How Splunk Connects Business and IT at Swiss Bank PostFinance Ltd

Patrick Hofmann

Head of IT Infrastructure, PostFinance

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.

About Me – In a Nutshell

splunk>

About Me – In a Nutshell

Agenda

- PostFinance Ltd at a glance
- Splunk@PostFinance
- Use case 1 – Fraud detection and report generation for E-Payment
- Use case 2 – Online banking security and threat detection
- Wrap up

PostFinance
At a glance

splunk>

PostFinance at a Glance

One of the leading **retail financial institutes** of Switzerland

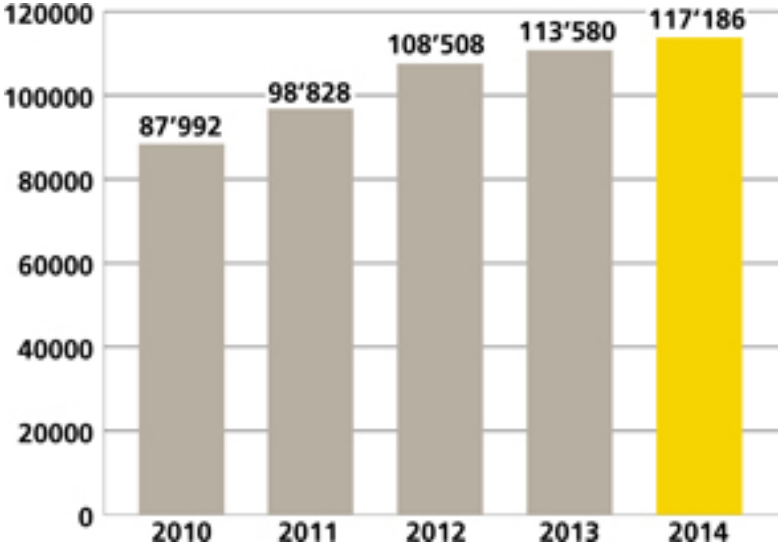
Number one in Swiss **payment transactions**

An ideal partner for customers who wish to **independently manage their finances**

Assets and Transactions

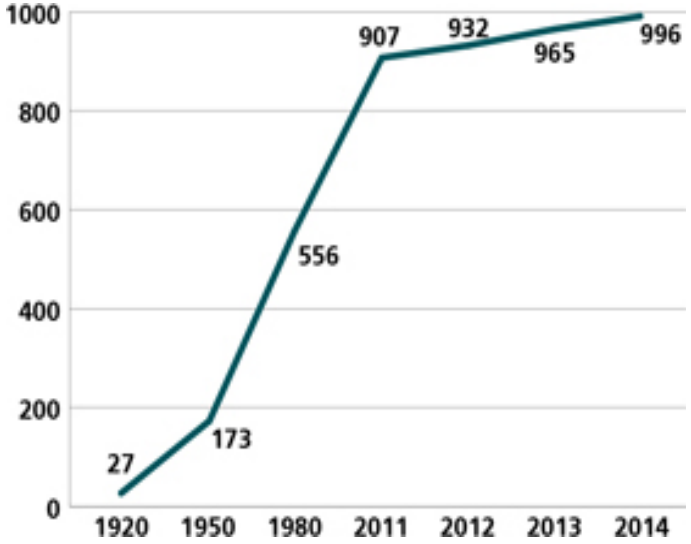
Customer funds (in CHF millions)

More and more customers entrust PostFinance with their money.



Transactions processed (in millions)

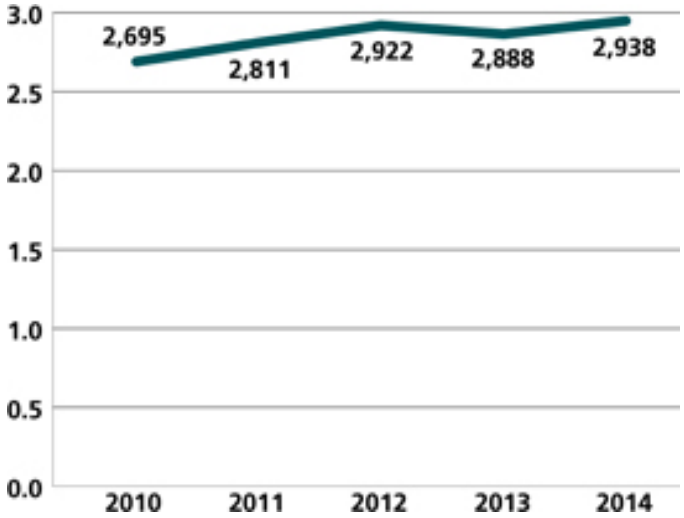
PostFinance is the market leader in Swiss payment transactions.



Customers Total and Online

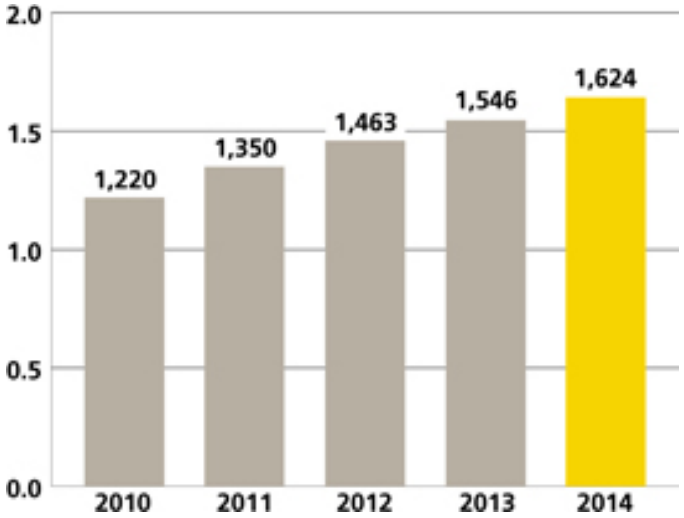
Number of customers (in millions)

PostFinance is one of Switzerland's leading retail financial institutions.



E-Finance users (in millions)

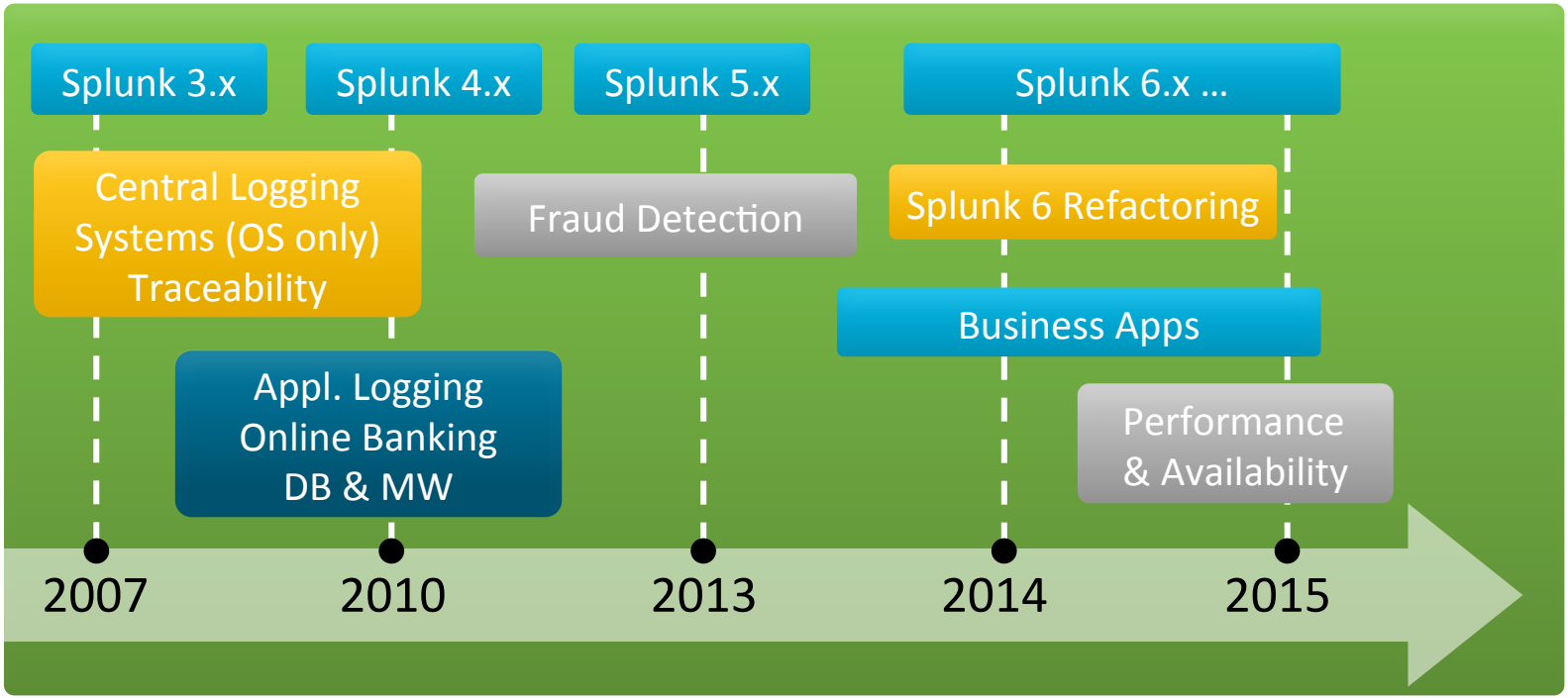
More than 1.6 million customers manage their finances online.



Splunk @ PostFinance

splunk>

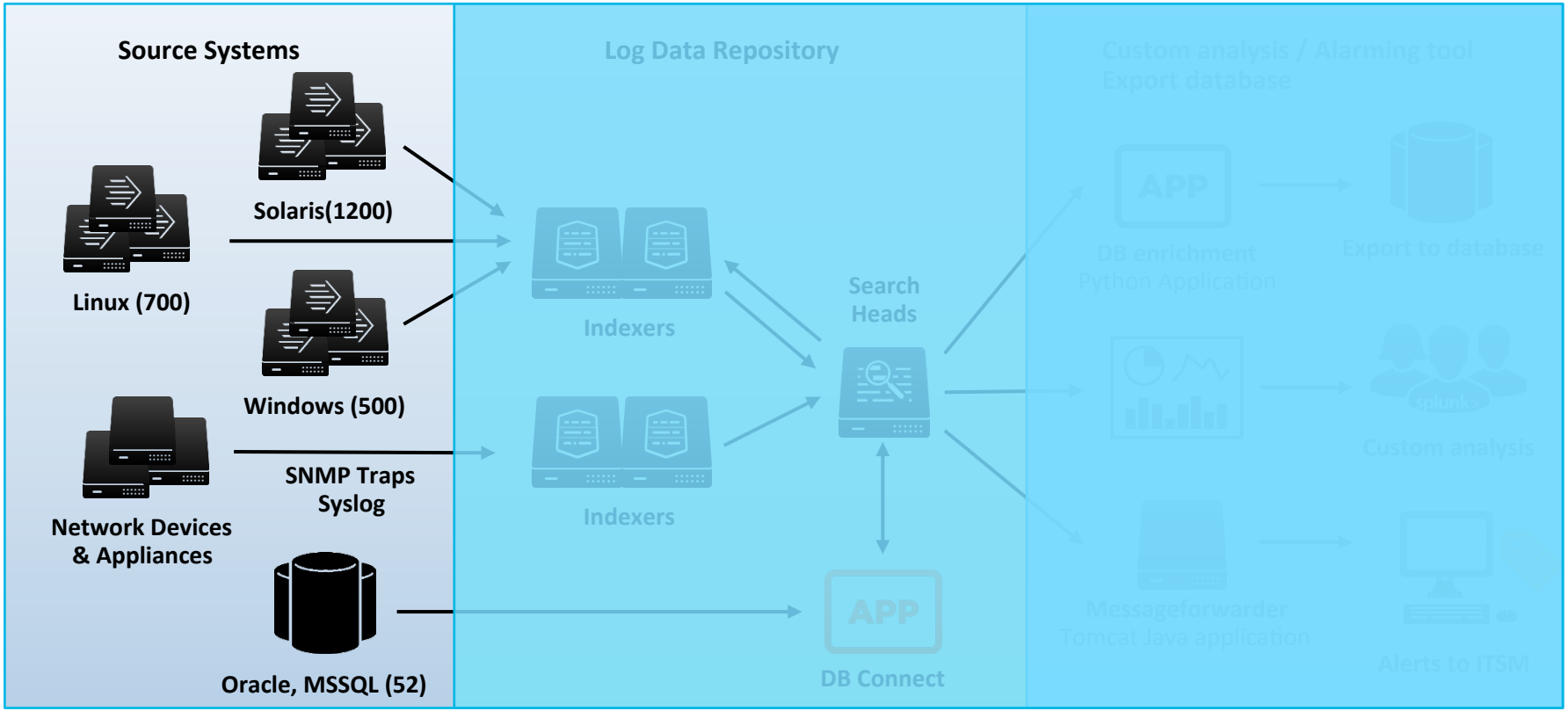
PostFinance's Splunk Timeline



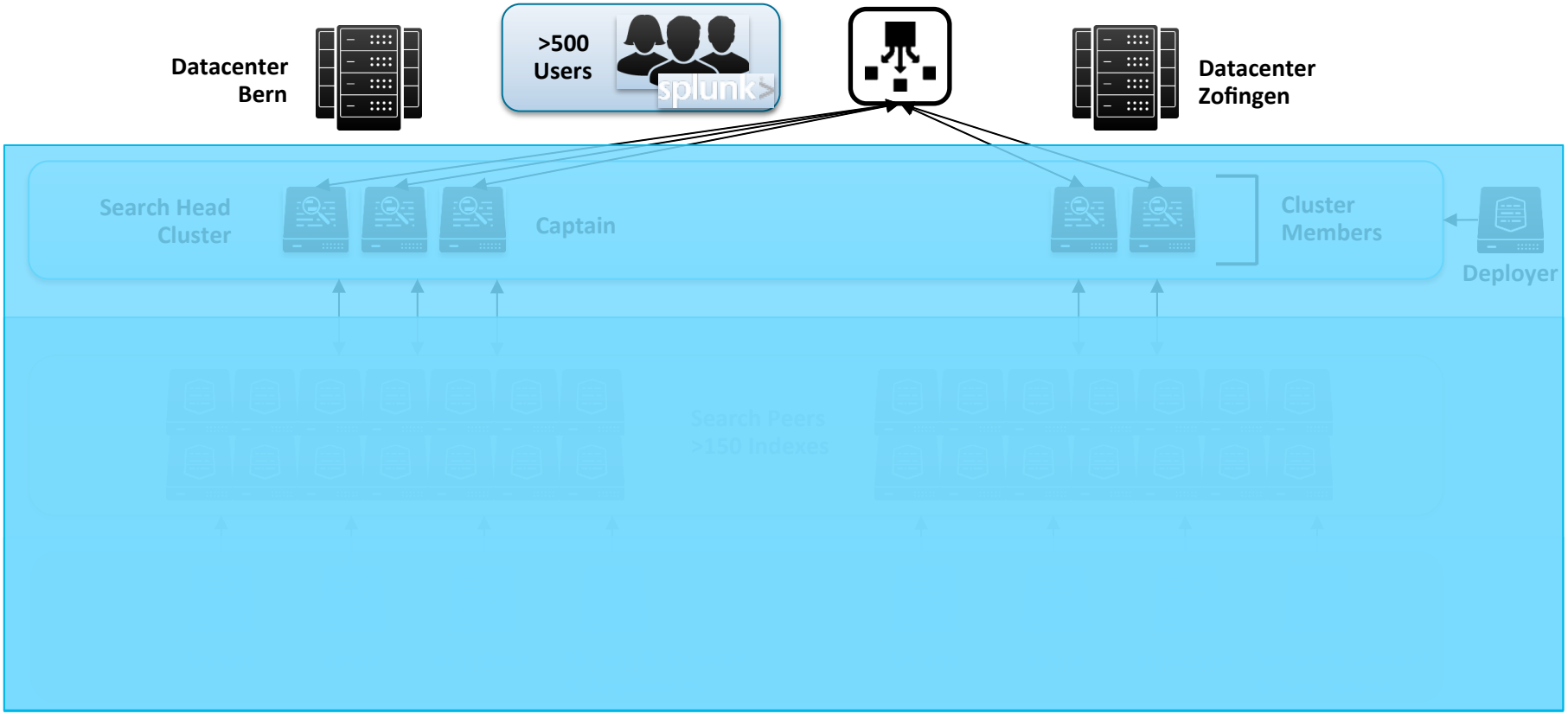
PostFinance's Splunk Numbers

Indexing rate average 434 KB/s		40 Terabytes SAN data (per site)	Number of applications > 30	Number of roles 68
Splunk apps > 55	28 Splunk indexers	Cores 480		800 Searches per minute
Data volume per day 800GB – 1TB		Search head cluster 5 Members 1 Deployer	Memory 2816GB	Source systems > 2360

High Level Architecture



Deployed in Two Datacenters



Use Case 1: Fraud Detection and Report Generation For E-Payment

splunk>

E-Payment - Introduction

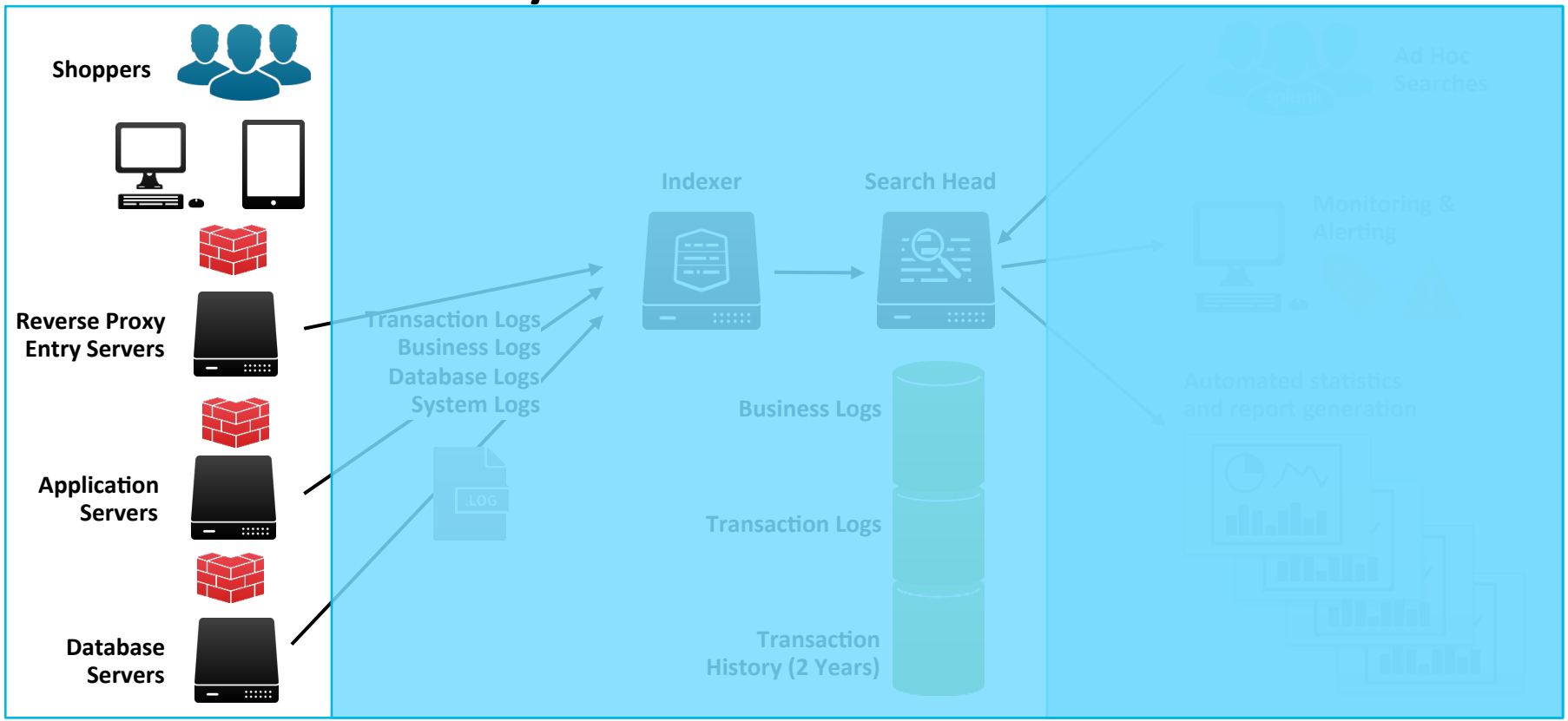
Automated Statistics Generation

for Fraud Detection
and Product Management

E-Payment Platform Info

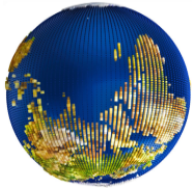
Automated Fraud Detection
General Support Info
Ad Hoc Searches for Support

E-Payment - Architecture



E-Payment - Overview of Splunk Usage

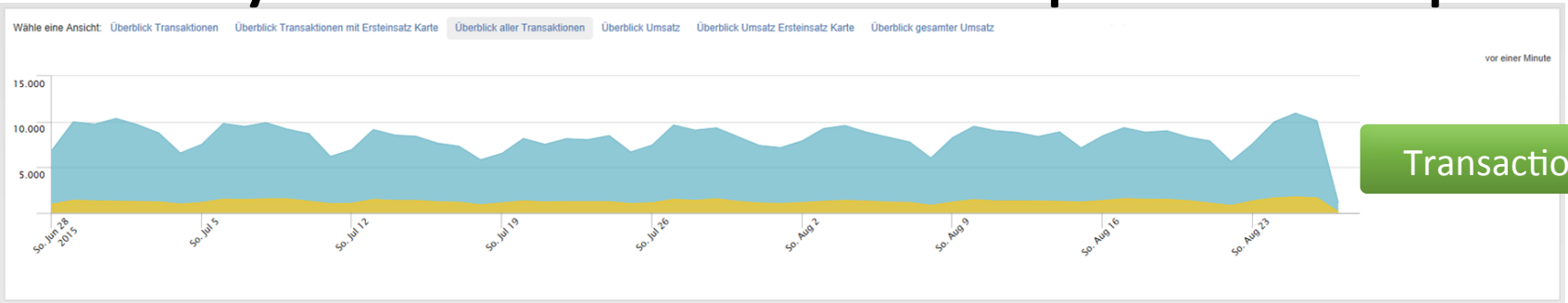
Two main types of Splunk searches:



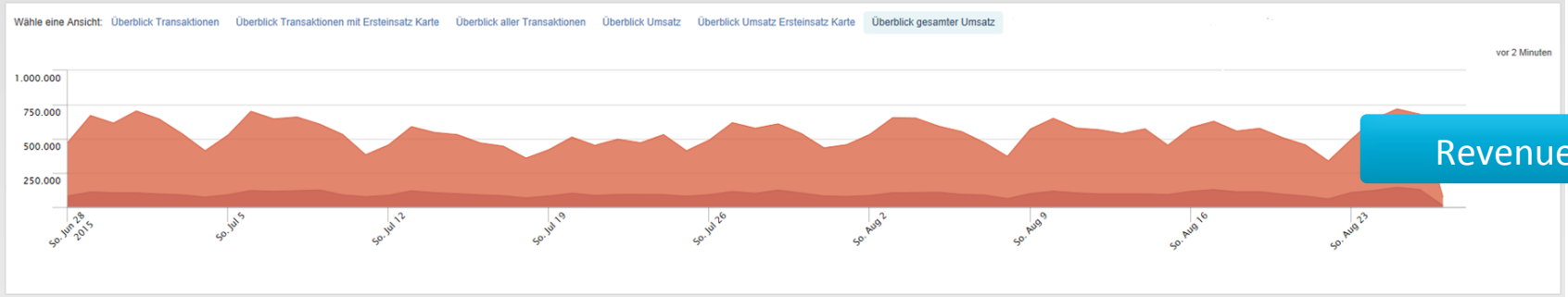
- Examples of global searches:
  - Attempted payments with wrong credentials
  - Payments with same card
  - Number of first time debit card users
  - Transactions close to the card limit

- Examples of merchant report searches:
  - Percentage of new buyers
  - Change of revenue

E-Payment – Merchant Report Example

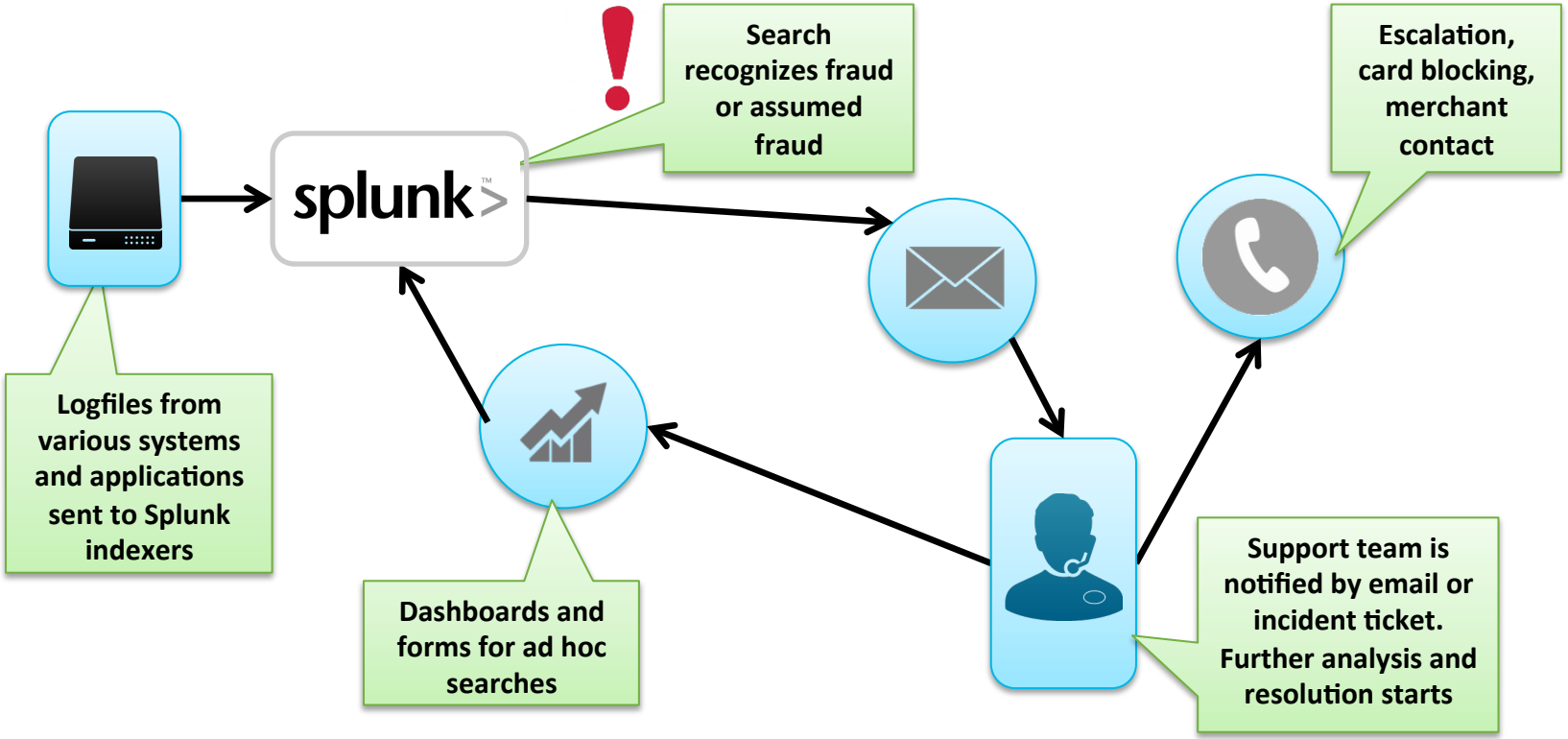


Transactions



Revenue

E-Payment: Fraud Workflow



E-Payment – Performance challenges

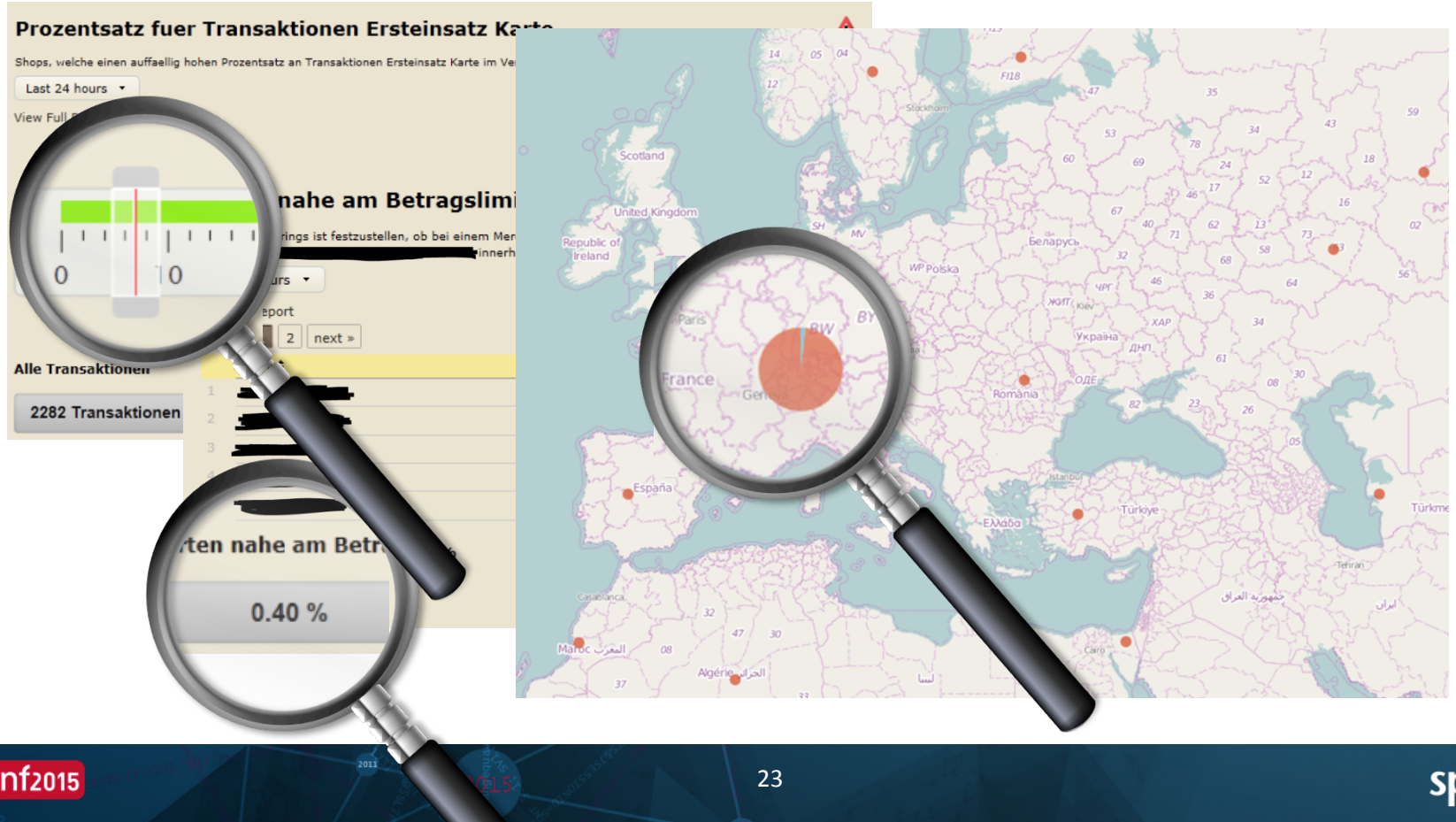
```
index=kgtsprod autoResX="OK" (authTypLiteral=" STRING_2" OR authTypLiteral="STRING_1")|
where trxTypLiteral="PURCHASE" | eval totalBetrag=case(waehrung=="CHF", betrag,
originalWaehrung=="CHF", originalBetrag, waehrung=="EUR" AND originalWaehrung=="EUR",
originalBetrag*$eurokurs$) | sistats sum(totalBetrag) as TxUmsatzTagGesamt, min(totalBetrag) as
TxUmsatzTagMin, max(totalBetrag) as TxUmsatzTagMax, avg(totalBetrag) as TxUmsatzTagAvg by
merchantId, merchantOrt, merchantName, authTypLiteral
```

```
index=sumkg_turnover_merch_24h_prod (authTypLiteral=" STRING_1" OR authTypLiteral="
STRING_2") | dedup authTypLiteral, _time, merchantId | bucket _time span=1d | stats
sum(totalBetrag) as Tagesumsatz by merchantId, _time | join merchantId [search
index=sumkg_turnover_merch_24h_prod (authTypLiteral=" STRING_1" OR authTypLiteral="
STRING_2") startdaysago=30 | dedup authTypLiteral, _time, merchantId | bucket _time span=1d |
stats sum(totalBetrag) as sumTagesumsatz by merchantId, _time | stats avg(sumTagesumsatz) as
Durchschnitt by merchantId] | eval Schwellenwert=round(Durchschnitt*$threshholdmult$) | where
Tagesumsatz > Schwellenwert | where Tagesumsatz>$dailyRevenueLim$
```

E-Payment – Searching for Fraud

```
index=kgtsprod autoResX="OK" (authTypLiteral="STRING_2" OR authTypLiteral="STRING_1|
transaction eComRetrievalNr keepevicted=true | where trxTypLiteral="PURCHASE" | eval
totalBetrag=case(waehrung=="CHF", betrag, originalWaehrung=="CHF", originalBetrag,
waehrung=="EUR" AND originalWaehrung=="EUR", originalBetrag*$eurokurs$) | stats
sum(totalBetrag) as Betrag by merchantId, idNr, limiteVID | where (limiteVID<=$lim$ AND
Betrag>=$amount$) | stats count as KAnzAuffaellig by merchantId | join merchantId [search
index=kgtsprod autoResX="OK" (authTypLiteral="STRING_2" OR authTypLiteral="STRING_1|
transaction eComRetrievalNr keepevicted=true | where trxTypLiteral="PURCHASE" | stats count as
KAnzGesamt by merchantId] | eval PzeAuffaellig=KAnzAuffaellig*100/KAnzGesamt | join merchantId
[search index=kgtsprod (authTypLiteral="STRING_1" OR authTypLiteral="STRING_2") | transaction
eComRetrievalNr keepevicted=true | where trxTypLiteral="PURCHASE" | where (authResX="NOK"
AND authResX="OK") | stats count(sourcetype) as KAnzLimit by merchantId] | eval
PzeLimit=KAnzLimit*100/KAnzGesamt | where (PzeLimit >=$pzelim$ AND PzeAuffaellig
>=$pzeauf$)
```

E-Payment – Dashboard Examples

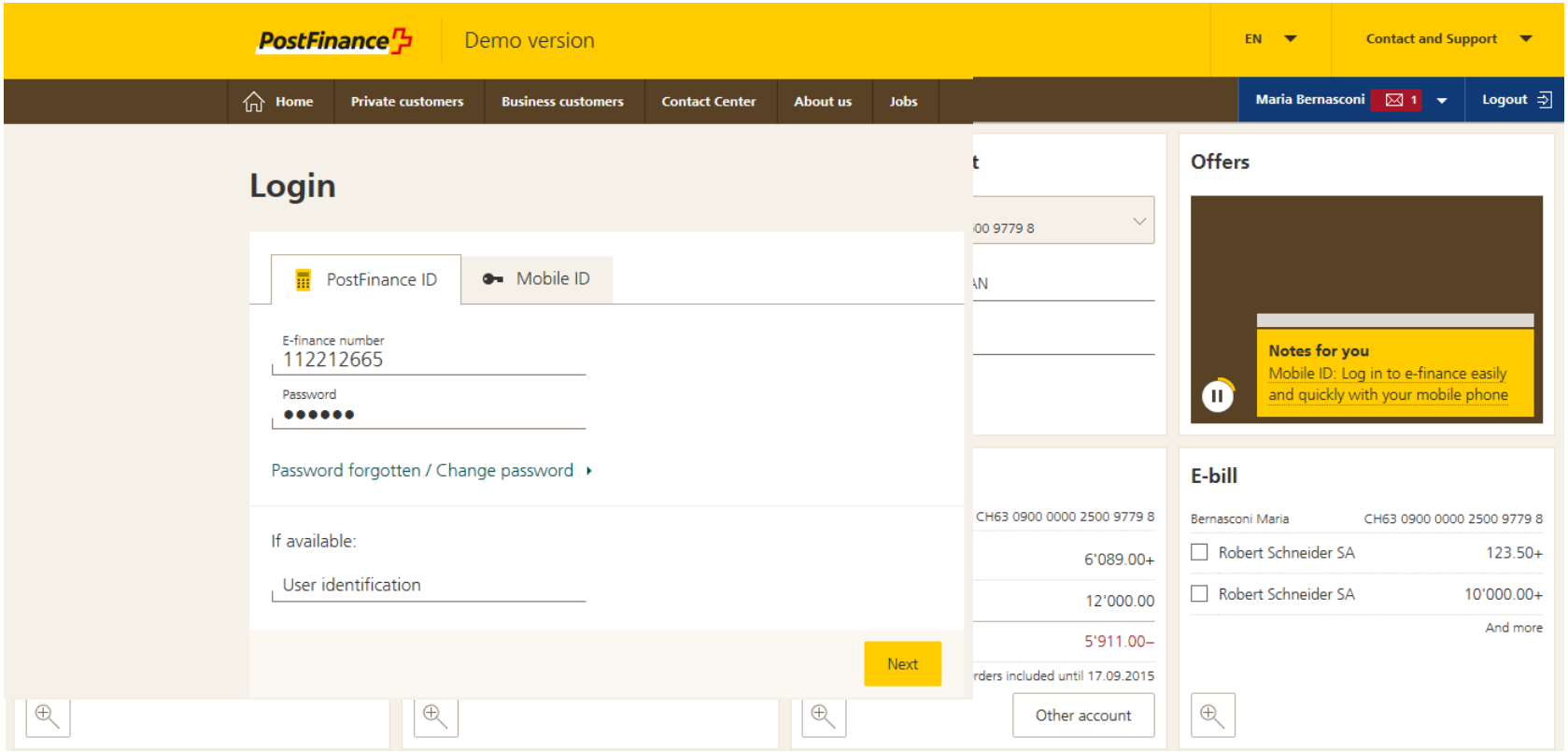


.conf2015

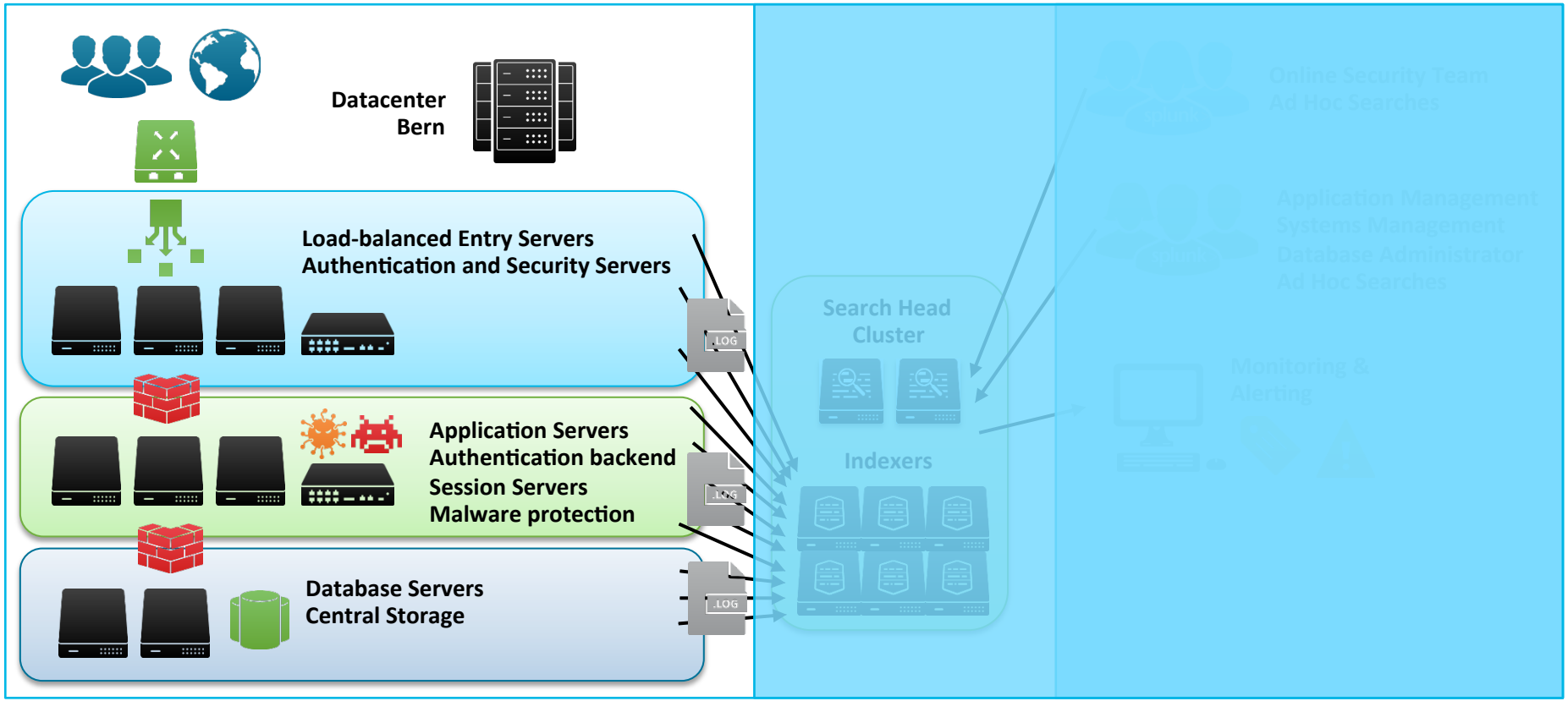
Use Case 2: Online Banking Security and Threat Detection

splunk>

PostFinance – E-Finance Introduction



E-Finance - Architecture



Online Banking - Phishing

Von: "PostFinance" <online.
Betreff: BetreffAW: Sicherl
Datum: 30. Dezember 2014
An: [redacted]

Sehr geehrte Kundin,
Sehr geehrter Kunde,

Wie Sie wissen, ist die Frist z
abgelaufen. Im Rahmen dess
geändert und Ihr Zugang hat
Zugangen manche der neuen
Diese Fehler können manuell
schon alle neuen Features de
klicken Sie bitte untenstehen

Klicken Sie hier ->

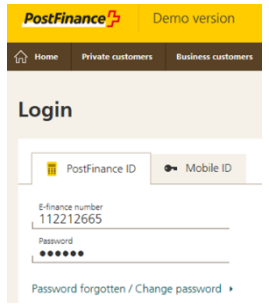
Nach Ausfüllen des Formulars
Finance -Abteilung generiert,
einem/einer unserer Mitarbeit
Fehler zu beheben. Bitte führ
um Ihr E-Finance auch weiter

Wir danken Ihnen für Ihre Zu

E-Finance - Phishing Attack Workflow

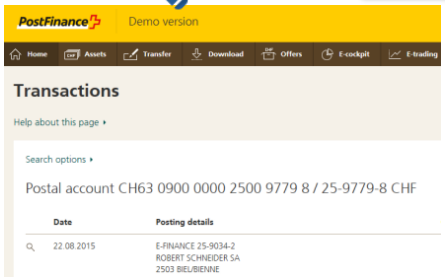
The online security team is notified about a new phishing attack by email

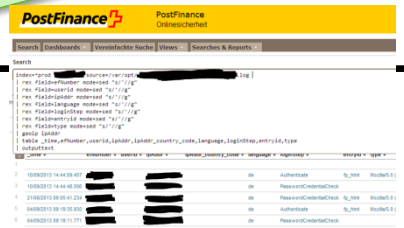
Security team analyzes the new attack patterns



All transactions are rated using CEP rules

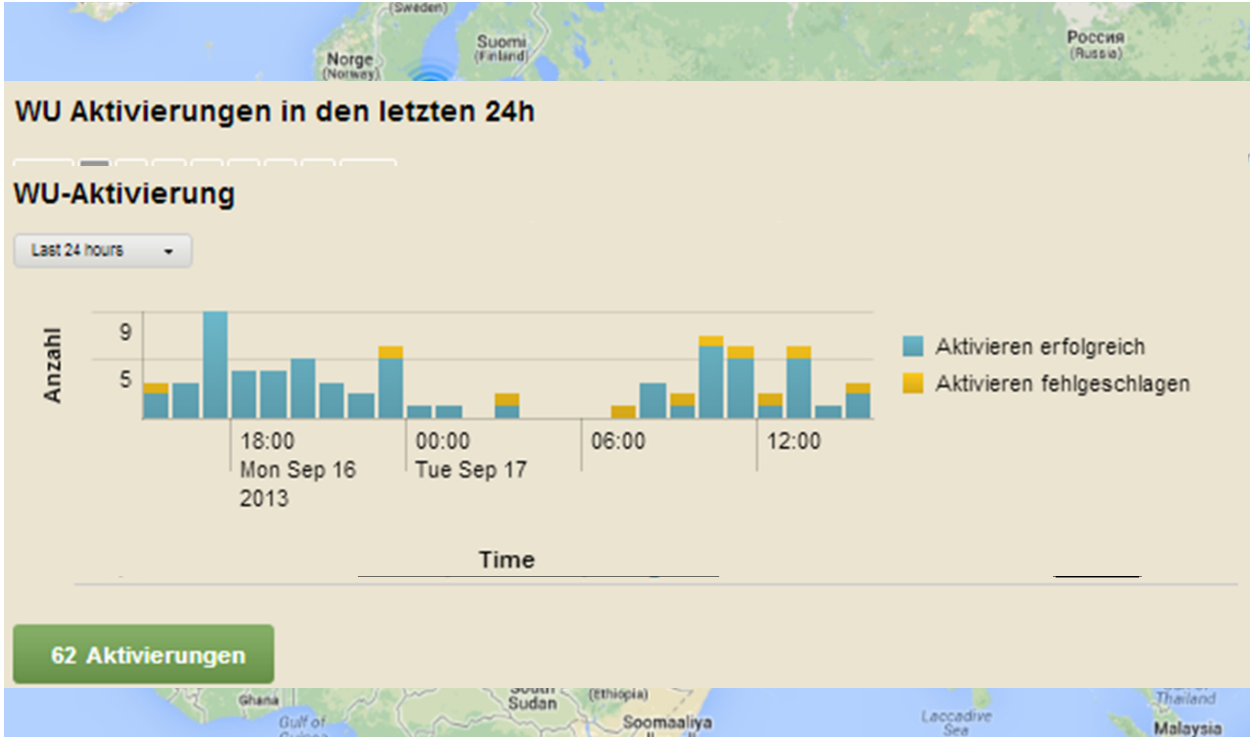
Operationalize the findings for use in daily business



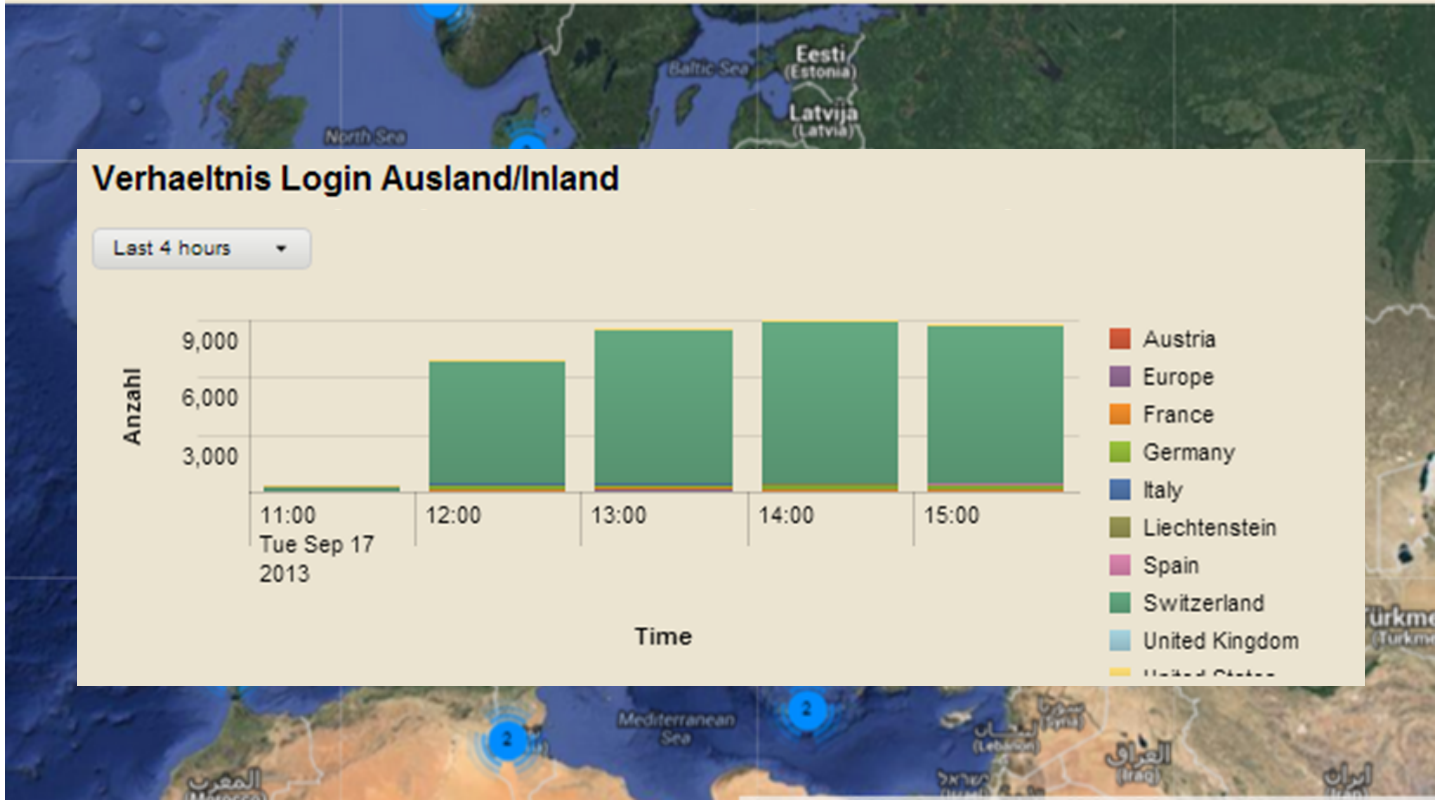


splunk>

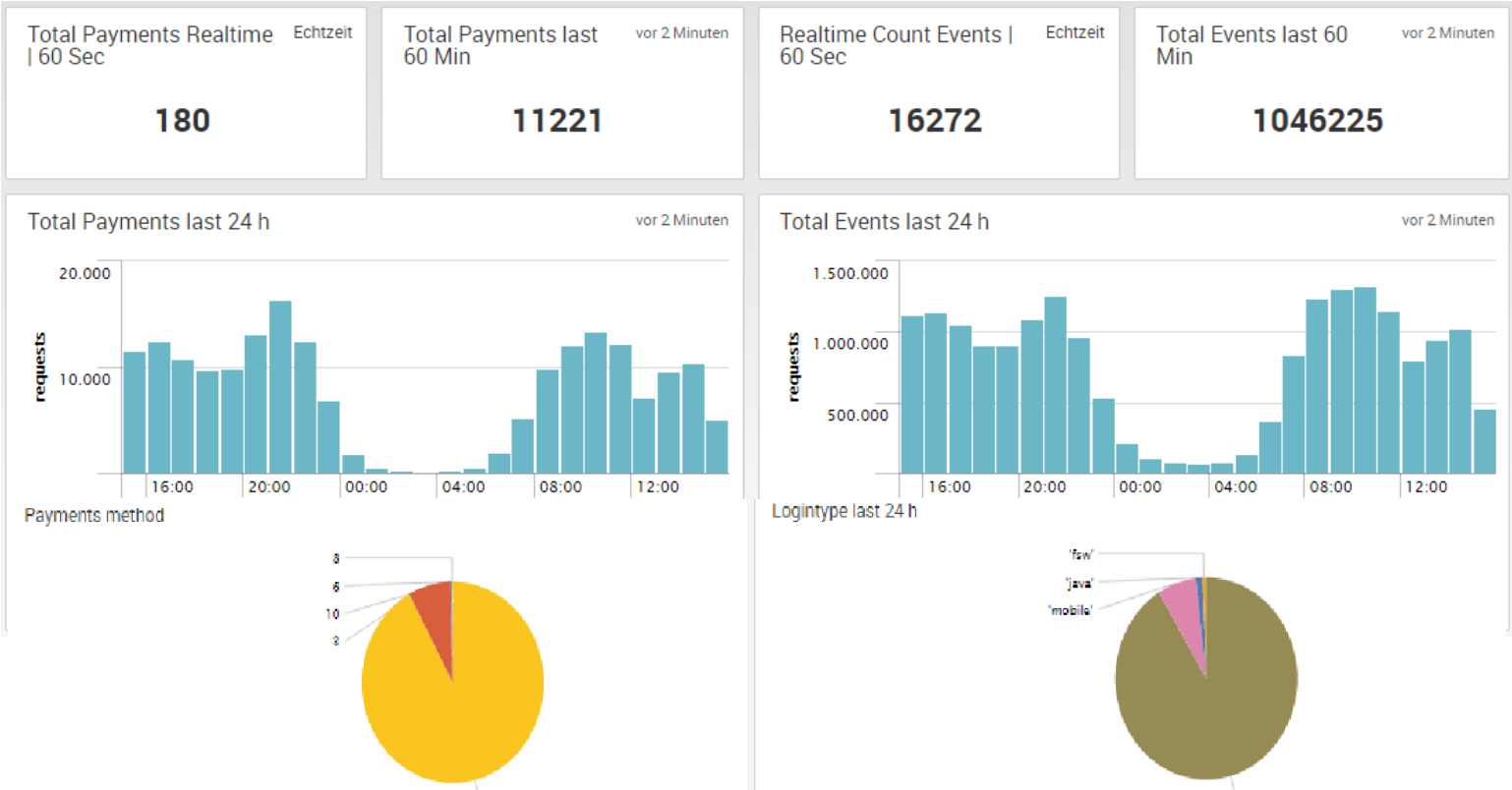
Online Banking Security – Western Union



Online Banking Security – Login Behavior



Online Banking Security – OI



Wrap-Up

splunk>

Wrap-Up: Success Factors

- Start small, think big
- Dedicated «virtual» team
- Business value always in mind
- Show & tell
- Have security on priority list
- Regulatory tightening
- Management support

THANK YOU

splunk>