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
After this session you know

- What the GDPR is
- How it will impact your organization
- What PI information can be in machine data
- How to treat log data in Splunk under the GDPR
- How Splunk can help you during a breach (Day in a life of a GDPR breach)
- What articles Splunk can help you with
- What further Workshops/Collateral Splunk provides you to

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
What are the general principles?

- Lawful, fair and transparent
- Specific, explicit and legitimate purpose
- Adequate, relevant and limited
- Accurate
- No longer than necessary
- Security and confidentiality
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.
The right of a data subject

• Data subjects have a right of access, rectification, transfer, removal

• 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
Storing and Analyzing Machine data with Splunk under the GDPR
Some frequently asked questions

Do I need the individuals consent for log data processing?

Do i need to pseudonymize all my log data?

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. [...]”
Do I need to pseudonymize all my machine data?

Risk mitigation techniques

---

**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 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/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
What if tomorrow is
What if you’re responsible for Security?
You wake up in the morning and you even haven’t had your coffee
Your friendly Data Privacy Officer is on the phone
Someone claims to sell PI data you hold
Your threat intelligence provider informed you and provided you samples.
It may be your data!

There is data in the deep web
He hangs up!
What’s next?
Your incident investigation plan kicks in

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

DPO
IT
PR/Media Team
Legal
(CEO)
The fire alarm button is pulled down
72 Hour Breach Notification
Incident commander

Internal Leak
External Leak

T- 70h
Reaching out to your security operations team

“We need to investigate!!!”
Where is that data stored in your environment?
Is data still leaking?

First Action

T- 45h
How will you watch them?
Nice, structured, tidy data
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
Take response actions to stop data leakage

T- 20h
Understand

T- 15h
Who processed your information?
Which user or systems was involved?

T-8h
Painting the picture
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?
How sensitive was the data?

Do individuals need to be informed additionally?
As an organization you want to control the story before chatter explodes.

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

T-0h
Best Practice:  
ABTA Breach

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

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.
Best Practice:

ABTA Breach
Example

ABTA Breach

2+ weeks later out of the news
Someone knocks on your door

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
Massive Fines

T+ 1 Week
Prove

What did you know?
When did you know?
How did you know about it?

T+ 2 Weeks
Logs become your digital fingerprints
GDPR Article Mapping

James Hanlon
Looking into the Details

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

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**

- Different people asking different questions
- Of the same data

---

**Machine Data**

- Monitor
- Detect
- Investigate
- Respond

- IT Security, Compliance & Fraud
- IT Operations
- Application Delivery
- Industrial Data & IoT
- Business Analytics, Future Markets

**ES, UEBA**

- On-Premise, Cloud, Hybrid | Analytics for Hadoop

---

**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

---

**Forrester Wave: Security Analytics Platforms, Q1 2017**

- Gartner MQ for SIEM, Aug. 2016

---

**IT Operations**

- Application Delivery
- Business Analytics, Future Markets

**Industrial Data & IoT**

- Application Delivery
- Business Analytics, Future Markets

**IT Security, Compliance & Fraud**

- Application Delivery
- Business Analytics, Future Markets
Splunk for GDPR

> Article 32 - Security of processing

> Risk Minimization

> Evaluate Controls Effectiveness

> Prove Appropriate Controls in Place
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.
Pseudonymization of PII
Stay compliant whatever occurs in your machine data

- 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

Supporting Your Risk Minimization Strategy
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 GDPR Support

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