

# A day in the life of a GDPR breach

Freddy Dezeure | Former Head of CERT-EU

James Hanlon | Director Security Specialists EMEA

Matthias Maier | Director Product Marketing EMEA

26th September 2017 | Washington, DC

# Forward-Looking Statements

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 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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.



# Who we are



# Freddy Dezeure

Former Head of the European Computer Emergency  
and Response Team (CERT-EU)



# Matthias Maier

Product Marketing Director, Splunk EMEA



# James Hanlon

Security Markets Specialization Director, Splunk  
EMEA

# What you will learn

---

## Get Data Privacy Right (GDPR)

- 

# About the GDPR

Freddy Dezeure



# GDPR Timelines

The regulation is binding across all EU members states

**January, 2012**

Commission proposes reform to Data Protection regulation

**April, 2016**

EU Council adopts new regulation

**December, 2015**

EU agreement on regulation

**25 May, 2018**

Regulation enters into force



# What's the scope of the GDPR?

*Any* information relating to an *identified* or *identifiable natural* person

- Individual IP, DNA, fingerprint, credit card, username, address, email address, phone number...
- Processed by *establishment in the EU*
- Or related to *data subjects in the EU*
- Or related to *behavior taking place in the EU*
- *Even if at no cost*





# How are the roles defined?

## Controller

- A **Controller** is the natural or legal person who determines the purpose and means of the processing of personal data

## Processor

- A **Processor** is a natural or legal person that processes personal data on behalf of a controller. The Controller remains responsible to make sure the processor applies the relevant measures to comply

## Responsibilities

- Controllers and Processors need to **maintain a record of their processing activities** and be able to **demonstrate compliance**



# What Does This Mean?

Identify why you collect and process personal data, how much, how you keep them up to date, how long and how you protect them.

Document all this and have processes in place to maintain and update the documentation.

- Data subjects have a right of **access, rectification, transfer, removal**

# The right of a data subject



- Right not to be subjected to automated decision-making (profiling).

# Mitigation

Measures to comply take into account the risk

- In case of **high risk** -> perform an impact assessment (PIA) to determine appropriate mitigation measures

**Appropriate** technical and organizational measures, taking into account the state of the art

- Pseudonymization & encryption
- Ensure confidentiality, integrity, availability and resilience of processing systems
- Backup & restore
- Testing of effectiveness



# The impact if a breach happens

- Notification within 72 hours to supervisory authority **if** there is a risk
- If high risk: communication to data subjects, coordinated with supervisor

## Possible consequences:

- Administrative fine up to 4% of world-wide annual turnover
- Victim damage compensation
- Criminal prosecution

## Waiver

- The controller or processor should be exempt from liability if it **proves that it is not in any way responsible** for the damage.



# How to treat log data containing PI information

Freddy Dezeure

A large, solid green circle is centered on the page. It is a simple, uniform shape with no internal details or text.

# Do I need to delete my log data in case of a delete request?

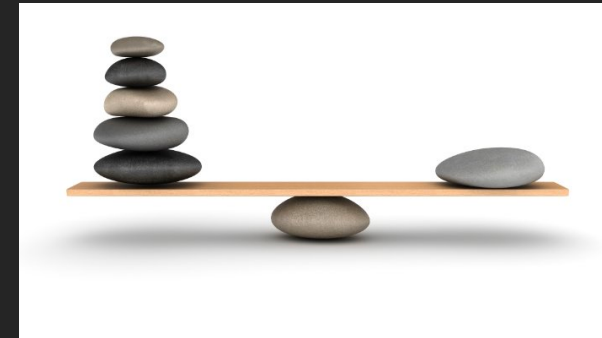
# Do I need the individuals consent for log data processing?

Read beyond (a) as well

## Article 6 : "Lawfulness of processing"

- (a) the data subject has given **consent** for one or more specific purposes
- (b) necessary for the performance of a **contract with the data subject**
- (c) necessary for compliance with a **legal obligation of the controller**
- (d) necessary in order to protect the **vital interest of a person**
- (e) necessary for the performance of a task carried out in the **public interest** (..)
- (f) necessary for the purposes of **legitimate interests** (...)

- ✓ Network and Information Security: (f) Legitimate Interest
- ✓ Other purposes of processing: understand them, document and validate with your DPO



# Special clause on Network Information Security

## Recital 49:

- “The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security [...] by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. [...]”





## Article 32 : "Security of processing"

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to **ensure a level of security appropriate to the risk**, including **as appropriate**:

(a) the pseudonymisation and encryption of personal data (...)

Finding the **balance** between risk, appropriate technical and organisational measures while maintaining productivity, availability and integrity of machine data for different purpose.

- Centralize machine data with controlled role based user access and audit trail

Further options based on risk assessment:

- Data minimization through anonymization techniques (Visualization Level or Raw Level needs to be decided - appropriate to the risk and need from different team's)
- Data pseudonymization by maintaining integrity, usability (Technical Concepts with Pro/Cons check .conf session „Data Obfuscation and Field Protection in Splunk“)

# Do I need to pseudonymize all my machine data?

## Risk mitigation techniques



# Do I need to delete my log data in case of a delete request?

## Review Paragraph 3

### Article 17 : “Right to erasure ('right to be forgotten')”

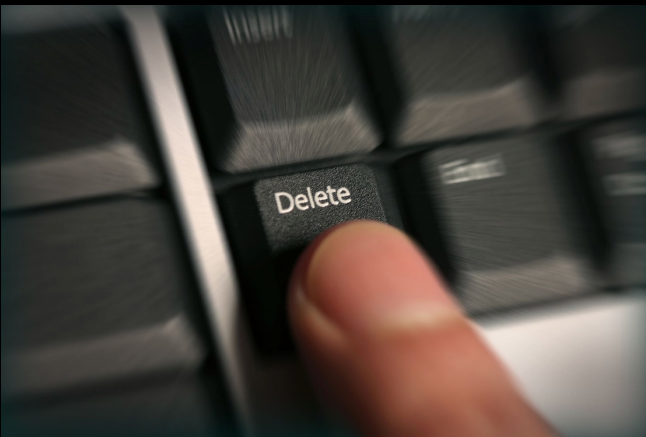
- (1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
  - (a) The data are no longer necessary for the purpose
  - (b) Withdrawal of consent
  - (c) ...
  - (d) The data was unlawfully processed
  - (e) ...
  - (f) ...

These conditions would very likely not apply for Network and Information Security logs.

In case the data subject has the right to erasure of data from logs, this function is supported by Splunk. ( | delete command stops processing, retention policy wipes it finally from disk)

<https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Delete>

<https://docs.splunk.com/Documentation/Splunk/6.6.3/Indexer/Setretirementandarchivingpolicy>



# “An IP address is personal data – this doesn’t mean there is a problem”

Freddy

# The day in a life of a GDPR breach

Matthias



25th of May

What if  
tomorrow is

2018

## A collage of five hands pointing in different directions against a white background. The hands are arranged in a circular pattern, each pointing towards the center. The hands are of different skin tones and are shown from various angles, creating a dynamic and multi-perspective composition.



A white alarm clock with two bells and a white ceramic mug on a matching saucer. The clock face shows the time as approximately 10:10. The word 'QUARTZ' is visible on the clock face. The items are placed on a light-colored wooden surface against a bright, out-of-focus background.

# Your friendly Data Privacy Officer is on the phone



1001111110110111101011100111111101101  
001000001011111000101010010000010101001000001011111  
0101010101010010010101010101010010101010101010100  
11111011001000111110011111111110011111011001000  
10101101110010111001111010111160111101011011100101  
010101100011001010100101010101001010101100011001  
011011101011011010101101101101010110110110101101  
1101101110101101111111111011100111111011011101011  
0111110001010101000010111100100010111100010101  
0111001111010111111111111001111001111010110  
01010100101010110111110101110110010101001010101  
10101011011011101011011011011011011011011011011  
10011111110110111010111001111110101110011111110110  
00100000101111100111110010000010101001000001011111  
0101010101010011111010101010101010101010101010100  
111110110010001111100111111111100111111011001000  
10101101110010111001111010111100111101011011100101



Your threat  
Intelligence  
provider  
informed you  
and provided  
you samples

[HOME](#)[PRODUCT](#)[PARTNERS](#)[MEDIA](#)[ABOUT](#)[BLOG](#)[CONTACT](#)

WE AUTOMATICALLY AND COVERTLY  
MONITOR THE DARK WEB TO

**OBSERVE THE ATTACKER  
AND THEIR PLANS**

Watch how Sixgill Sheds Light on the Dark Web



splunk>

.conf2017



# There is data in the deep web

[illegible]



# He hangs up! What's next?



# Your incident investigation plan kicks in

## Emergency Plan

An emergency plan is a good action plan to mitigate the effects of an emergency planning.

DPO  
IT  
PR/Media Team  
Legal  
(CEO)





# Emergency call

# Emergency chatroom



# The fire alarm button is pulled down









# Reaching out to your security operations team

“We need to  
investigate!!!”



T-65h



# T-55h



# Is data still leaking?

First Action



T-45h



# How will you watch them?



T-40h

Nice,  
structured,  
tidy data



T-39h



# Diving deep into the digital infrastructure



# Machine data

time series, in motion,  
unstructured



T-34h



**External  
authorities  
might come in  
to your  
organization  
and say:  
“Don’t stop it”**

Worst Case



T-25h

# Take response actions to stop data leakage



T-20h

# T-15h



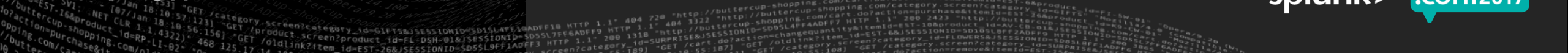


# Who processed your information?



T-10h

# T-8h



# You know what you know

# You know what you don't know





# Puts the breach data subjects at risk?

Maybe resulting in a non event?







# As an organization you want to control the story

before chatter explodes

- Inform Authority
- Inform affected Individuals
- (Inform Public)



T. Oh




# Best Practice: ABTA Breach

## Security

# UK's Association of British Travel Agents cops to data breach

Yes there's still such a thing as a travel agent

By John Leyden 16 Mar 2017 at 14:28

11  SHARE ▼



A hack attack on the Association of British Travel Agents (ABTA) has exposed the personal details of thousands of consumers and hundreds of tour operators and travel agents.

Data for up to 650 ABTA members and up to 43,000 consumers was exposed by the breach, which dates from late last month.

In a **statement** on Thursday. The travel industry organisation blamed a successful attack against its hosting provider. It sought to downplay concerns by saying the problem had already been contained.


[Tips & latest](#)
[Holiday help & complaints](#)
[Conferences & events](#)
[Working with the industry](#)
[Services for business](#)
[About us](#)

[UPDATES](#) [ABTA statement on the earthquake in Mexico](#)

## Data security incident March 2017

[← NEWS HOME](#)

### NEWS TEAM

16 March 2017

#### Statement from ABTA CEO, Mark Tanzer, relating to Data Security Incident (March 2017)

We recently became aware of unauthorised access to the web server supporting abta.com by an external infiltrator exploiting a vulnerability. The web server is managed for ABTA through a third party web developer and hosting company. The infiltrator exploited that vulnerability to access data provided by some customers of ABTA Members and by ABTA Members themselves via the website.

On further, urgent investigation we identified that the incident occurred on the 27 February 2017 and related to some customer information, including complaints about ABTA Members, and to documentation uploaded via abta.com in support of ABTA membership. Although encrypted, passwords used by ABTA Members and customers of ABTA Members to access our website may also have been accessed.

Having become aware of the unauthorised access, we immediately notified the third-party suppliers of the abta.com website who immediately fixed the vulnerability. ABTA immediately engaged security risk consultants to assess the potential extent of the incident. Specialist technical consultants subsequently confirmed that the web server had been accessed.

We are not aware of any information being shared beyond the infiltrator. We are actively monitoring the situation, but as a precautionary measure we are taking steps to warn both customers of ABTA Members and ABTA Members who have the potential to be affected. We are today contacting these people and providing them with information and guidance to help keep them safe from identity theft or online fraud. We have also alerted the relevant authorities, including the Information Commissioner and the Police.

I would personally like to apologise for the anxiety and concern that this incident may cause to any customer of ABTA or ABTA Member who may be affected. It is extremely disappointing that our web server, managed for ABTA through a third party web developer and hosting company, was compromised, and we are taking every step we can to help those affected. I will personally be working with the team to look at what we can learn from this situation.

Outlined below, we have answered further questions, which include some guidance for customers of ABTA and ABTA Members.

[What has happened?](#)
[What type of information may have been accessed?](#)
[What is ABTA doing about this incident?](#)
[ABTA Member companies – what do I need to do?](#)
[Members of the public – what do I need to do?](#)





# Example

## ABTA Breach

2+ weeks later out of the news

Google search for "abta breach" (March 16, 2017):

- About 6,480 results (0,29 seconds)
- News results include:
  - UK's Association of British Travel Agents cops to data breach - The Register - 16 Mar 2017
  - ABTA website hacked, 43000 people affected by breach - ZDNet - 16 Mar 2017
  - Abta data breach: Tens of thousands of holidaymakers hit in ... - Computer Business Review - 16 Mar 2017
  - ABTA takes more than a fortnight to alert customers of data breach - ITV News - 16 Mar 2017
  - Abta suffers security breach affecting thousands of glum British ... - Ars Technica UK - 16 Mar 2017
  - Personal details of 43000 holidaymakers including email addresses ... - In-Depth - Daily Mail - 16 Mar 2017
- Image results show various related images (e.g., people, a padlock, a beach, a shopping bag).
- Link: [View all](#)
- Snippet: **ABTA experiences data breach**

Google search for "date today" (April 3, 2017):

- About 742.000.000 results (0,57 seconds)
- Date widget: **Monday, 3 April 2017**
- Location: Date in Salzweg

# T+1 Week



# Data Privacy Audits

Have you deployed  
“countermeasures  
appropriate to the risk”?

Have you used “state  
of the art” best  
practices?



T+ 1 Week



# T+1 Week

# Prove

What did you know?

When did you know?

How did you know  
about it?



T+ 2 Weeks



## A photograph of a wooden table with three white evidence markers numbered 1, 2, and 4. A small, light-colored, irregular object, possibly a piece of evidence, is on the table near marker 1. The background is a plain wall.



# GDPR Article Mapping

James Hanlon

# Looking into the Details

4.5.2016

EN

Official Journal of the European Union

L 119/1



I

(Legislative acts)

## REGULATIONS

**REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**of 27 April 2016**

**on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**

(Text with EEA relevance)

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

# Splunk for GDPR



# Detect and Investigate Data Breaches



# Prove GDPR Security Controls are enforced



# Search and Report on Personal Data Processing



# Article 33 & 34

## Breach Notification

**“In light of the tight timescales for reporting a breach - it is important to have robust breach detection, investigation and internal reporting procedures in place.”**

# ICO (Information Commissioner's Office) on the GDPR Breach Notification

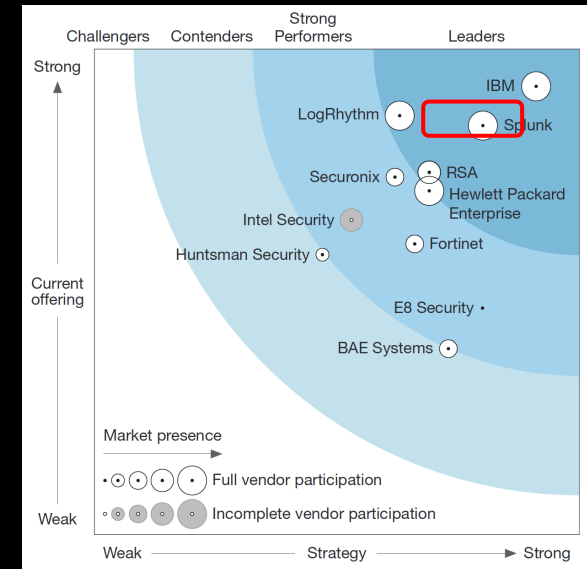
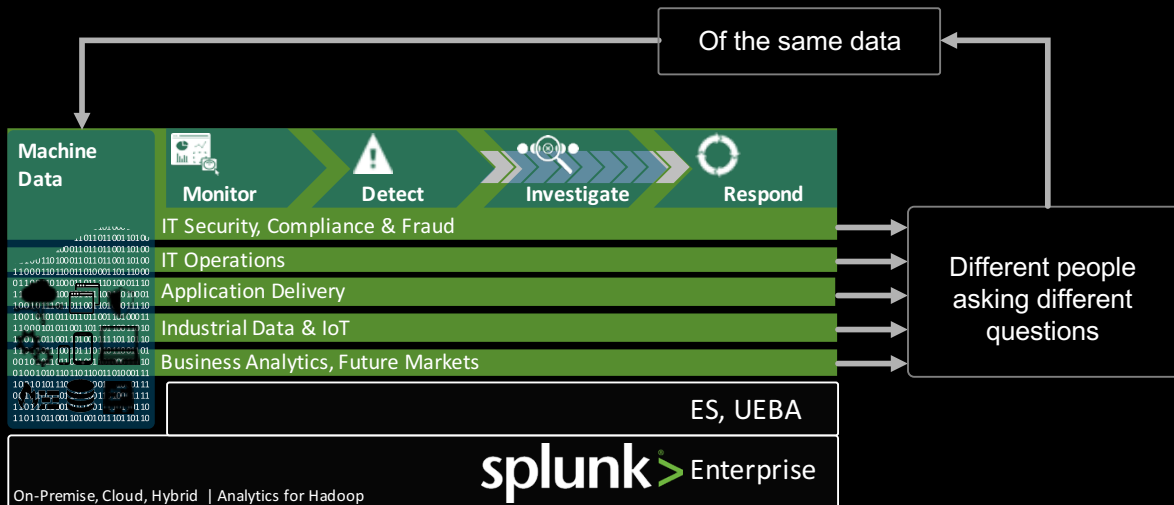
<https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/breach-notification/>

# Splunk for GDPR



- > **Article 33** - Notification of a personal data breach to the supervisory authority
- > **Article 34** - Communication of a personal data breach to the data subject

> **Data Breach Notification**



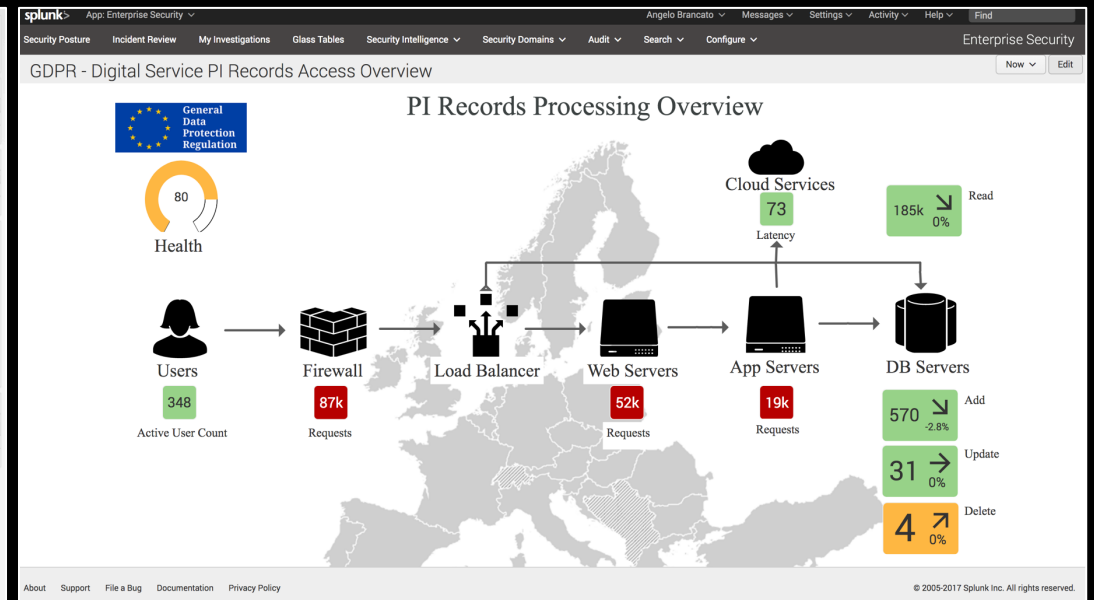
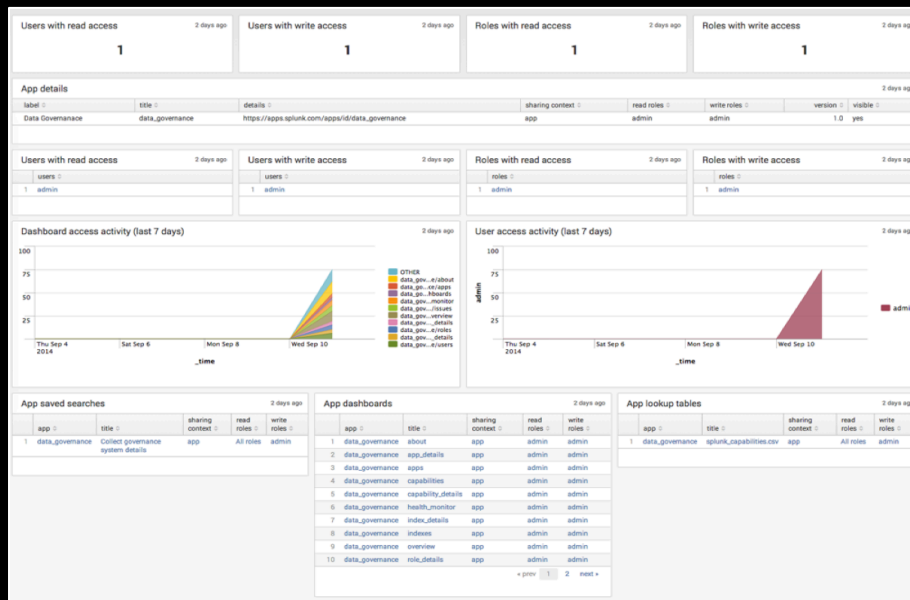
# Splunk for GDPR

## > Article 32 - Security of processing

> **Risk  
Minimization**

> **Evaluate  
Controls  
Effectiveness**

> **Prove  
Appropriate  
Controls in Place**





## Findings from ICO work relating to Community Pharmacies

# Article 30

## Records of Processing

The majority of IT systems had a single company or branch logon to the computers in branch. From here the PMR system was accessed. Some organisations operated a single username and password for the PMR system allowing access to all staff. This means there are no audit logs created of viewing or amending records. At others each member of staff has a unique user logon and password. In the best examples these passwords expire after set time periods and must have a minimum level of complexity.

**Recommendation:** Systems that contain patient identifiable data should always have individual user logons to enable a full audit trail of view and change events to a customer record. Having an auditable log of changes and access to systems containing sensitive personal data is important to prevent illegal activity and maintain data quality standards.

In England some companies were able to act as issuing authorities for the NHS Smart Cards, while others were merely sponsoring bodies. It was seen that not all pharmacies have full compliments of eligible staff issued with

# Splunk for GDPR



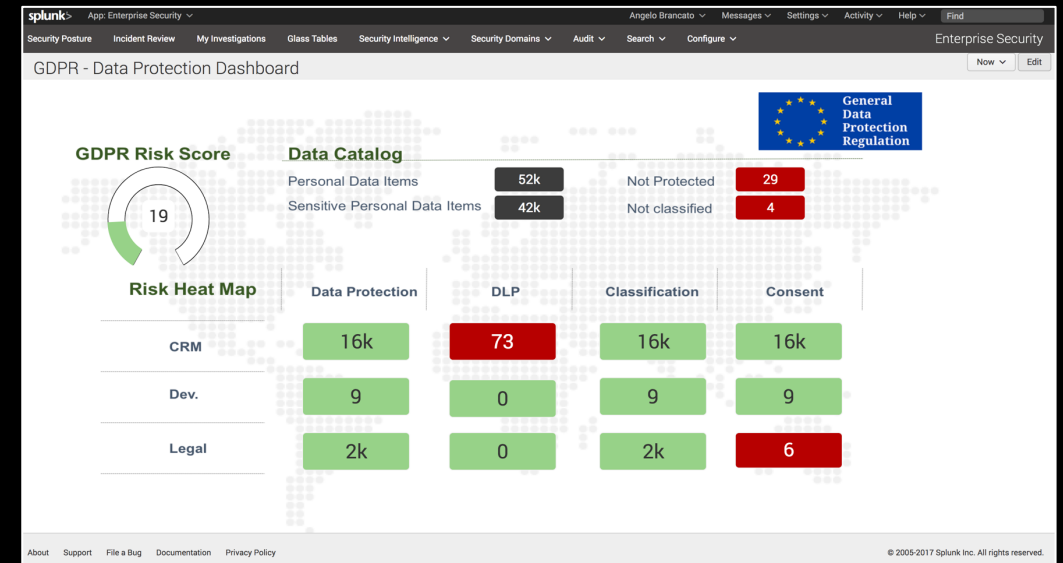
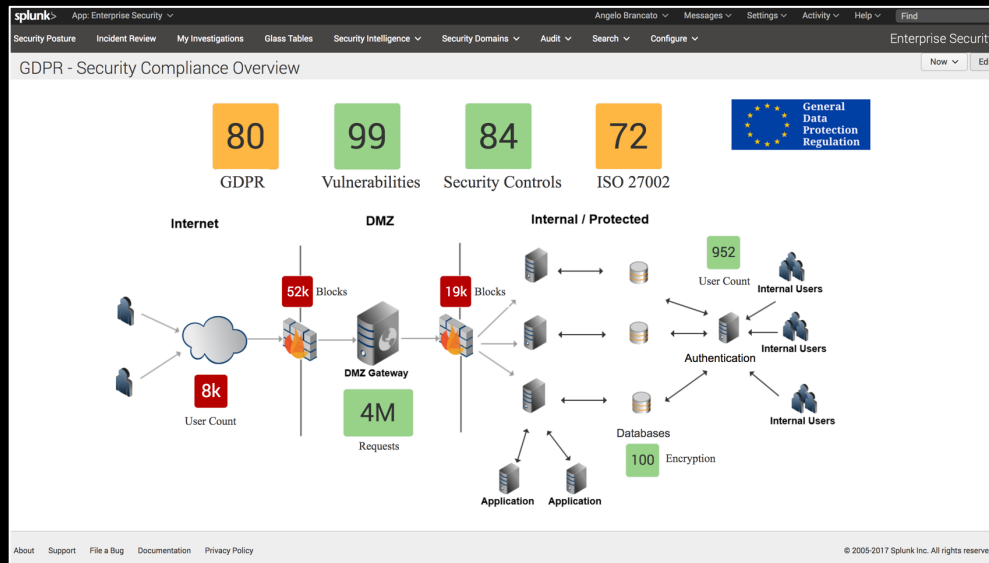
- > Article 30 - Records of Processing Activity
- > Article 5, 15, 17, 18 and 28 - Data Subject Rights

> Right to be Forgotten

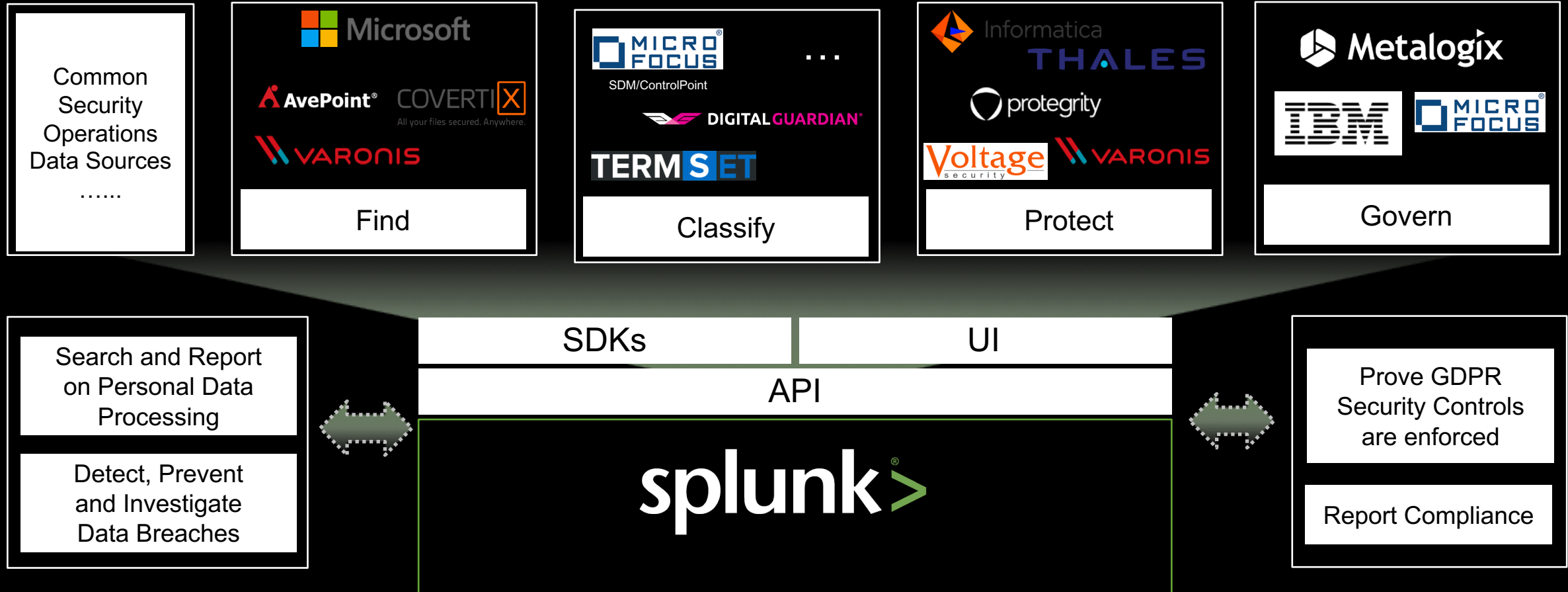
> Right of rectification

> Right of access

> Right of data portability



# Visibility and Enforcement for GDPR



*No rigid schemas – add in data from any other source.*



# Supporting Your Risk Minimization Strategy

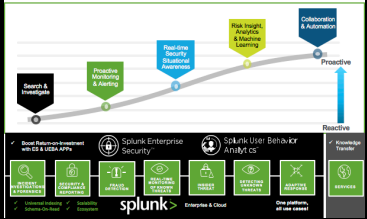
- ✓ Data in transit: Encryption
- ✓ Data at rest: Encryption
- ✓ Data at rest: Integrity
- ✓ Data/Fields within Splunk:
  - ✓ Anonymization in raw event
  - ✓ Anonymization in presentation layer
  - ✓ Pseudonymization in raw event
  - ✓ Pseudonymization in presentation layer



# Resources to help you

James

# Splunk Support for the GDPR Journey

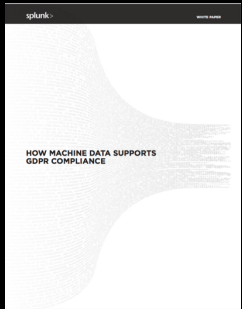
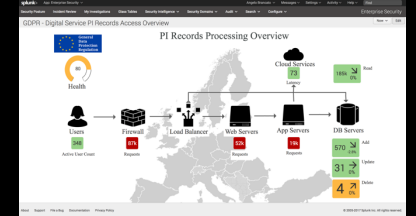


## Security Analytics & Investigation Readiness

Define a strategy & outcome for security analytics & breach Investigation

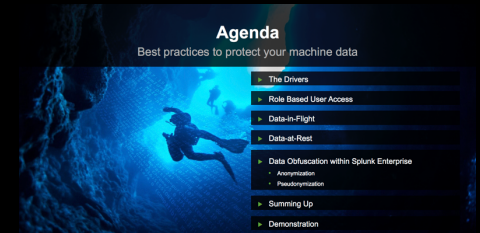
## GDPR Workshop

Map analytics capabilities to GDPR security monitoring & reporting needs



## How to use Machine Data for GDPR

Whitepaper outlining how machine data can support GDPR



## Splunk Data Obfuscation

How to protect data using anonymisation, pseudonymisation & encryption in Splunk  
Thursday, September 28, 2017 | 11:35 AM-12:20 PM



# Q&A

Freddy, Matthias, James