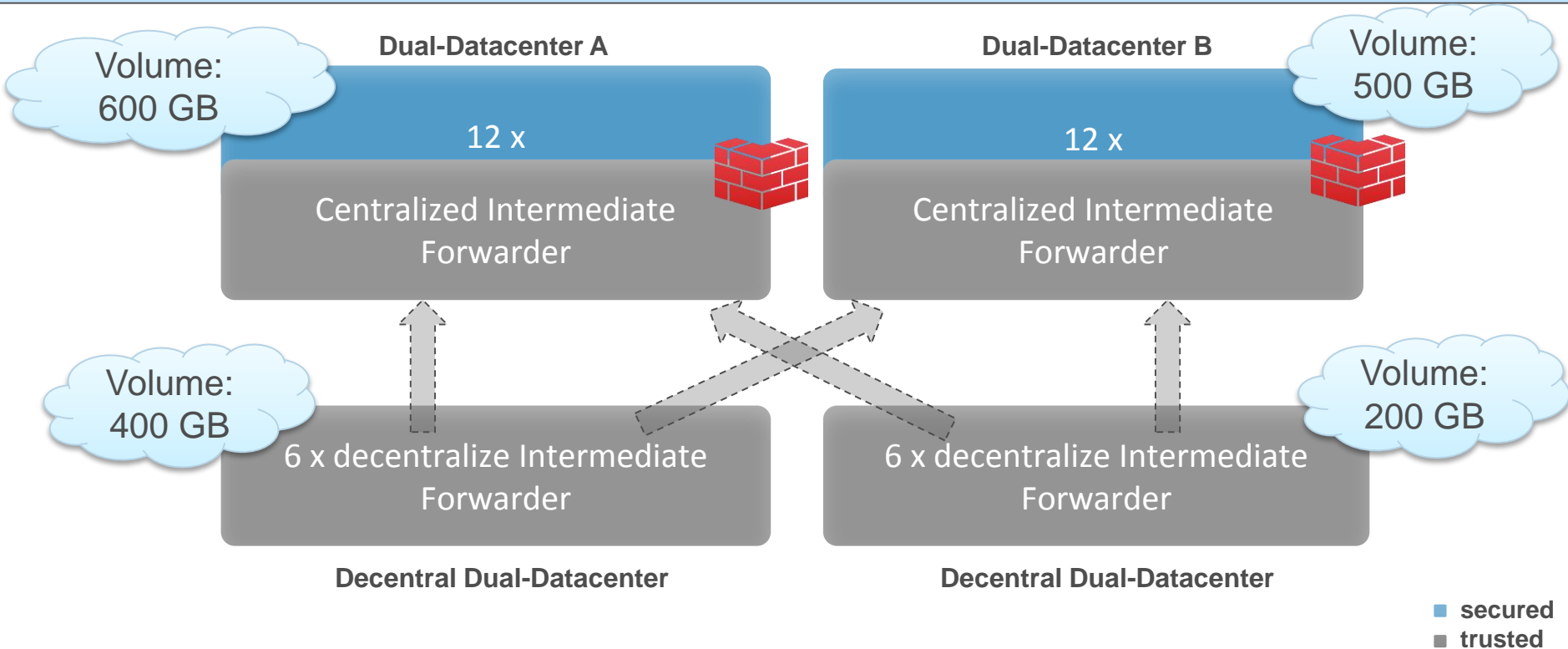
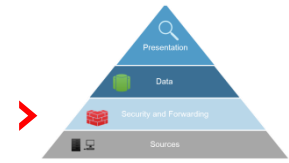


Datacenter 1

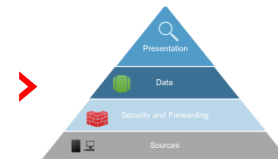
Datacenter 2



Decentral event-data transportation to the datacenters



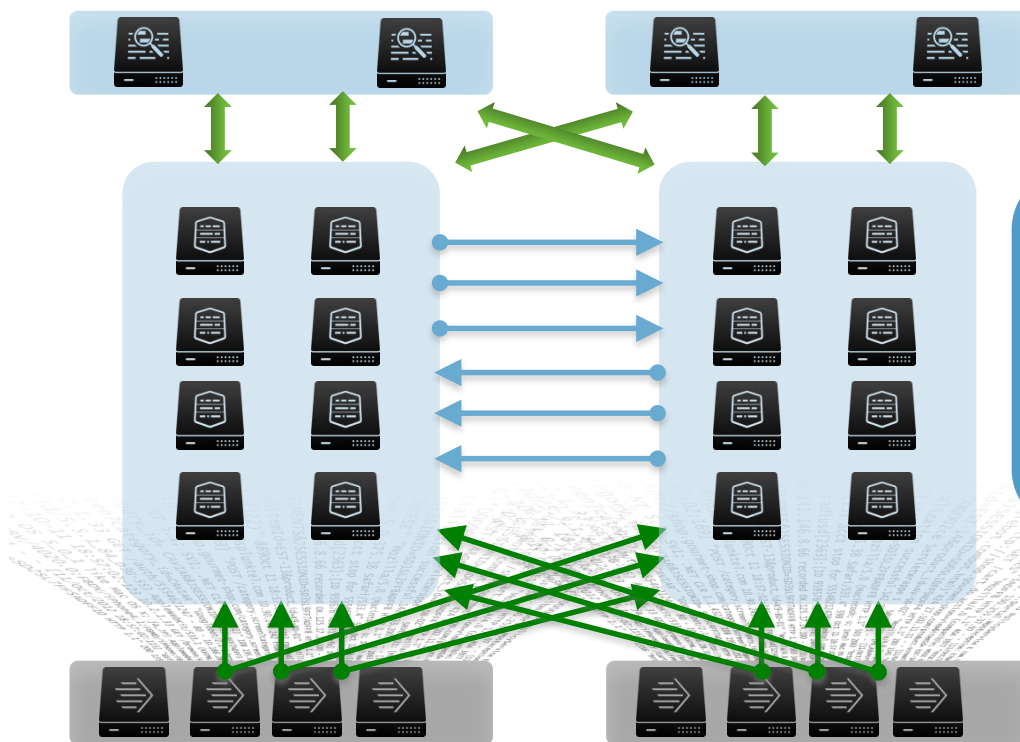
The Main-Core: Data delivering, replication and searching within a dual datacenter design



Searching

Replication and
distributed
data storing

Data delivering



Infrastructure-Data

38 Indexer (physical)

- each 24 Cores and 128 GB

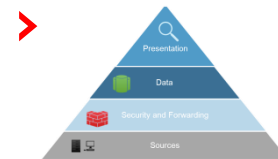
48 Forwarder

12 Search Heads (physical)

30 TB NAS

120 TB SAN

Presentation and Administration: Operating with well known apps ...



S.o.S - Splunk on Splunk



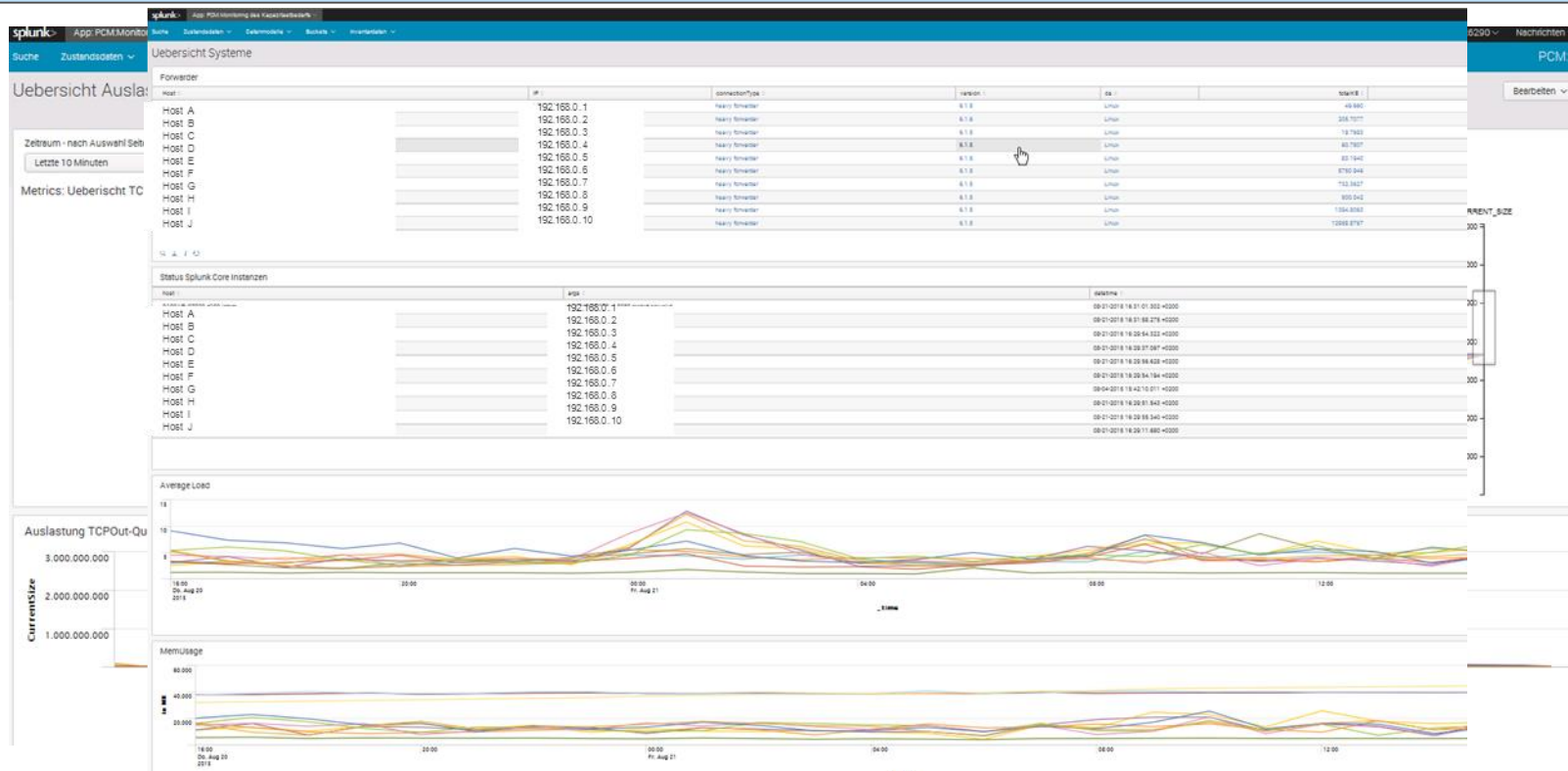
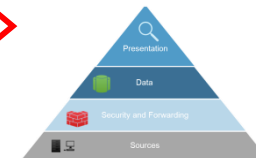
Data Governance



Splunk App for Unix and Linux

... and self developed Apps!

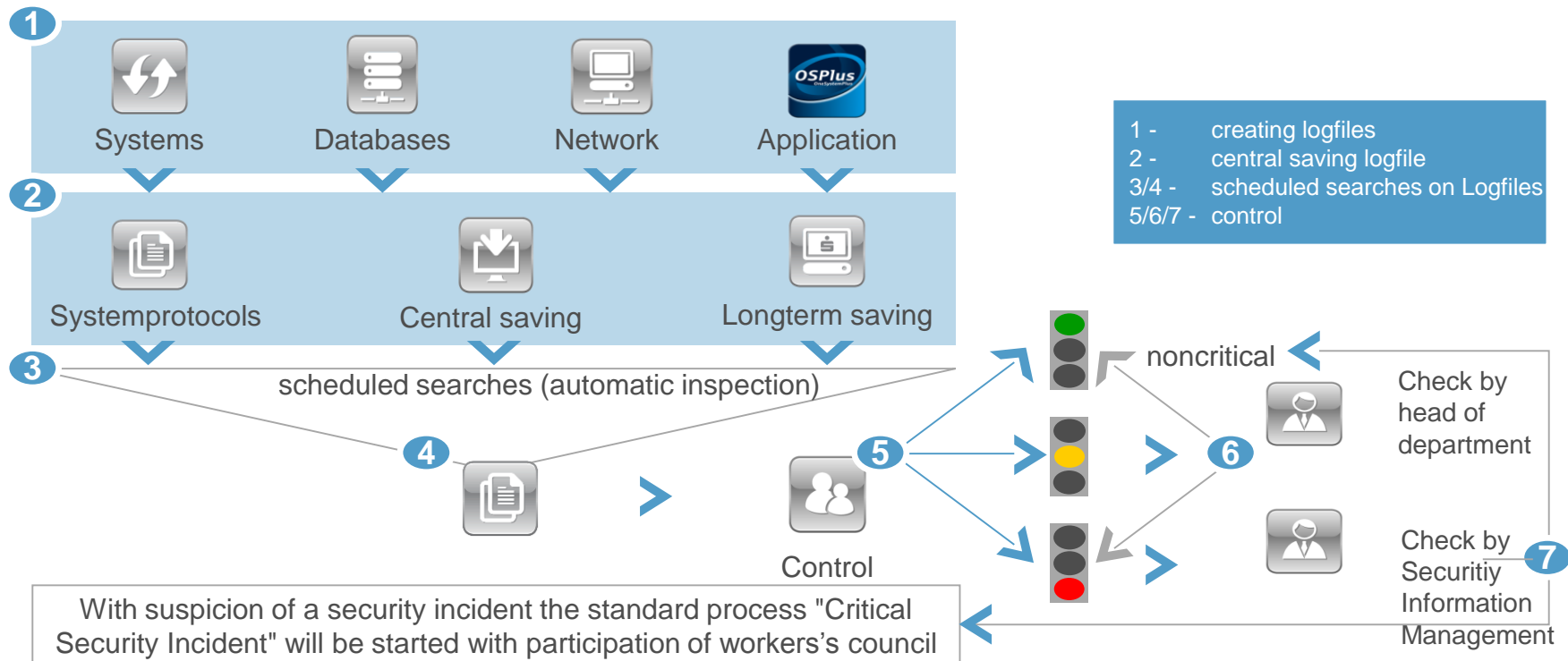
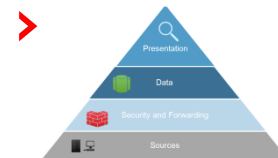
FI-Operation-Monitoring-App for administration and monitoring of the infrastructure



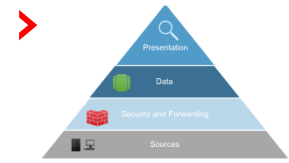
A short story about one of our main use cases

.Use case

Control checks the contact with customer data and follows on all platforms a uniform expiry



In the Finanz Informatik the demands of control are fulfilled with the application splunk>



Services of control are offered to saving banks and to Finanz Informatik departments

- **90 savings banks** (End of 2015) daily get the results of savedsearches as automatically created reports (pdf)
- each report inherits the results of (at the moment) 25 saved searches
- **Head of departments (Finanz Informatik)** also get daily reports and an alarm in one hour (in case of a security incident)
- depending on the requirement the amount of savedsearches is between 15 up to 30 savedsearches
- each report is equivalent to on app(UI)

login

- unsuccessful logons
- successful logons on non-buiseness times, etc.

Access to and change of configuration

- (un-)successful access to objects under control,etc.

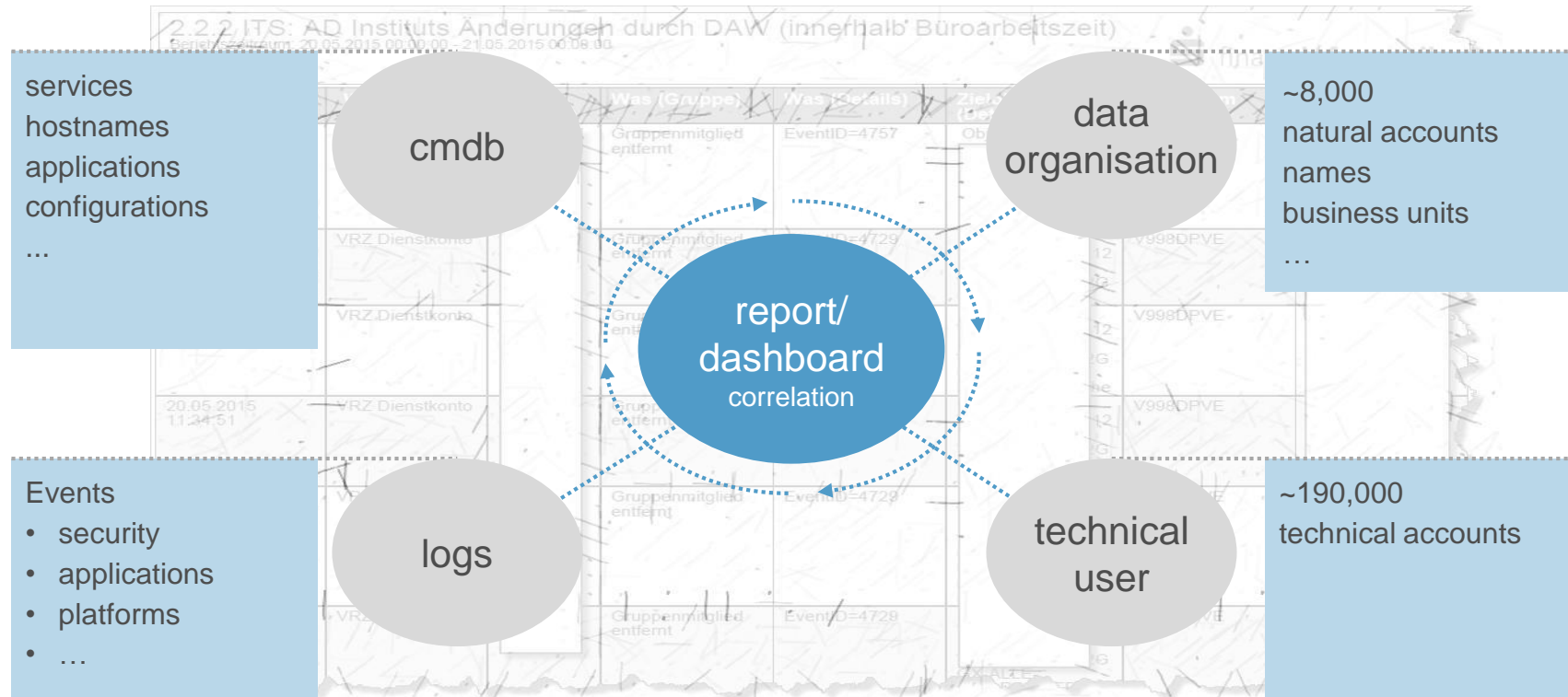
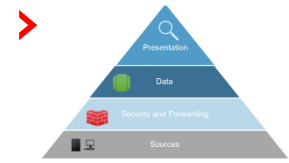
Change of access authorization

- creating and deleting/deactivating accounts, etc.
- blocking accounts
- right escalation

when – who – what – where – from where

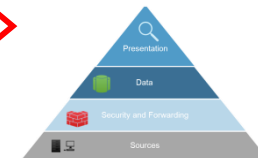
Datum/Zeit (Detail)	Wer (Gruppe)	Was (Gruppe)	Was (Detail)	Zeitsystem (Detail)	Zeitsystem (Detail)	Quelle (DetLog)
17.08.2015 00:55:09	Institut Benutzerkonto	Logon fehlgeschl.	EventID=680, LogonType=0, ResultCode=0xC0000064, Protocol=0			
17.08.2015 03:02:42	Institut Benutzerkonto	Logon fehlgeschl.	EventID=680, LogonType=0, ResultCode=0xC0000064, Protocol=0			
17.08.2015 06:08:02	Institut Benutzerkonto	Logon fehlgeschl.	EventID=680, LogonType=0, ResultCode=0xC0000064, Protocol=0			
17.08.2015 06:09:38	Institut Benutzerkonto	Logon erfolgreich	EventID=472, LogonType=0, ResultCode=0, Protocol=0			

Different sources and mechanisms are used to create ~200 dashboards/reports



Complex IT-architecture

High amount of searches will be scheduled daily in a short time period



~200 Apps (UI)

Platforms

- mainframe (zOS),
- unix (solaris, AIX, linux),
- Windows (2003, 2012)

Databases

- DB/2, Oracle, MSSQL, IMS

Network

- switches, routers, firewalls

Application

- OSPLus (core banking)
- transaction management
- identity access management
- and many, many more ...

System Control

~300 Technical Apps

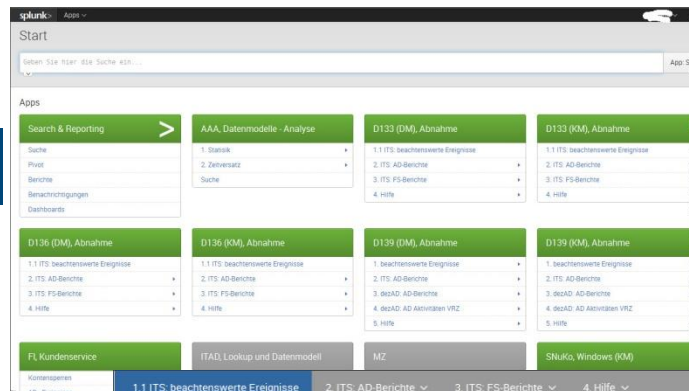
- TA, CFG, LK, SA



Administrator



Business Intelligence

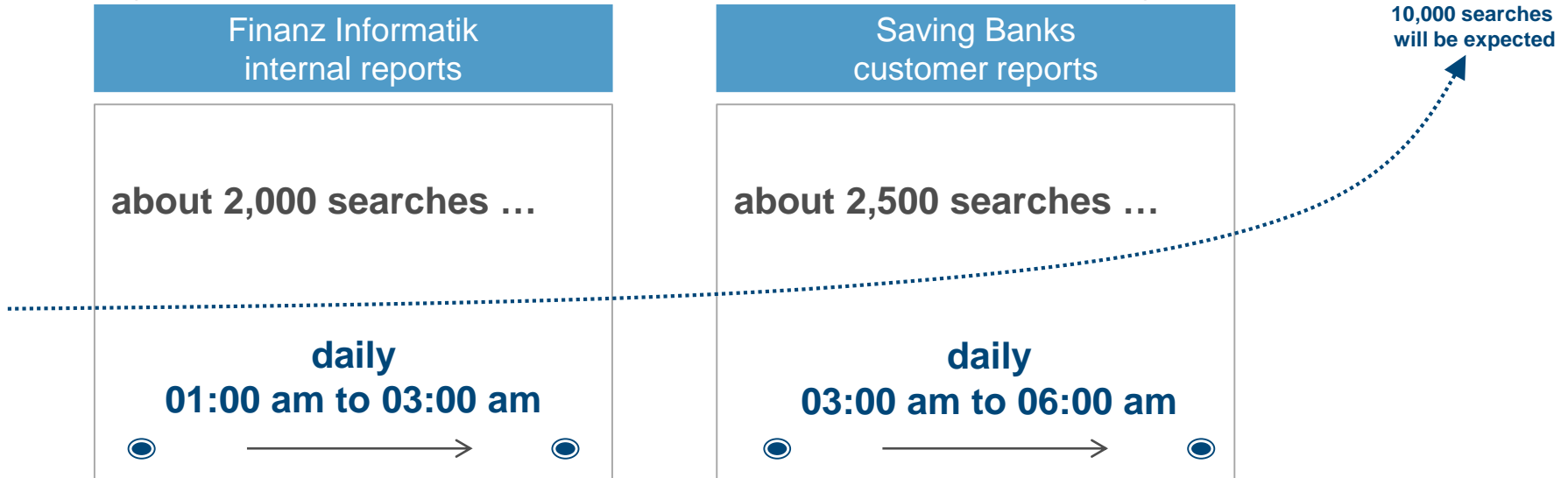


1.1 ITS: beachtenswerte Ereignisse				
Gestern				
ITS: Instituts Adminkonto	0	0	0	0
Kennwort neu gesetzt	gesperrt/deaktiviert	Berechtigungen geändert	Logon fehlerhaft	
ITS: Instituts Benutzerkonto	0	0	0	44
Kennwort neu gesetzt	gesperrt/deaktiviert	Berechtigungen geändert	Logon fehlerhaft	
ITS: Instituts Dienstkonto	0	0	0	0
interaktiv betätigt	Kennwort neu gesetzt	gesperrt/deaktiviert	Berechtigungen geändert	Logon fehlerhaft
ITS: Instituts non-standard Konto	0	0	0	0
interaktiv betätigt	Kennwort neu gesetzt	gesperrt/deaktiviert	Berechtigungen geändert	Aktivitäten festgestellt

Complex IT-architecture


Very great amount of searches will be scheduled daily in a short time period

Actually Finanz Informatik schedules about 4,500 searches a day



Great challenge for splunk> and infrastructure at Finanz Informatik (economic view)

.Questions?



Thank you for
your kind attention.



Back up