Building an Enterprise-grade Security Intelligence Platform at Yoox.com

(Gain the Big Picture)

Gianluca Gaias

Head of Information Security,
YOOX Group

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.

Personal Introduction

- Gianluca Gaias, YOOX Group
- YOOX Group is the global Internet retailing partner for leading fashion and luxury brands
- Head of Information Security:
  - Application Security
  - Organizational Security
  - Compliance
  - Security Monitoring

Key Takeaways

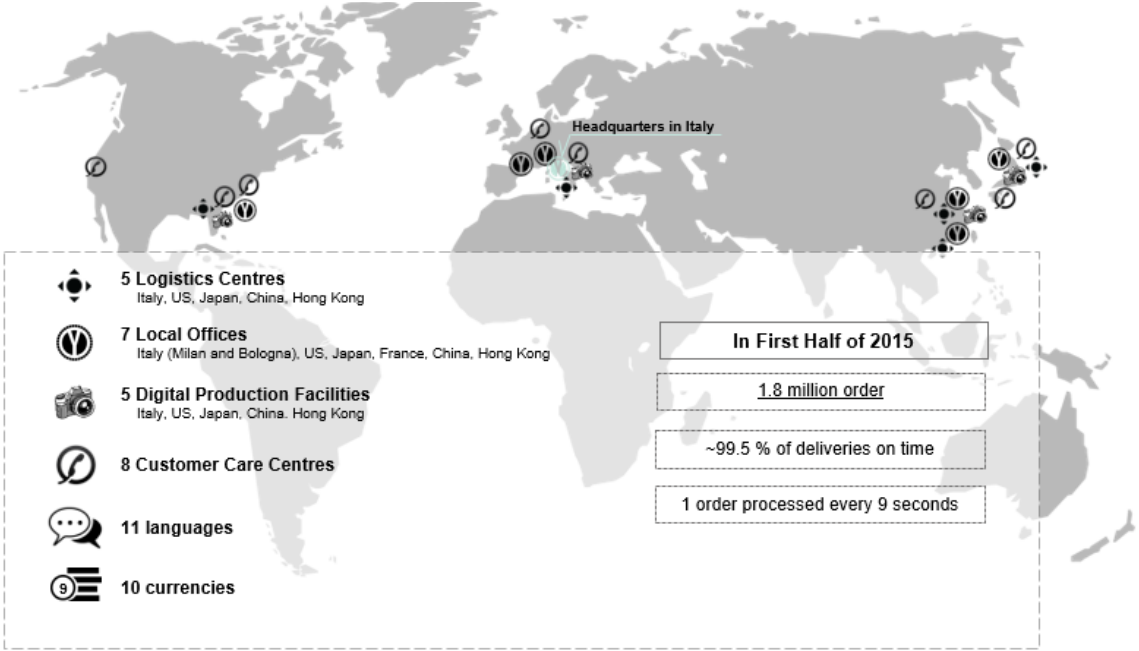
- From a ***technology oriented*** approach to an ***info-centric approach***
- From ***log correlation*** to ***pattern recognition***
- From a ***passive/display platform*** to a ***proactive/executive platform***
- From ***standard dashboards*** to ***real-time dynamic dashboards***
- From a ***security event*** to an ***context-aware security information***

Agenda

- YOOX Group: business and challenges.
- Security evolution overview
- From Tech Oriented approach to Information Oriented approach
  - Deep Investigation
  - Proactive Dashboard: IP Blacklist
  - Real-time Dynamic Dashboard: Attack Map
- Risk Management and Pattern Recognition
  - Use Case: Attackers Activity
- Reconsidering dashboard design
- Next Steps

YOOX Group

- Global reach to more than 100 countries worldwide
- Five logistics centers strategically located, guaranteeing top service to all major fashion markets (United States, Europe, Japan, China, Hong Kong)



YOOX Group: OS & Multi-Brand

MULTI-BRAND

YOOX.COM

- The world's leading online lifestyle store for fashion, design and art
- Broad offering of end-of-season premium apparel and accessories, exclusive collections, vintage, home & design and artworks
- Launched in 2000

THECORNER.COM

- The luxury online boutique with in-season assortment of high fashion and directional designers for men and women
- Dedicated mini-stores
- Launched in 2008

SHOESCRIBE.COM

- The online destination for women dedicated entirely to in-season high-end shoes
- Exclusive shoe-related services and innovative editorial component
- Launched in 2012

MONO-BRAND

- Exclusive official online flagship stores of leading fashion and luxury brands
- Long-term partnerships

Online stores "Powered by YOOX Group"

ALEXANDER WANG	.com	JIL SANDER	.com
ARMANI	.com	MISSONI	.com
BRUNELLO CUCINELLI	.com	MONCLER	.com
DOLCE & GABBANA	.com	roberto cavalli	.com
DSQUARED²	.com	VALENTINO	.com
EMILIO PUCCI	.com	Zegna	.com

JVCo with Kering

ALEXANDER MCQUEEN	.com	Brioni	.com
MC	.com	SAINT LAURENT PARIS	.com
BALENCIAGA	.com	sergio rossi	.com
BOTTEGA VENETA	.com	STELLA McCARTNEY	.com

and many more ..

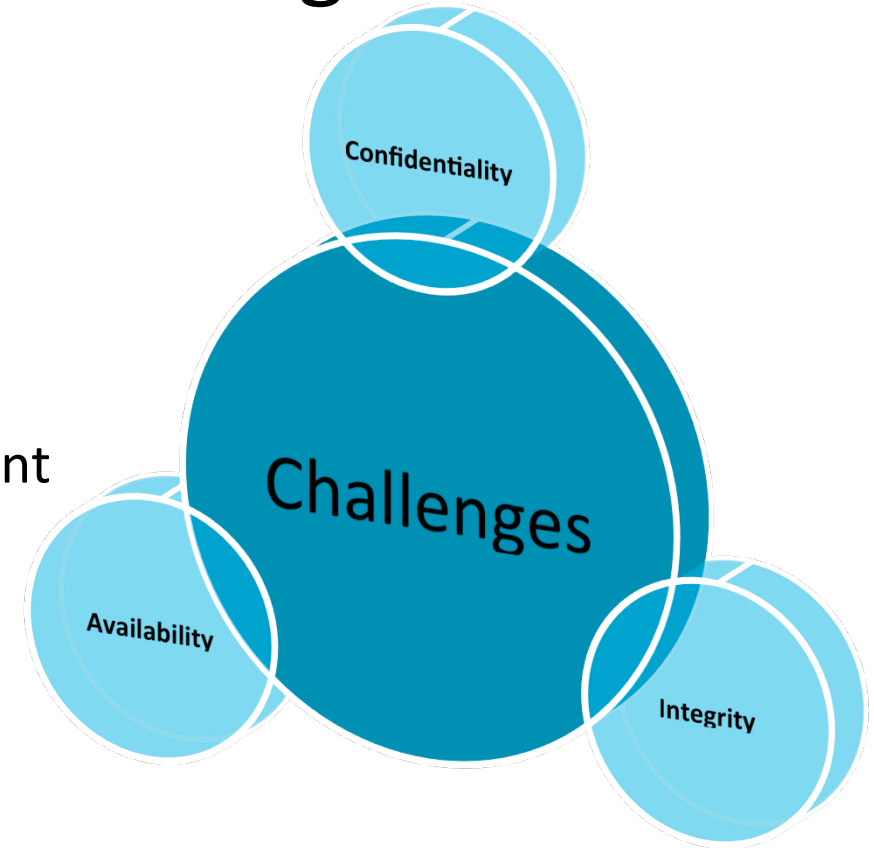
YOOX Group: Challenges

- Keep the trust
  - Data Confidentiality
  - Data Integrity and Completeness
  - Data Processing Transparency

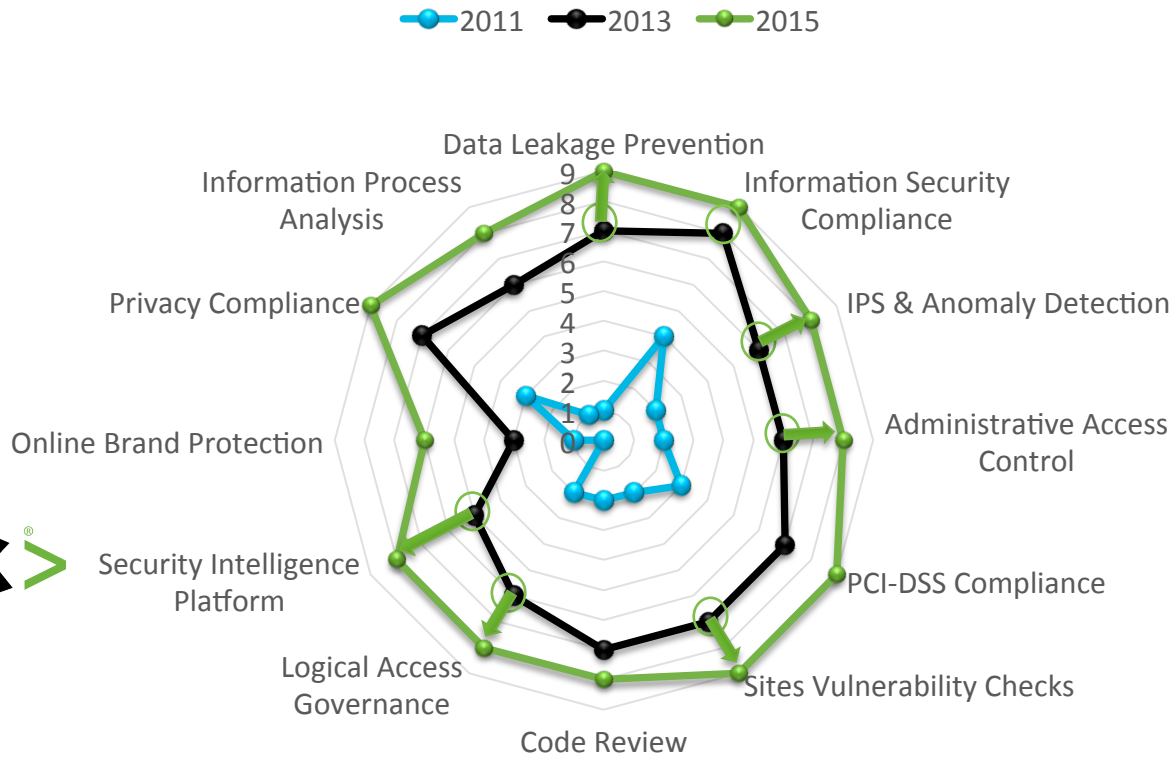
✓ Shareholders
✓ Customers
✓ Stakeholders

- High Availability in hostile enviroment

- Gain the big picture:
  - Challenge and Enabler



Security Evolution Overview

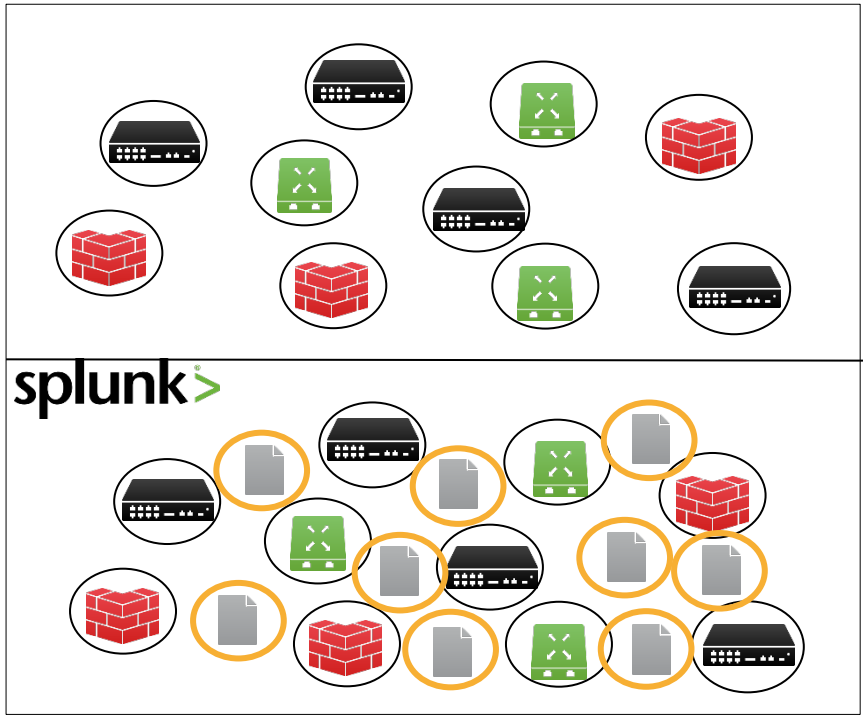


splunk>

Security Evolution – Tech vs Info

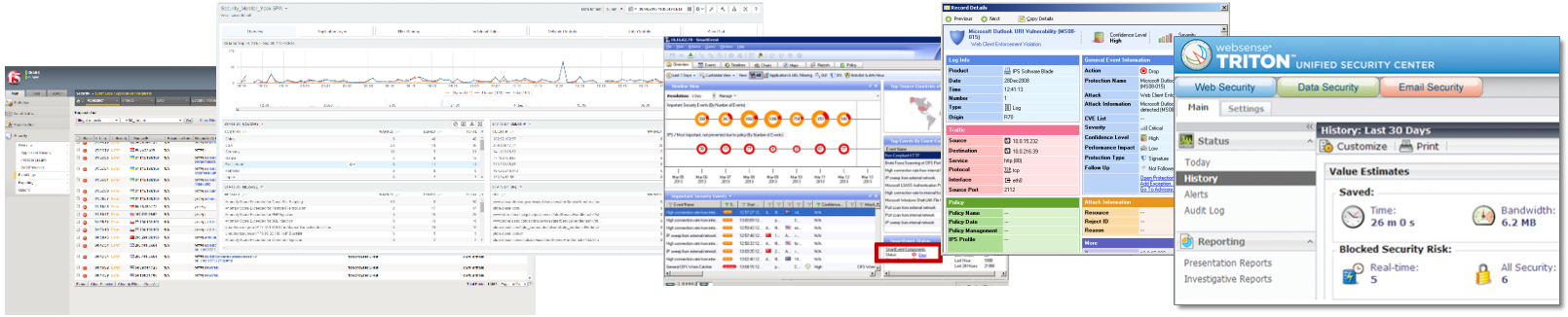
- Technology Oriented:
  - Info confined to technology
  - Partial identity definition
  - No covered gaps

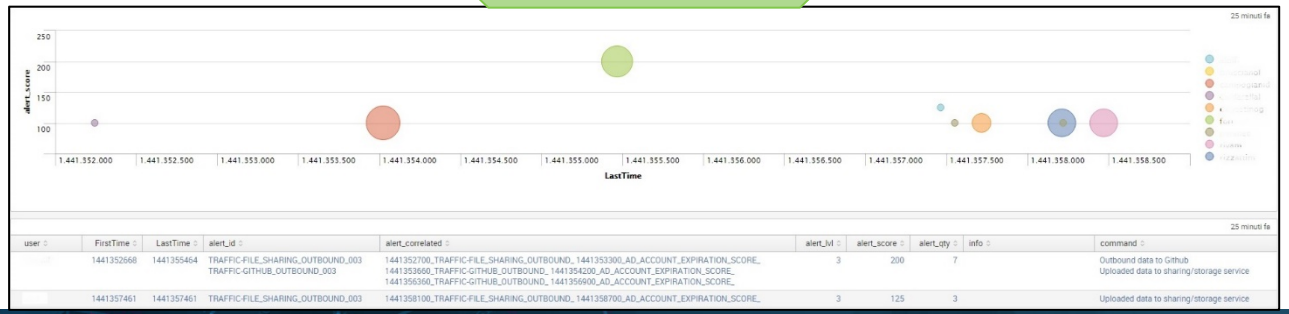
- Information Oriented - Splunk:
  - Enrichement of tech logs
  - Event correlation
  - Clear identity definition



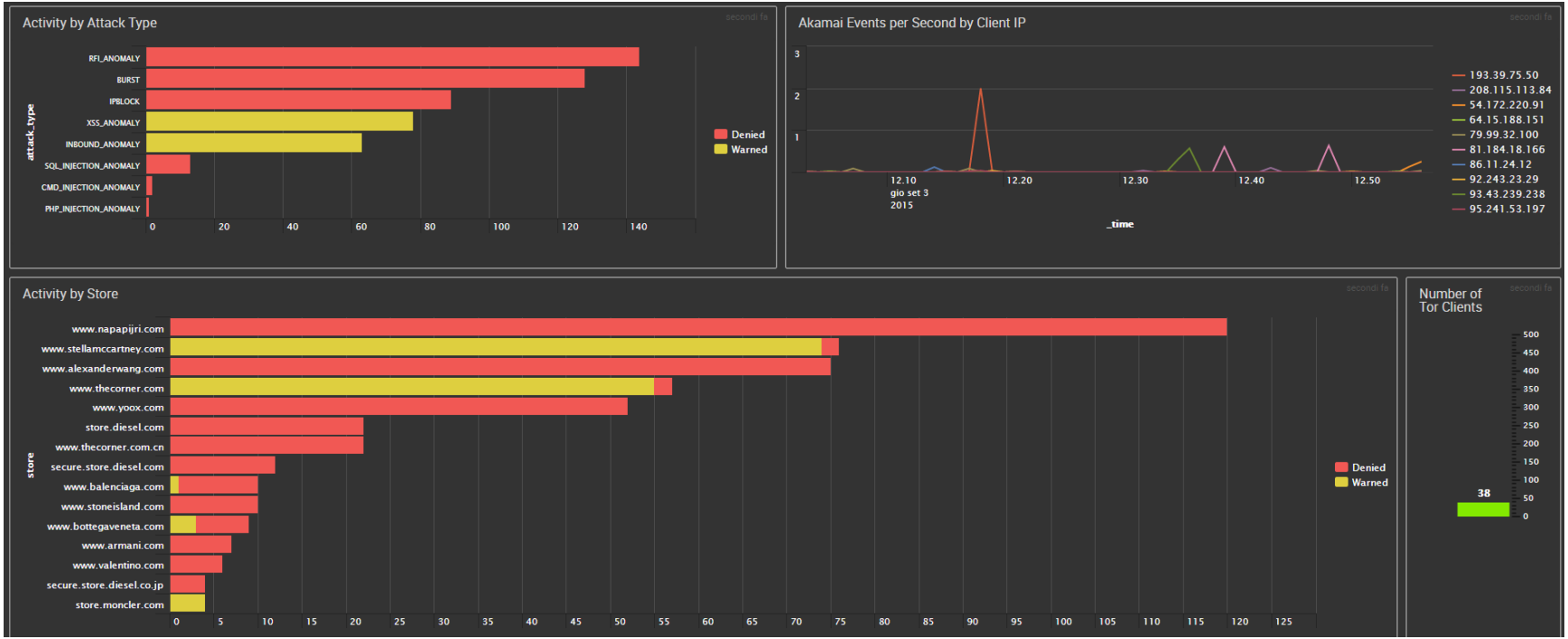
From Tech to Info

- "From a ***technology oriented*** approach to an ***info-centric approach***."

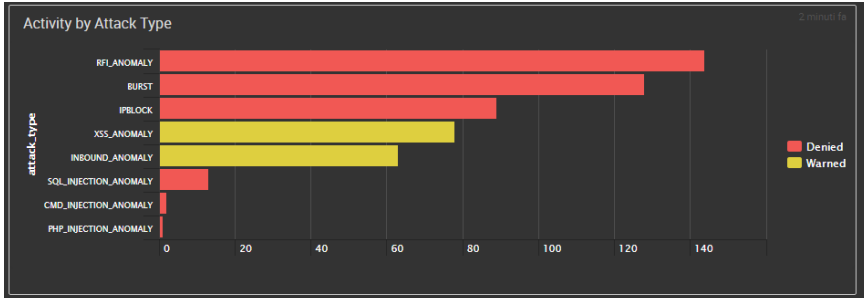




Investigation

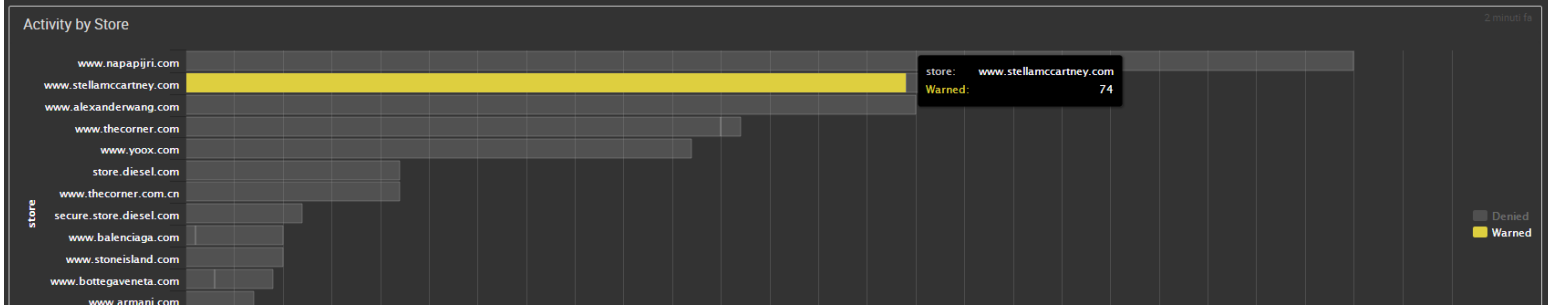


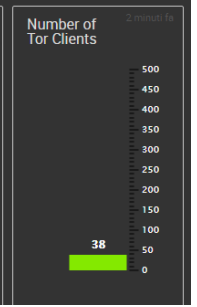
Investigation: Show Details



Client IP Details

Client IP	IP Domain	City	Country	Region	threatscore	visitor	Signature	Store	Action	count
81.184.18.166	81.184.18.166.dyn.user.ono.com	Barcelona	Spain	Barcelona	0	Suspicious	Anomaly Score Exceeded for Cross-Site Scripting	www.stellamccartney.com	Warned	37
81.184.18.166	81.184.18.166.dyn.user.ono.com	Barcelona	Spain	Barcelona	0	Suspicious	Anomaly Score Exceeded for Inbound	www.stellamccartney.com	Warned	37
180.140.125.73		Nanning	China	Guangxi Zhuangzu Zizhiqu	0	Suspicious	Anomaly Score Exceeded for Remote File Inclusion	www.stellamccartney.com	Denied	1
180.140.127.136		Nanning	China	Guangxi Zhuangzu Zizhiqu	0	Suspicious	Anomaly Score Exceeded for Remote File Inclusion	www.stellamccartney.com	Denied	1

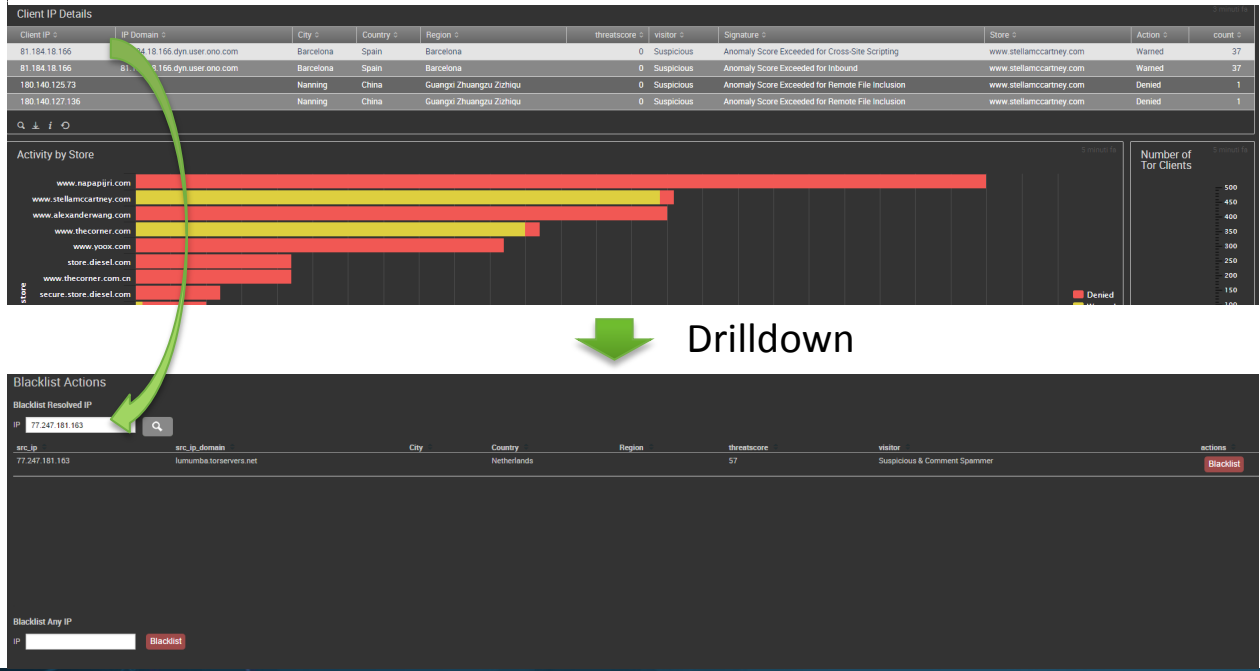




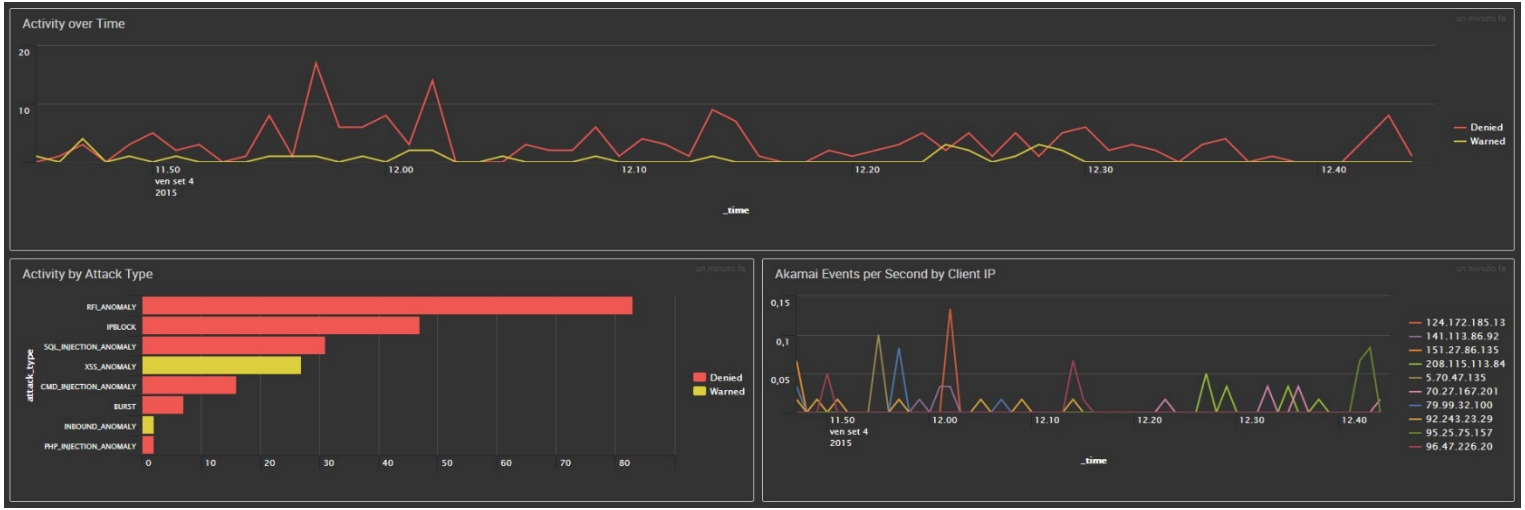
Advanced Dashboard: IP Blacklist

- Proactive Dashboard
- One-click blacklist on Akamai WAF through Akamai API calls
- ***Splunk is able to run a command on input source***

«From a ***passive/display platform*** to a ***proactive/executive platform***»



WAF Activity Representation: Standard Dashboard



Pros

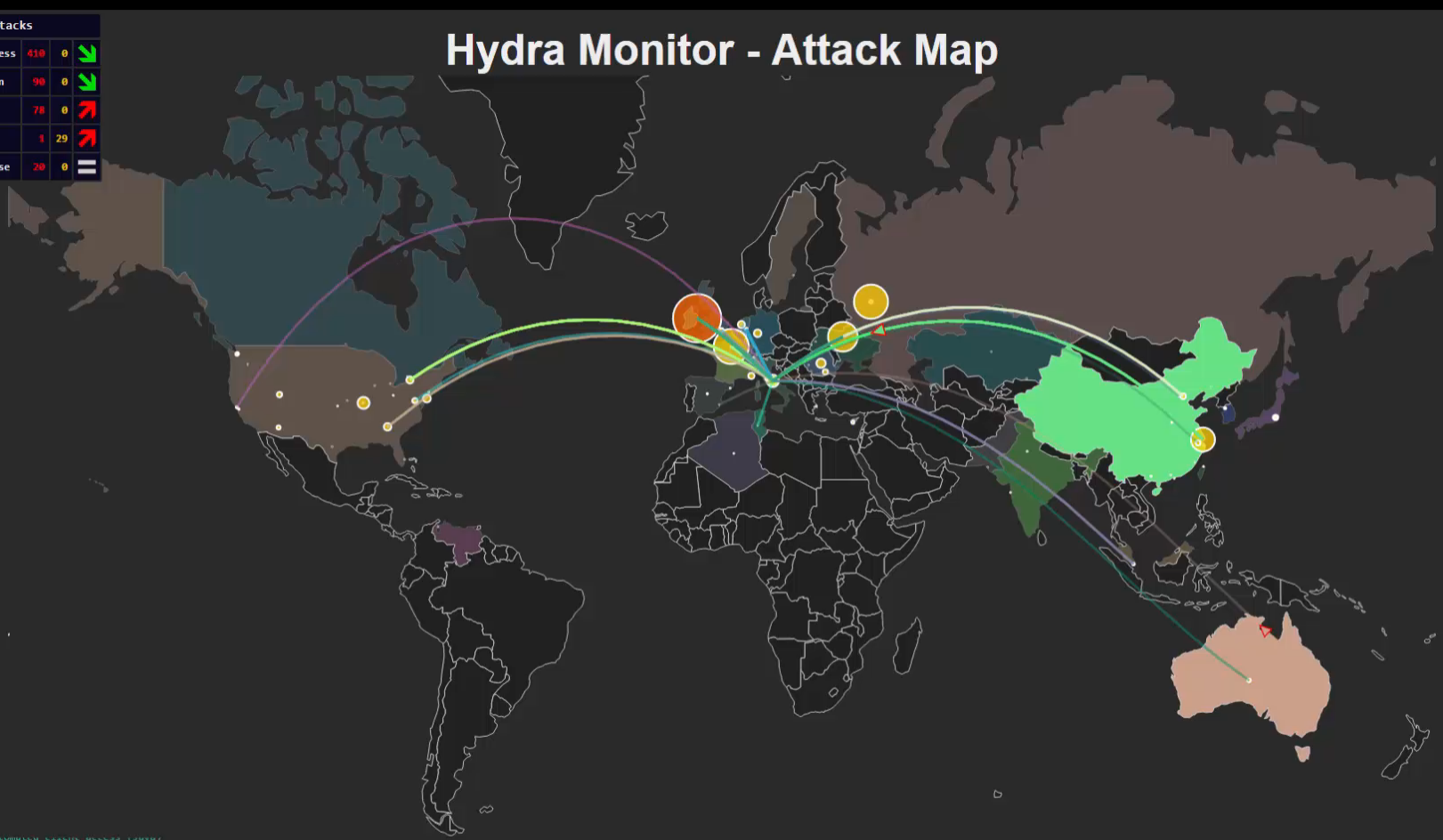
- Statistical evidences by:
  - Source IP
  - Attack type
  - WAF Action
- Event distribution over the time

Cons

- Spike visibility depends from the scale
- Is not evident:
  - Attack frequency
  - Relation between Source IP, Attack type and WAF action

Hydra Monitor - Attack Map

Top 5 Attacks			
Automated Client Access	410	0	↘
Remote File Inclusion	90	0	↘
Injection	78	0	↗
XSS	1	29	↗
yoox_custom_ua_synapse	20	0	=



IRL (54.72.126.60) Automated client access (Java)
IRL (54.72.126.60) Automated client access (Java)
IRL (54.72.126.60) Automated client access (Java)
CHN (101.226.33.205) PHP-CGI Shell Code Injection (v2)
IRL (54.72.126.60) Automated client access (Java)
IRL (54.72.126.60) Automated client access (Java)
AUS (203.161.139.196) YOOX_Custom_UA_SiteCon
IRL (54.72.126.60) Automated client access (Java)

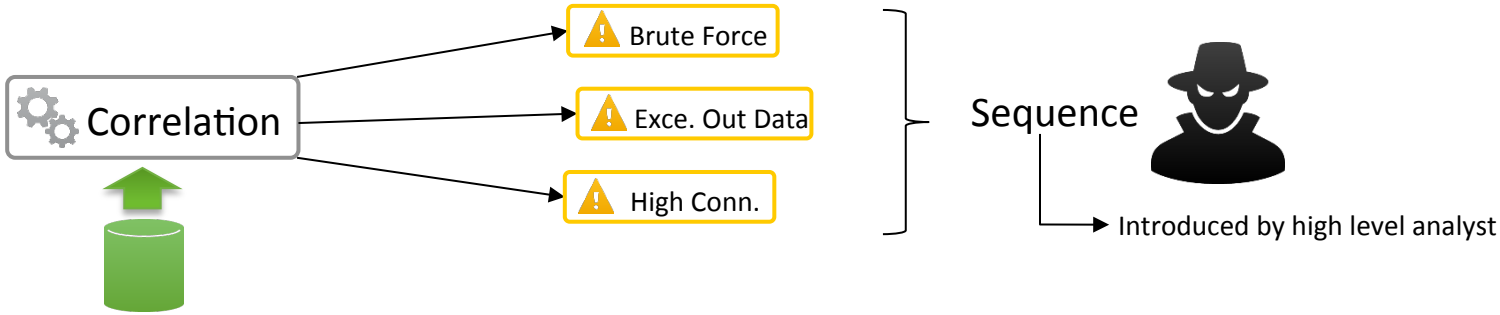
Security Evolution – Risk Mgmt & Pattern Rec.

- Risk Management:
  - Correlation of Tech Elements and Business Elements
  - Support to quantitative risk analysis
  - Assigning Risk value to alerts

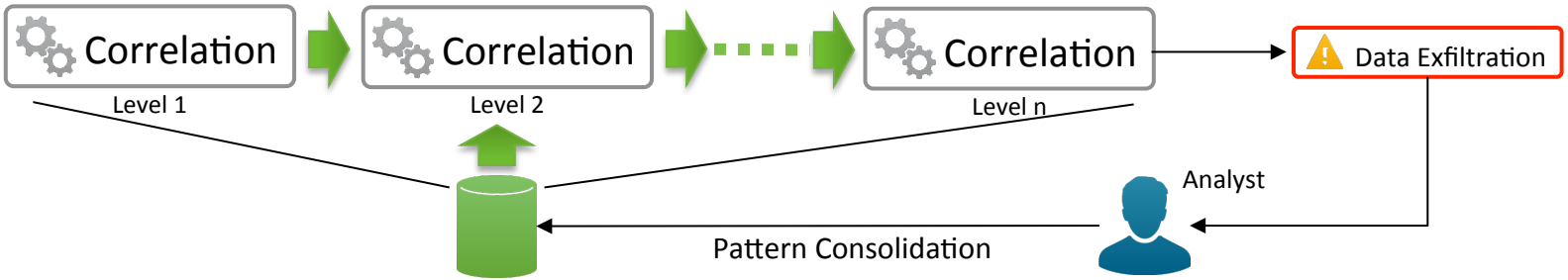
- Pattern Recognition:
  - Different levels of correlation
  - Pattern as result of several high-level events from different systems by identity
  - Knowledge from historical incidents and analysts experience
  - **Goal**: detect user behavior and recurrent attack patterns

Pattern Recognition

- Single security events may be part of a more complex action.



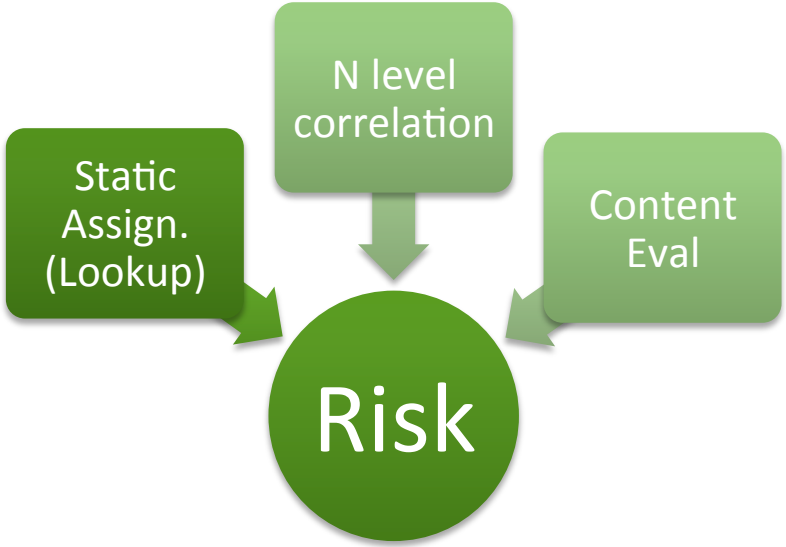
«From ***log correlation*** to ***pattern recognition***»



Risk Management

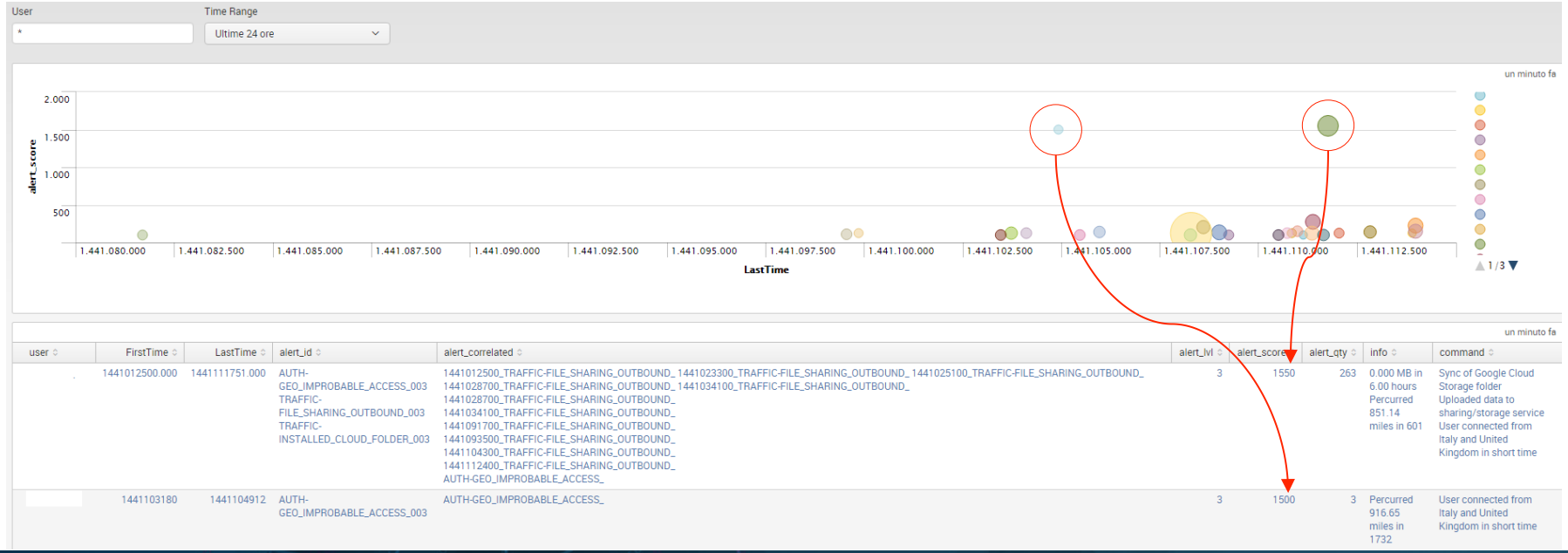
- Usually single security event has a static risk
- We need risk value based on content and other events correlated

"From a ***security event*** to an ***context-aware security information***"

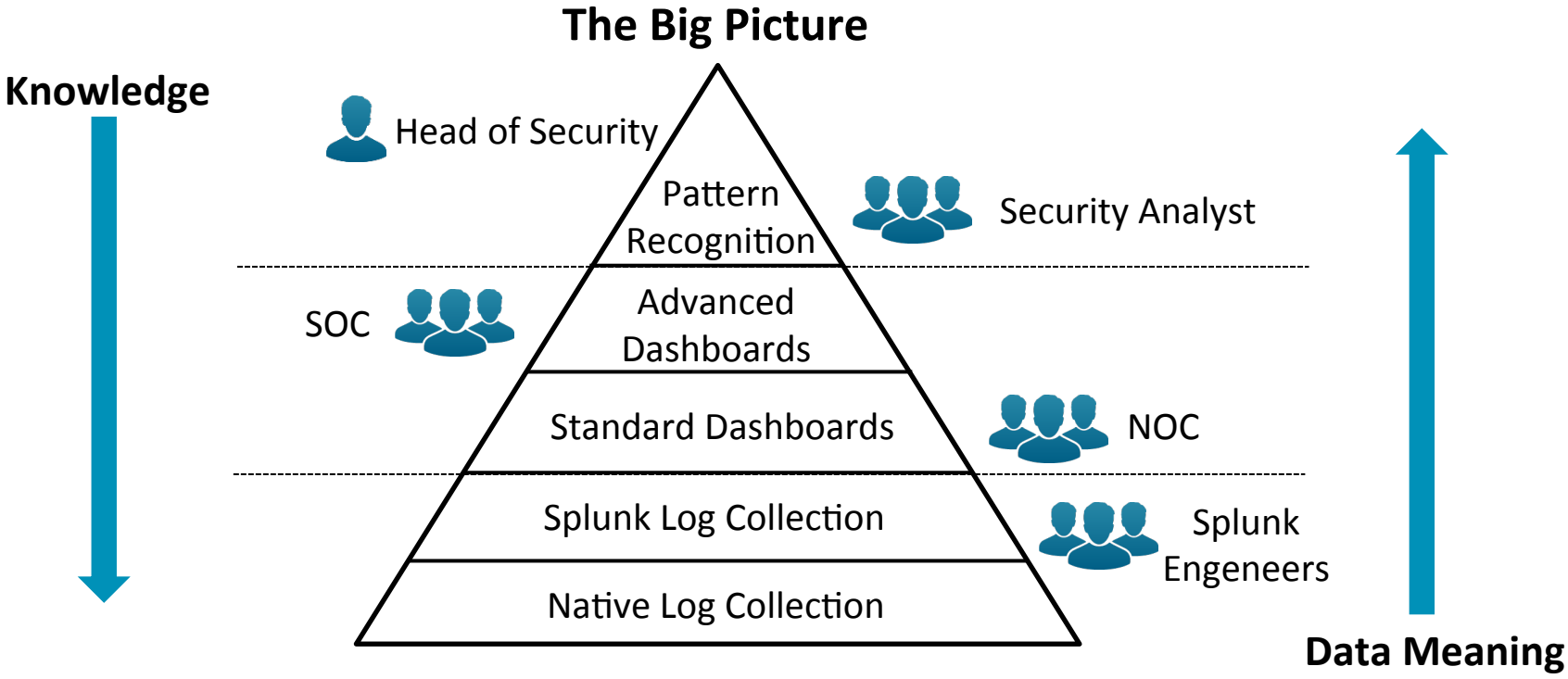


Use Case: Attackers Activity

- Detect sequence of relevant event by **identity** → **Pattern Recognition**
- Activity Score: vertical axes, max of the same alert type → **Risk Value**
- Activity Frequency: ball diameter



Reconsidering Dashboard Design

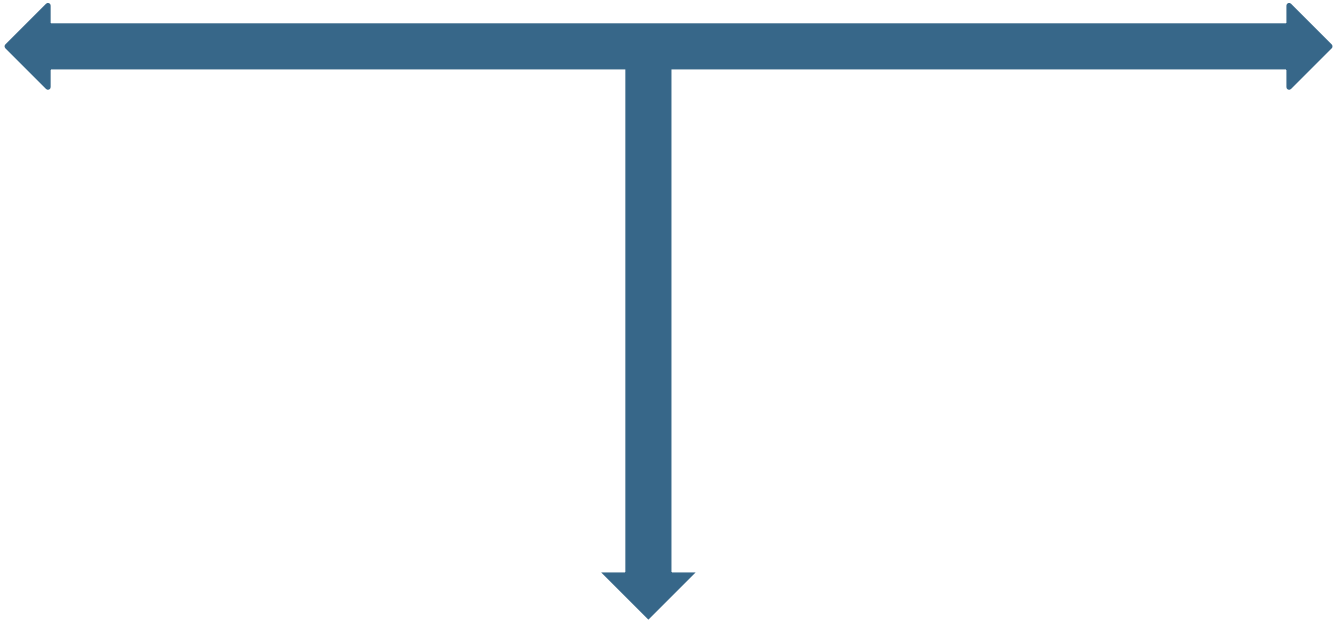


Key Takeaways

- From a ***technology oriented*** approach to an ***info-centric approach***.
- From ***log correlation*** to ***pattern recognition***.
- From a ***passive/display platform*** to a ***proactive/executive platform***.
- From ***standard dashboards*** to ***real-time dynamic dashboards***.
- From a ***security event*** to an ***context-aware security information***.

Next Steps

Extend the scope (channels, data, devices)



Deep into the noise

Questions?

THANK YOU

splunk>