.conf2014

YOUR DATA ADVENTURE

How Machine Learning Anomaly Detection + Splunk Enable Faster Application Rollouts

EQUENS
PAYMENT SERVICES FOR EUROPE

Giulio Covassi
Marco Bizzantino @bizzam
@kiratech

Rich Collier @richcollier
@prelert

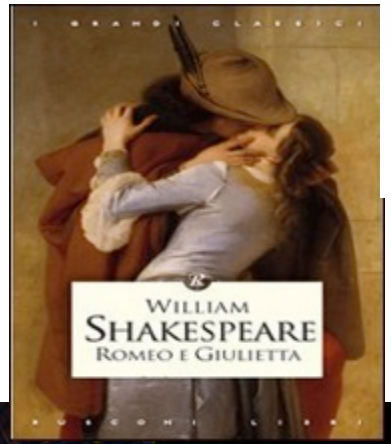
KIRATECH
WE LOVE IT

prelert

splunk>

We are from Verona

City of Amarone wine



City of love

What we do!

Big Data Analytics

Monitoring
Self-Learning Analytics
Operational Intelligence
Business Insight
Compliance
Troubleshooting
Dynamic Reports

Cloud

Management
Automation & Orchestration
Storage & Data Protection
Application Performance Monitoring
Infrastructure Performance Monitoring
Capacity & Cost Planning
Software Defined Storage
Software Defined Network
Mobile Device Management
WAN Optimization
Distributed wi-fi
Business Continuity

Security

Next Generation Firewall
EndPoint Protection
Anomalies Detection & Predictive analysis
SIEM
Penetration Tests & Vulnerability Assessment
Auditing
Strong Authentication

a BIG data story…

Splunk partner since 2009

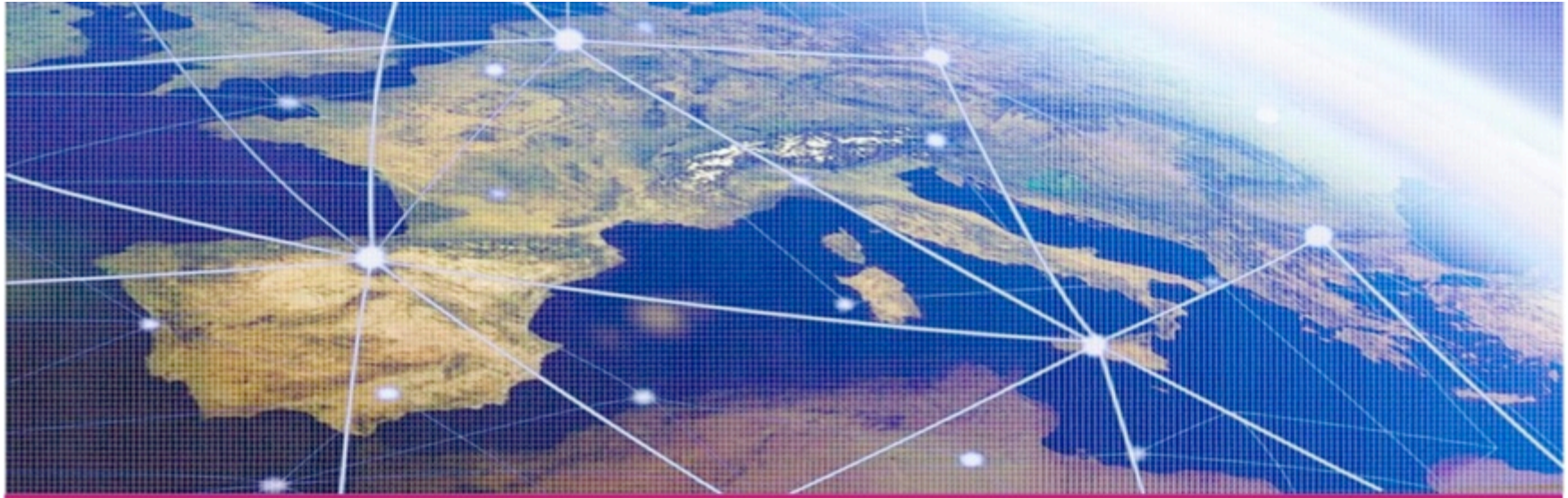
+50 happy customers

prelert®

2013 Partner of the Year
EMEA

Prelert EMEA partner 2013

Top Customers



Introduction to Equens

EQUENS

EQUENS

PAYMENT SERVICES FOR EUROPE

The largest pan-European card & payment processor

Annual figures and medium-term objective

Processing
4.7 billion ➔ at least 5 billion card transactions

10.6 billion ➔ at least 13 billion payment transactions

Market share within Europe
over 12.5% ➔ 17%

Our mission is to achieve the lowest possible processing costs while abiding by the highest standards of quality, reliability and security.

+

splunk>

COA - The monitoring team

- Who are we and what we do
- One year in COA
- Our targets
- The change
- The future … Now!

COA Presentation

Who are we and what we do

Centrale Operativa Allarmi

(Alarm Control Room)

- 20 operators monitor 24/7/365 all EQUENS systems and networks
- Junction point between Customers and Company
- 1st level support and analysis
- Incident coordination
- New monitoring tools development

COA Presentation
Who are we and what we do

- COA is the recipient of all critical notifications from customers and suppliers.
- The alarm management and the direct contact with specialists allow to quickly analyze and solve problems.

COA Presentation
Who are we and what we do

- First analysis
- Engagement of specialists
- Solution
- Problem Management
- During non-office hours COA covers the Incident Manager role

COA Presentation
One year in COA

> 40 000

- Non stop working hours

30

- Constantly checked monitors

> 25 000

- Managed E-Mail

5

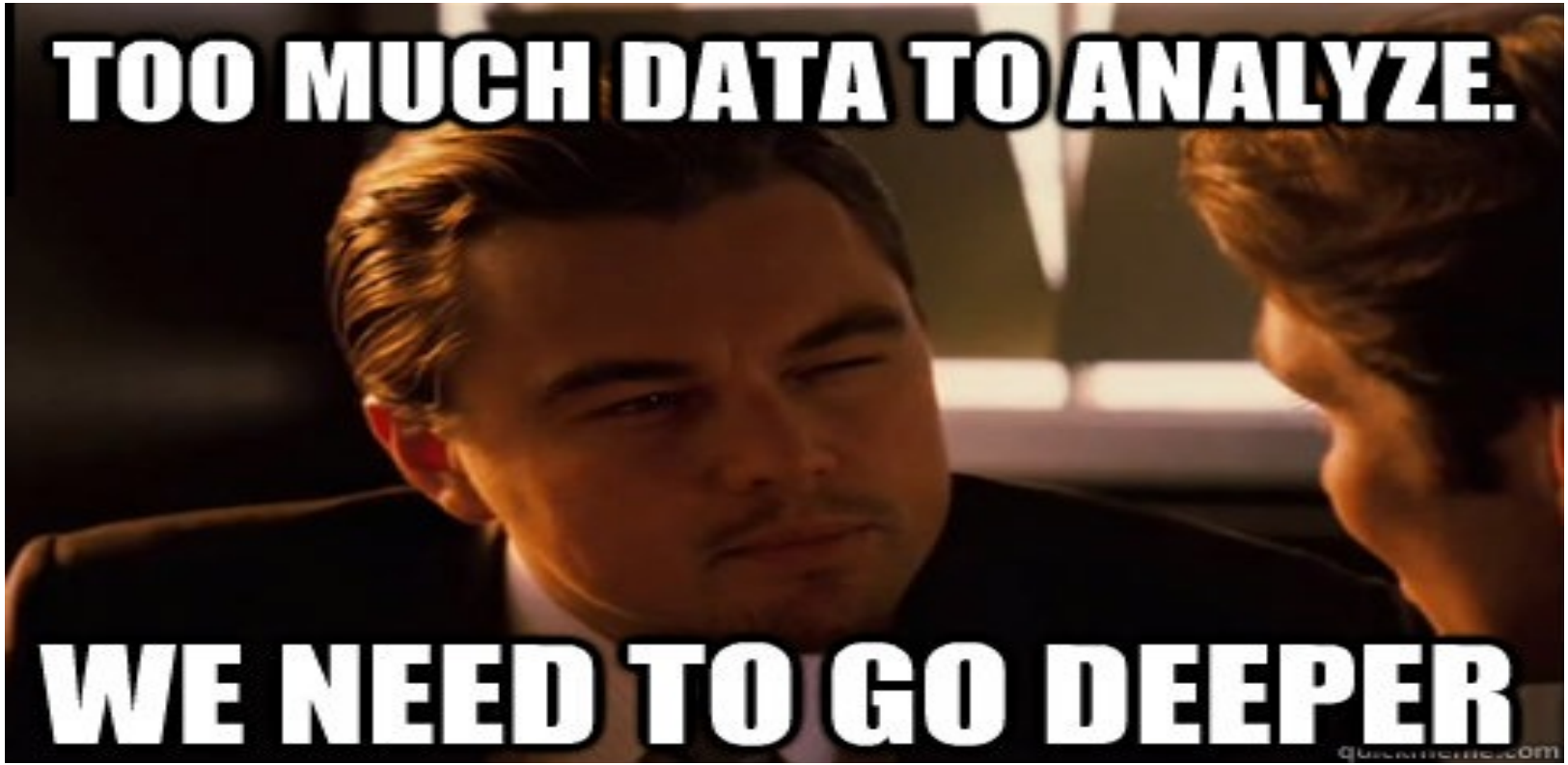
- minutes to make the first level analysis

COA Presentation
Our targets

- Incidents reduction through proactive checks
- Response time reduction
- Quality of service improvement
- Easier and quicker tools to analyze data

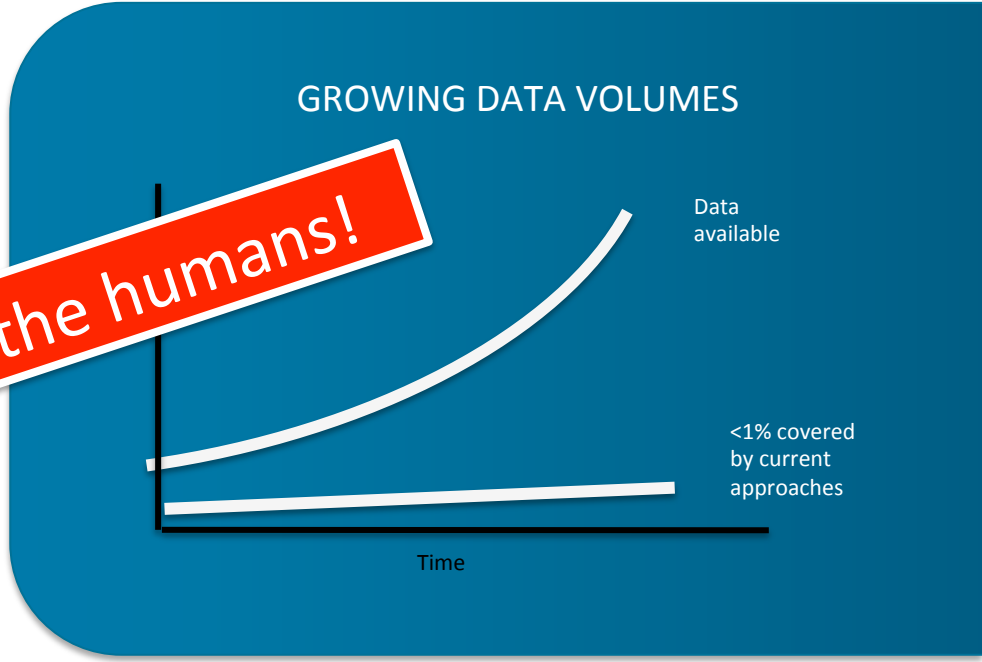
COA Presentation
The change

- New conception of monitoring
- Graphical representation of transactions flow
- Easy implementation and integration with existing tools
- Real-time analysis
- Fast root cause discovering
- Quick and easy reports creation

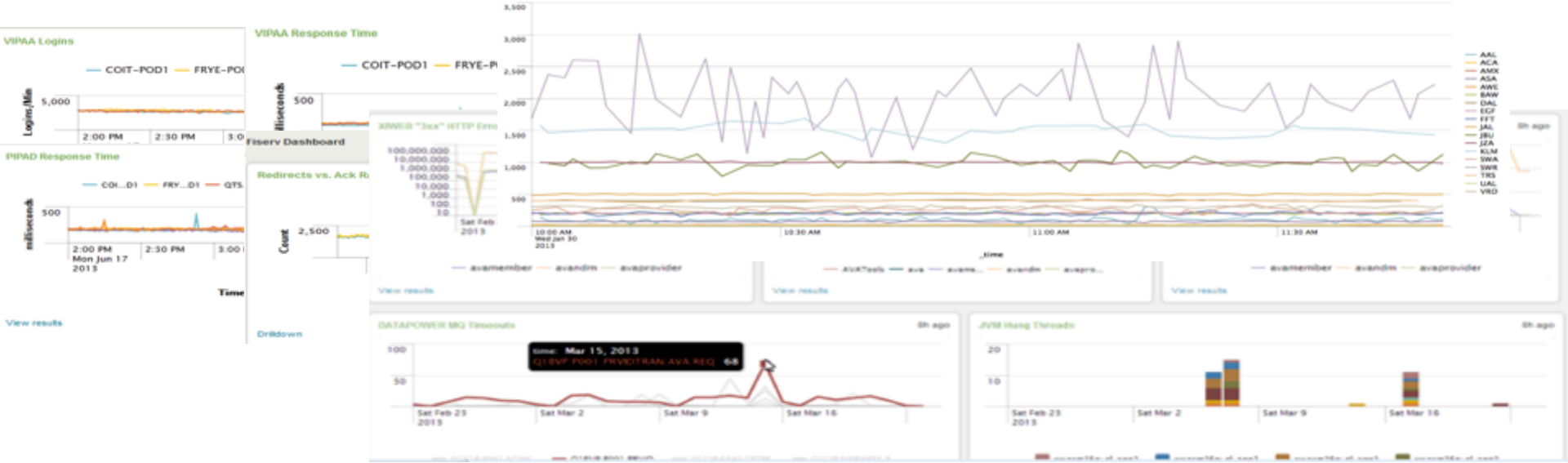

TOO MUCH DATA TO ANALYZE.
WE NEED TO GO DEEPER

Data Volumes Far Exceed Current Approaches

- Dashboards & alerts via rules & signatures
  - Difficult to implemented broadly
  - Lots of false positives
- Manual Search
  - Dependent on expertise, effort, & luck (known bad)
  - Highly unpredictable results

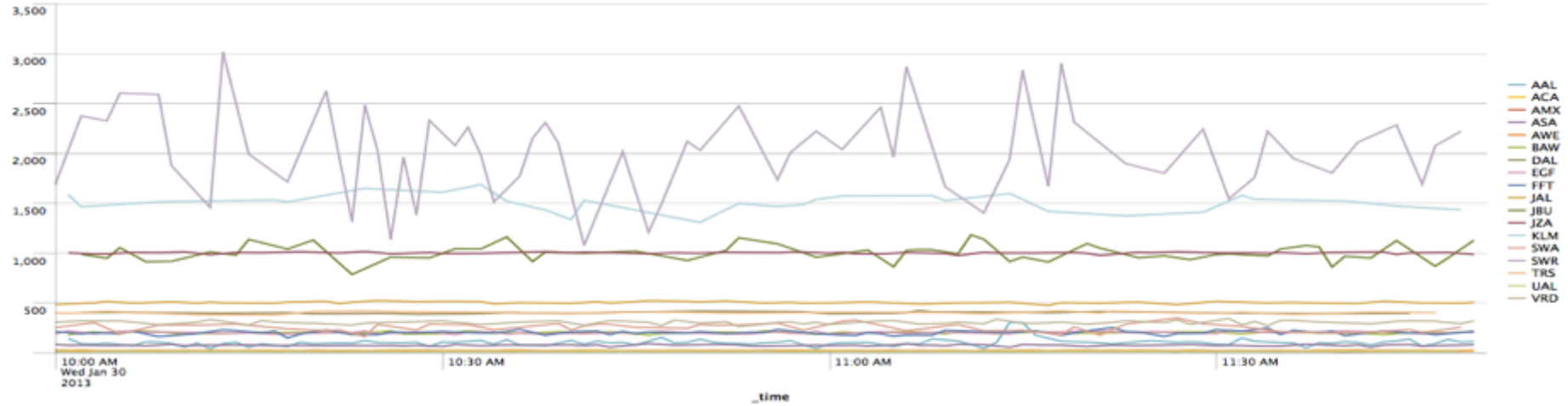


Blame the humans?



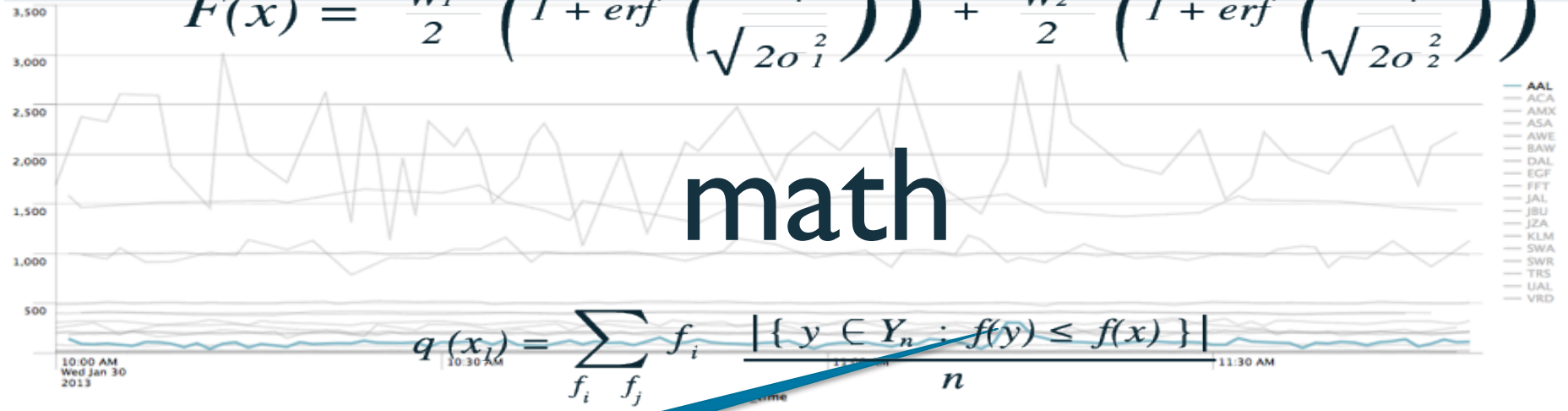
math + data =

What's Interesting Here?



Only That Which is Unexpected!

$$F(x) = \frac{W_1}{2}\left(1 + erf\left(\frac{x - \mu_1}{\sqrt{2\sigma_1^2}}\right)\right) + \frac{W_2}{2}\left(1 + erf\left(\frac{x - \mu_2}{\sqrt{2\sigma_2^2}}\right)\right)$$

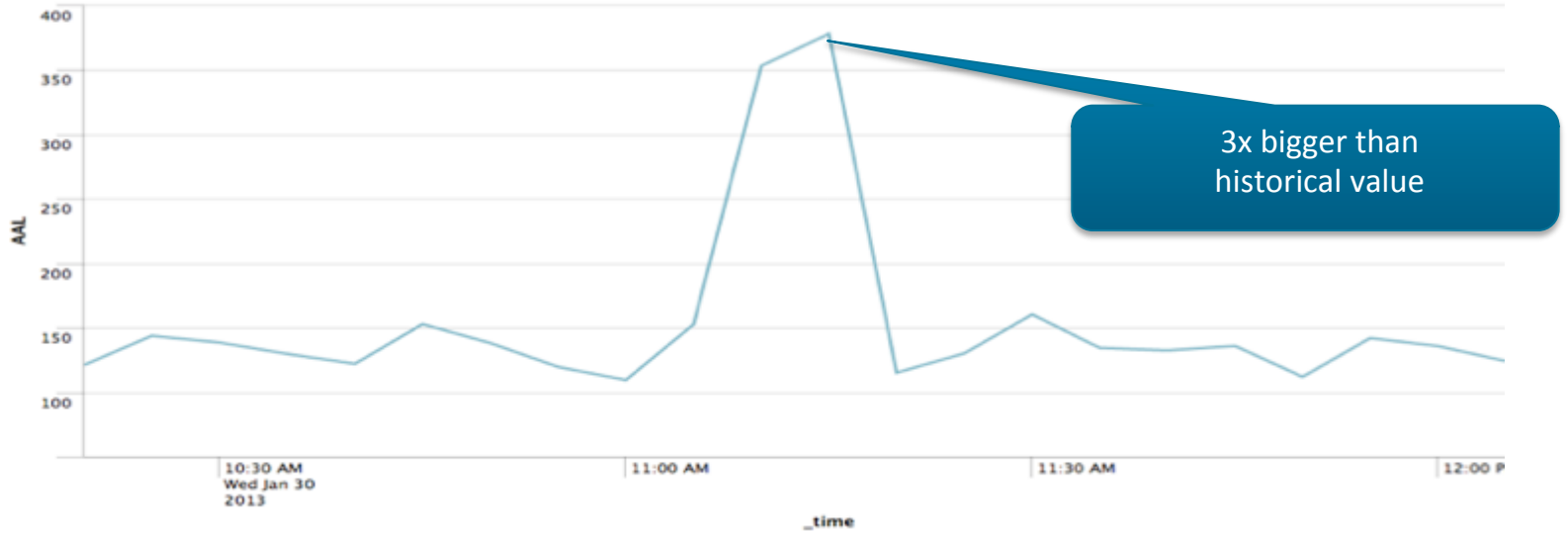


math

$$q(x_i) = \sum_{f_i \quad f_j} f_i \frac{|\{ y \in Y_n : f(y) \leq f(x) \}|}{n}$$

Problem that was lost in the noise

Viewed in Context…



Anomaly Detective®

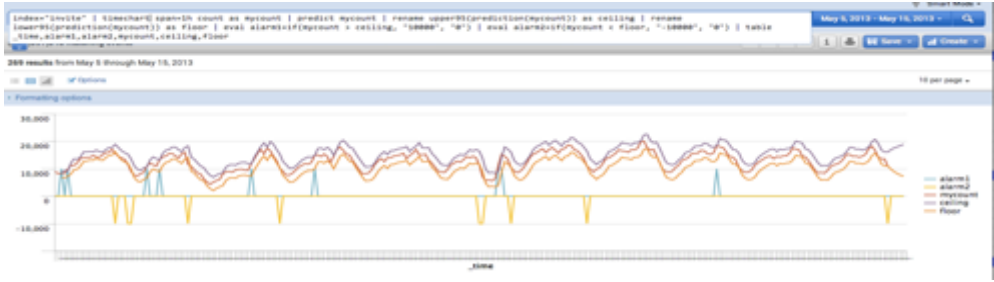
- Anomaly Detection via Machine Learning and Advanced Statistical Algos
- Provides accurate, relevant alerts that IT teams trust
- Slashes troubleshooting & RCA times

Wait…Why Prelert?

- What about core Splunk capability?
- Doesn’t Splunk already have stats/predict/anomalies?
- Aren’t there lots of Splunk “ninjas” out there?

prelert®

- More sophisticated statistical modeling
- Massively scalable parallel detection
- Automatic “Real-Time”
- Easier to Use



COA Presentation
The future ... Now!

- Predictive analysis
- Proactive intervention on possible incidents
- Deepest real-time analysis
- Automatic problem detection
- Quick comparative analysis

splunk> + prelert

Some real use cases

"Using Splunk we strongly reduce Time To Monitor
Card Processing services, without any application changes.

Adding Prelert now we can find anomalies in historical trends
and in realtime in core business application and
unstructured data become easy to investigate and categorise.

Our Business Monitoring now sends only real alerts."

Viste Esci MONITOR

Key Client Customer Service

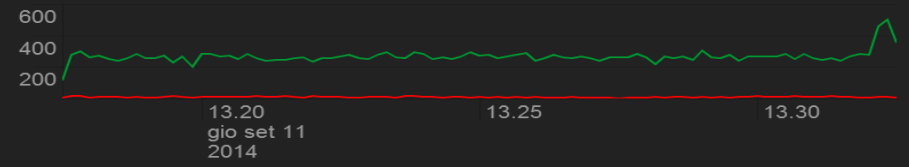
POS Transactions (Last 15min)

OK 24324 KO 883

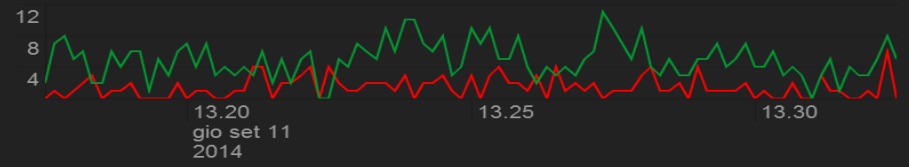
ATM Transactions (Last 15min)

OK 447 KO 129

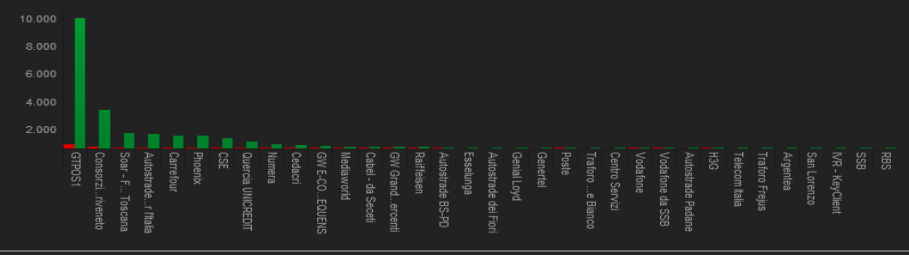
POS transactions progress (last 15min)



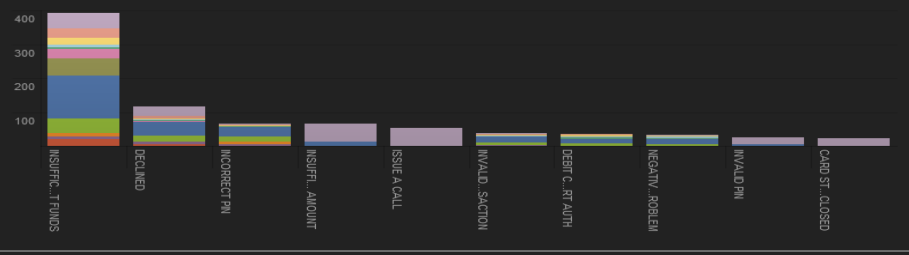
ATM transactions progress (last 15min)



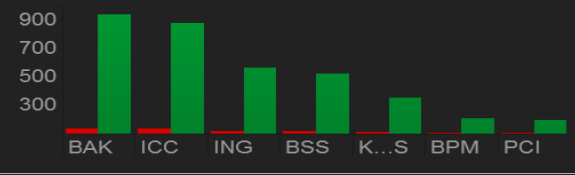
Transactions by GT_CODE - Last 15min



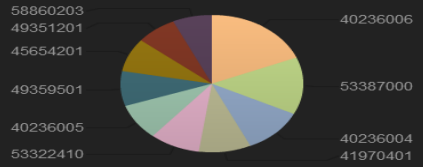
Transactions by GT_CODE - Last 15min



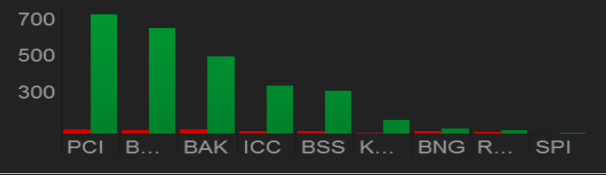
ISSUING VISA (Last 15min)



TOP 10 BINs with denials in last 15min



ISSUING MASTERCARD (Last 15min)



QMB Plus

Modifica

Ultimo Evento

in tempo reale

2014-09-11 14:09:02

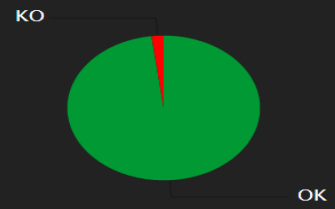
Criticità (KO >30%)

in tempo reale

In attesa di dati...

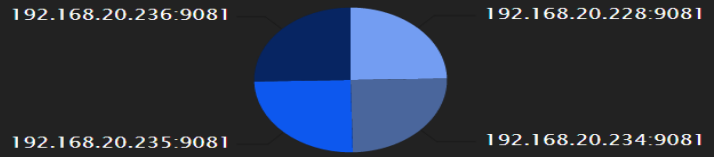
% ATM OK / KO

in tempo reale



Distribuzione carico dei cloni

in tempo reale



ATM principali

in tempo reale

BANCA	TOT ATM	KO	%KO
BANCA POPOLARE DI MILANO	919	57	**6.20**
CASSA DI RISPARMIO DI FANO	51	2	**3.92**
CASSA DI RISPARMIO DI ORVIETO	55	2	**3.64**
CREDITO SICILIANO S.P.A.	165	3	1.82
Banca Popolare di Bari	208	3	1.44
BPER BANCA POPOLARE DELL'EMILIA ROMAGNA	598	8	1.34
Banca Sella	298	4	1.34
UBI - BANCA CARIME SPA	309	4	1.29
UBI - BANCA POP.COMMERCIO E INDUSTRIA	286	3	1.05
UBI - BANCA REGIONALE EUROPEA SPA	307	3	0.98

ATM Principali

in tempo reale

100
90
80
70
60
50
40
30
20
10

splunk> App: International Routing

Administrator | Messaggi | Impostazioni | Attività | Guida

Smart Search

International Routing

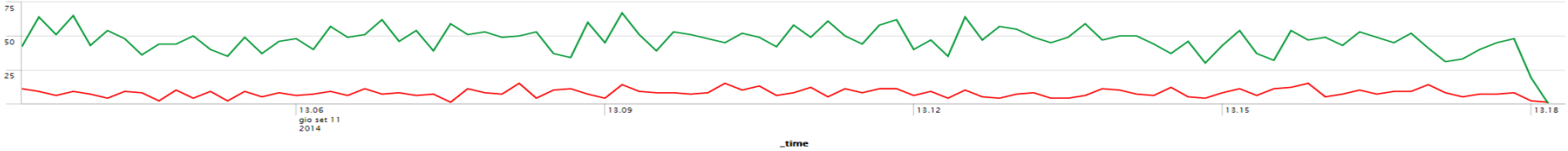
RI Smart Search

Modifica | Altre info

Transaction type: Any | Response: Any | HPNS system: Any | FIID_C: Any | FIID_T: Any | other search: * | Ultimi 15 minuti | Invia

Transactions in time

secondi fa



Totals by OK / KO

secondi fa

OK **4230**

secondi fa

KO **705**

secondi fa

%KO **14.29**

Totals by type

secondi fa

POS **3242**

secondi fa

ATM **1693**

Raw data

secondi fa

_time	HPNS	LN	TYP_REC	FIID_C	FIID_T	TYP_MSG	DRAFT_CPT	POS_EM	TRX_CODE	AUTH	ESITO	Description	TERMID	RETAILER	AMOUNT	VALUTA	TERM_STAT	VALUTA_ORIG	MCC	GT_CODE	ECOM
2014-09-11 13:18:06	BOSON	SWCH	P	SECE	BNET	210	0	51	100000	7	0	APPROVED WITH BALANCES	00670680	0001910363	18510	978		0	7011	00000	
2014-09-11 13:18:06	BOSON	SWCH	P	SECE	BNET	210	0	51	100310	7	0	APPROVED WITH BALANCES	32782267	371130500001	28532	978		0	7299	00300	
2014-09-11 13:18:05	BOSON	SWCH	P	SECE	BNET	210	0	51	100000	7	0	APPROVED WITH BALANCES	30172728	301002401359	8325	978		0	5411	00000	
2014-09-11 13:18:05	BOSON	SWCH	P	SECE	BNET	210	0	12	130000	7	0	APPROVED WITH BALANCES	00000001	000980200090994	1000	978		0	4814	00000	7
2014-09-11 13:18:04	BOSON	SWCH	P	SECE	VISA	210	0	10	100000	7	0	APPROVED WITH BALANCES	00000001	000980020221993	150	978		978	8999		7
2014-09-11 13:18:04	BOSON	SWCH	P	SECE	VISA	210	0	10	100000	7	0	APPROVED WITH BALANCES	190099000156182	190099000156182	598	978		978	5969	330	7
2014-09-11 13:18:04	QUARK	SWCH	P	SECE	BNET	210	0	51	100000	7	0	APPROVED WITH BALANCES	30392267	300142377	2200	978		0	5651	00000	
2014-09-11 13:18:04	QUARK	SWCH	A	SECE	BNET	210			100000	7	000	APPROVED WITH BALANCES	6729624		20000	978		0		01000	
2014-09-11 13:17:04	QUARK	EPY	A	BNET	SECE	210			100000	7	001	APPROVED;	55847362		10000	978		0			

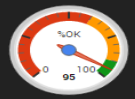
splunk> App: TMC

Administrator Messages Settings Activity Help

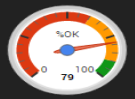
TMC Base24 v1.5

Today is 11/9/2014 13:46:54

KCCS Totals by Day



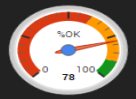
637.470 trx.
POS transactions so far today
▲454.707 (71,3%) above last Thursday



15.854 trx.
ATM transactions so far today
▲9.428 (59,4%) above last Thursday

BANCA SELLA Totals by Day

227.958 trx.
POS transactions so far today
▲169.629 (74,4%) above last Thursday



7.479 trx.
ATM transactions so far today
▲4.883 (65,2%) above last Thursday

GT-POS Totals by Day

1.144.405 trx.
GT-POS transactions so far today
▲897.470 (78,4%) above last Thursday

INTL. ROUTING Totals by Day

77.611 trx.
POS transactions so far today
▲53.279 (68,6%) above last Thursday

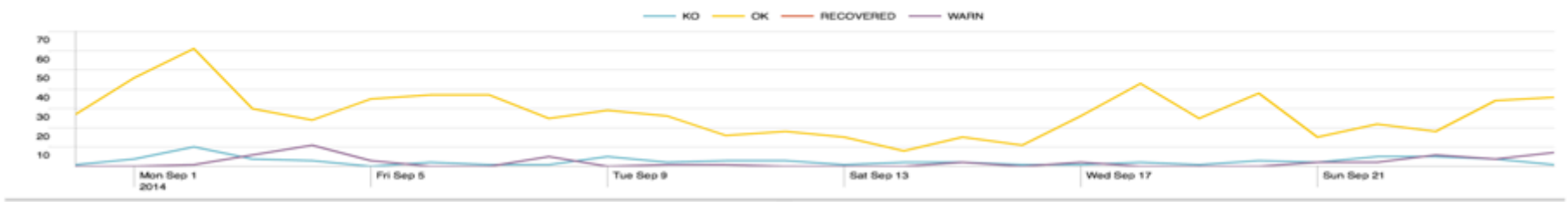
44.284 trx.
ATM transactions so far today
▲29.007 (65,5%) above last Thursday

Grand Total

▼Total trx. today: **2.155.061**
-1.618.403 (75,0%) less than last Thursday

Total mln.Euros moved today: **10.208,811**
GT-POS data not available

Timechart data



Anomalies by relative severity - Click for details

Anomalies by relative severity - Click for details

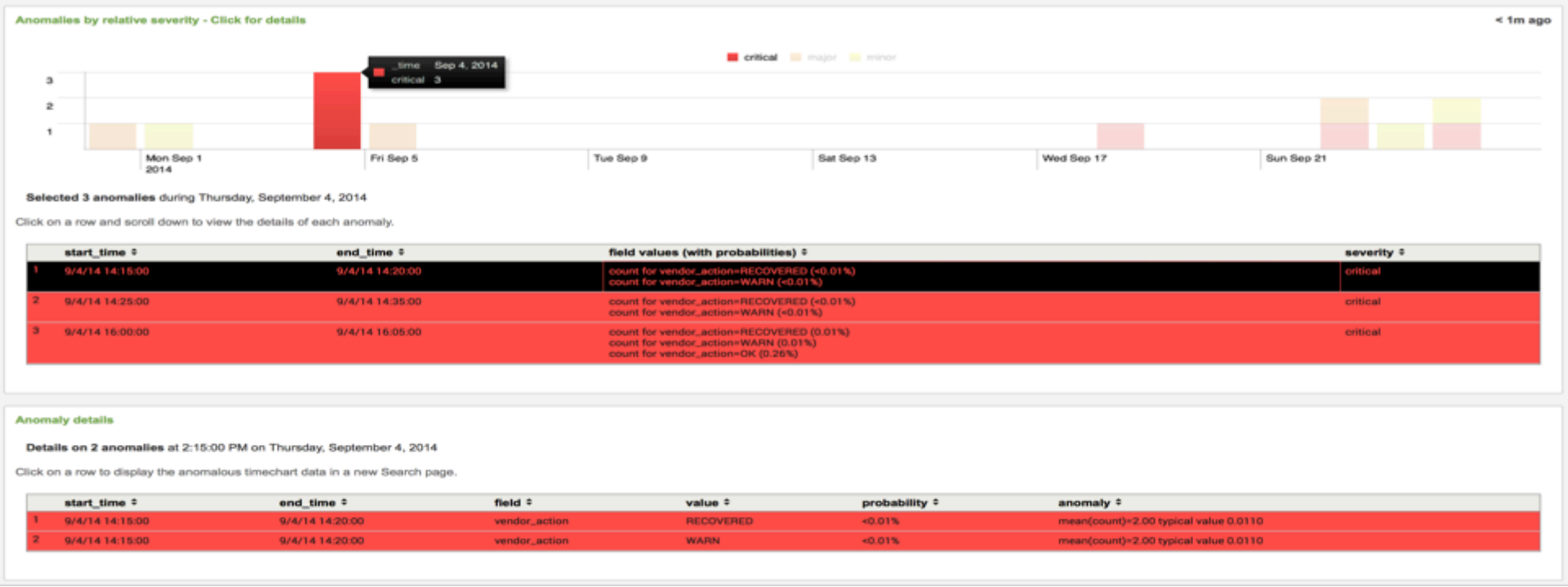
< 1m ago

Selected 3 anomalies during Thursday, September 4, 2014

Click on a row and scroll down to view the details of each anomaly.

	start_time	end_time	field values (with probabilities)	severity
1	9/4/14 14:15:00	9/4/14 14:20:00	count for vendor_action=RECOVERED (<0.01%) count for vendor_action=WARN (<0.01%)	critical
2	9/4/14 14:25:00	9/4/14 14:35:00	count for vendor_action=RECOVERED (<0.01%) count for vendor_action=WARN (<0.01%)	critical
3	9/4/14 16:00:00	9/4/14 16:05:00	count for vendor_action=RECOVERED (0.01%) count for vendor_action=WARN (0.01%) count for vendor_action=OK (0.26%)	critical

In just 3 steps we found the root cause of an hidden anomaly in our trends data



Conclusion

- Automatic Anomaly Detection is key to making alerts easy and accurate
- Equens wants to focus on delivering best service to customers
- Leave advanced anomaly detection to the experts
- Splunk + Prelert = makes Equens superhuman!

Come to the Prelert booth for more information

Download free trial from Splunkbase or prelert.com

Questions?