

Giacimenti di informazione: estrarle e gestirle

Saipem come fa?

Alessio L.R. Pennasilico - *apennasilico@clusit.it*

Luca Mazzocchi - *Saipem*

4 Ottobre 2017



Clusit
Education

Alessio L.R. Pennasilico, aka -=mayhem=-

Cyber Security Advisor



Membro del Comitato Direttivo e del Comitato Tecnico Scientifico



Vice Presidente del Comitato di Salvaguardia per l'Imparzialità



Presidente dell'Associazione Informatici Professionisti (AIP)



Membro del Comitato di Schema UNI 11506 Informatico Professionista



Luca Mazzocchi

Saipem ICT Security Manager



BIO:

ICT Security Manager in Saipem Spa from 2010 with the responsibilities of two main security functions for the company.

The first is overseeing the security operations of the enterprise's solutions through the management of the security infrastructure. The second is establishing an enterprise security stance through standard, architecture and the implementation of all, increasingly modern, security solution. Secondary tasks include the design and selection of appropriate solutions.

Information management

- Cosa è un log?
- Dalla semplicità alla complessità
- Troppe informazioni = nessuna informazione
- Cosa può imparare la PMI e l'Enterprise dalla Large Enterprise / Multinazionale?

SAIPEM TODAY: THE COMPANY

Saipem is one of the world leaders in drilling services, as well as in the engineering, procurement, construction and installation of pipelines and complex projects, onshore and offshore, in the oil & gas market. The company has distinctive competences in operations in harsh environments, remote areas and deepwater. Saipem provides a full range of services with “EPC” and “EPCI” contracts (on a “turn-key” basis) and has distinctive capabilities and unique assets with a high technological content.

Our Numbers

REVENUES

- 2016 ≈ 9.9 B€
- 2017 guidance ≈ 9.5 B€

THE COMPANY

- Operating in more than 60 countries
- ~ 37,000 employees from ~ 120 nationalities
- More than 20 engineering and project execution centres worldwide
- 9 fabrication yards on 5 continents

SAIPEM

IT figures

Worldwide

Locations



Headquarters
San Donato Milanese

106 Sites

66 Offices

35 Vessels

Italy



Other Countries



281 Physical Servers
2,219 Virtual Servers



724 Physical Servers
1,712 Virtual Servers



3 Data Centres



2 Data Centres
~ 100 Data Rooms



~ 5,500 Work stations



~ 18,500 Work stations



~ 300 Applications



~ 100 MPLS links

~ 90 Satellite links



16 Voice Servers

117 VideoConf Endpoints



251 Voice Servers

241 VideoConf Endpoints



Workloads

Others

Saipem “pain”

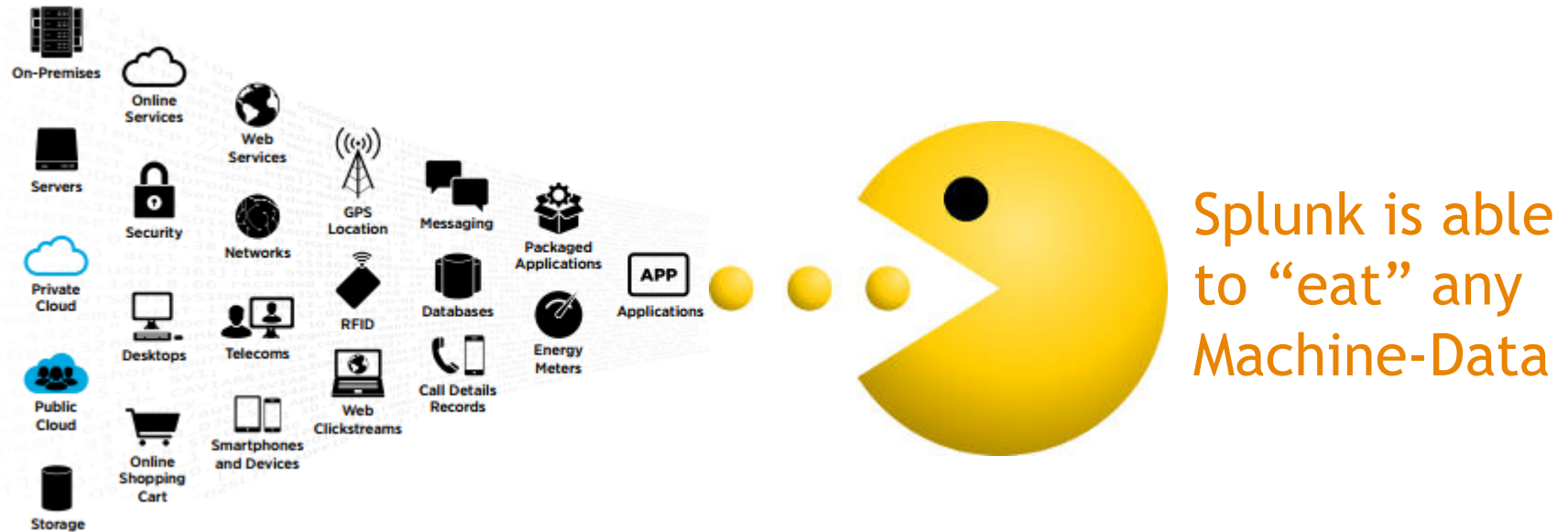
Which WAS the PROBLEM?



Data was distributed and replicated

Splunk

Which IS the SOLUTION?



And then...

Collect &
Index Data

Search &
Investigate

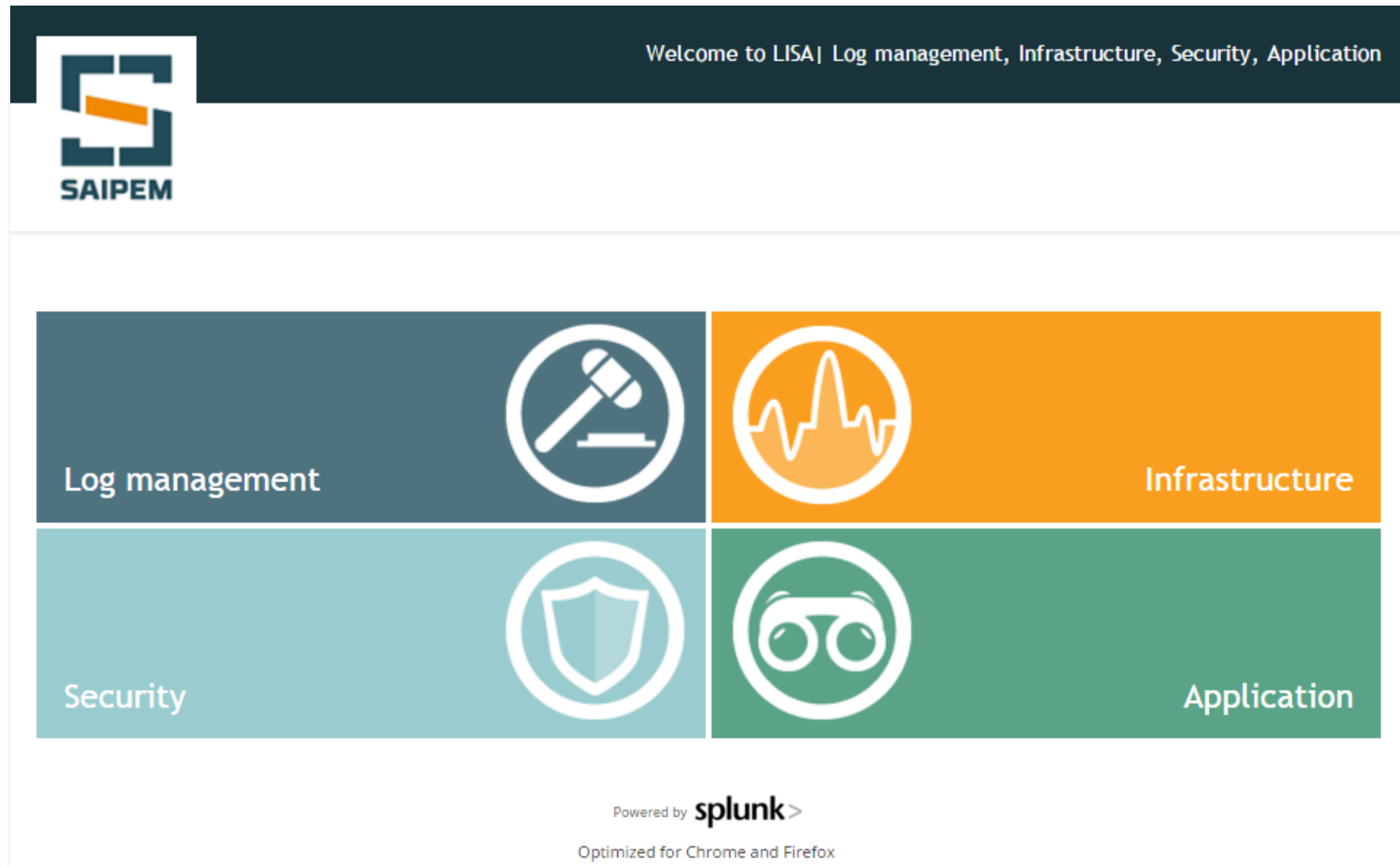
Correlate &
Analyze

Visualize &
Report

Monitor &
Alert

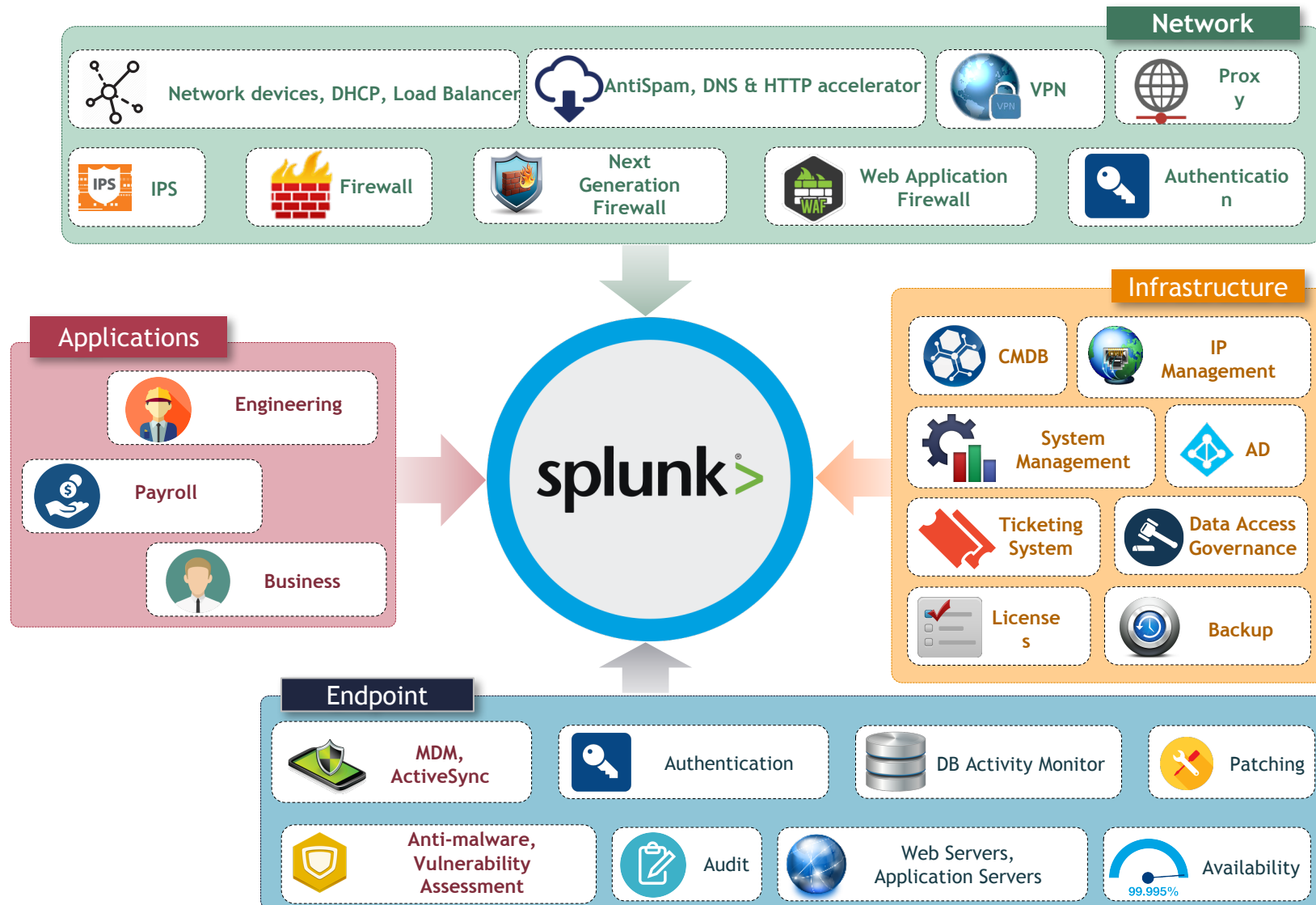
L.I.S.A.

Splunk customized unique PORTAL



Sources

LANDSCAPE of the collection



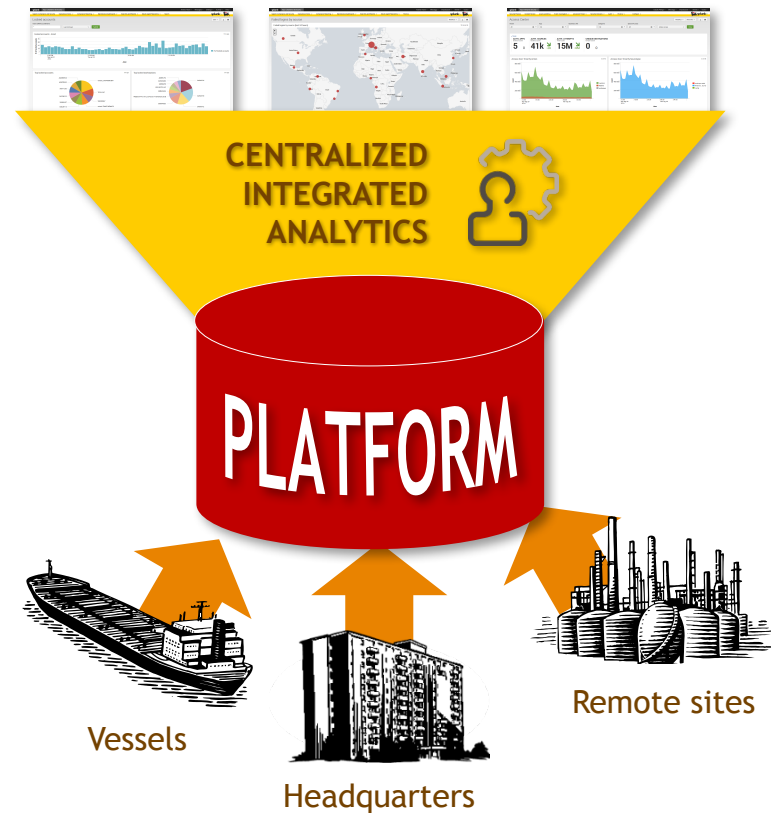
Benefits...

... achieved with SPLUNK

Data is collected from **distributed** and **heterogeneous** sources

The traditional Relational Model is a rigid frame unsuitable for **unstructured** data

A centralized and integrated platform allows **real time analytics**



Conclusioni

- *Gestire la complessità:*
 - Lo strumento adatto può rendere enormi quantità di informazioni disomogenee e distribuite interpretabili
- *Troppe informazioni = nessuna informazione*
 - Sintesi significa monitoraggio, strategia, azione
- *Cosa può imparare la PMI e l'Enterprise dalla Large Enterprise / Multinazionale?*
 - Sfruttare l'esperienza di chi ha staff, competenze e budget permette di adottare una soluzione egualmente efficace, azzerando i “costi di R&D” ed assorbendo costi di implementazione adatti al contesto di riferimento

Grazie dell'attenzione!

Domande?

mayhem@obiettivo.it
twitter: @mayhemspp
FaceBook: alessio.pennasilico
linkedin: alessio.pennasilico