IBM Security

The most painful way to implement GDPR

BASED ON 40+ CUSTOMER GDPR PROJECTS I MADE

Marcin Spychała
Senior Security Architect

25.05.2018

IBM

THE FOLLOWING SCENARIO HAS BEEN APPROVED FOR

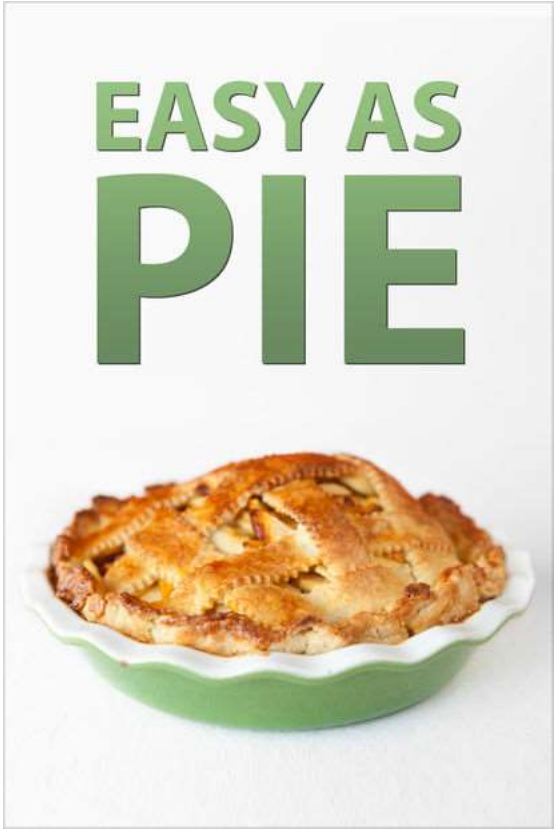
RESTRICTED CYBERSECURITY AUDIENCES ONLY

BY THE IBM SECURITY FINANCIAL SERVICES TEAM OF AMERICA

IT HAS BEEN RATED

S	**Scarily Realistic**
	THIS CONTENT REQUIRES THAT EXECUTIVES AND BUSINESS UNIT LEADERS BE ACCOMPANIED BY AN ARCHITECT OR SOC LEADER
HARSH REALITIES, GRAPHIC BREACHES	

I just hacked ….YOU



Why so late?

Interest over time

Google Trends

Interest by region

Region

1	Jersey	92
2	St Helena	75
3	Czechia	64
4	Luxembourg	59
5	United Kingdom	50

Include low search volume regions

Showing 1–5 of 51 regions

24 Apr 2016

10 Sep 2017

Plenty of tools

OFFICE OF THE INFORMATION COMMISSIONER

THE OFFICE OF THE DATA PROTECTION COMMISSIONER

GENERAL DA

SELF-ASSE

12/27/2001

GDPR Questionnaire

GDPR Ready? Take our Questionnaire

ill appear automatically at the foot of the page. Please be sure to answer all

pointed a Data Protection Officer (DPO)? Yes No

GDPR? Yes No

Yes No

Yes No

Yes No

Protection Yes No

it consent Yes No

managing Yes No

subject data access requests?

[click here for more]

Have processes been developed to allow individuals to amend or delete their personal data? Yes No

[click here for more]

Have data retention and destruction procedures been reviewed for all data (including offline) as used by your organisation? Yes No

[click here for more]

Have you re-assessed your suppliers and supplier contracts in relation to the GDPR? Yes No

Classic GDPR readiness approach….and its consequences

- Legal layer
  - “Lets review our Ts&Cs, consent and make sure we are covered from legal perspective”
  - And why is that important?

- Process layer
  - Let’s hire EY, KPMG, PWC, Accenture you name it… to get proper data management process description and book of conduct
  - And why it is useless?

Finally…

- IT layer
  - 20 years of data protection legislation
  - Audit based compliance
  - Snapshot based data repository

2 key concepts

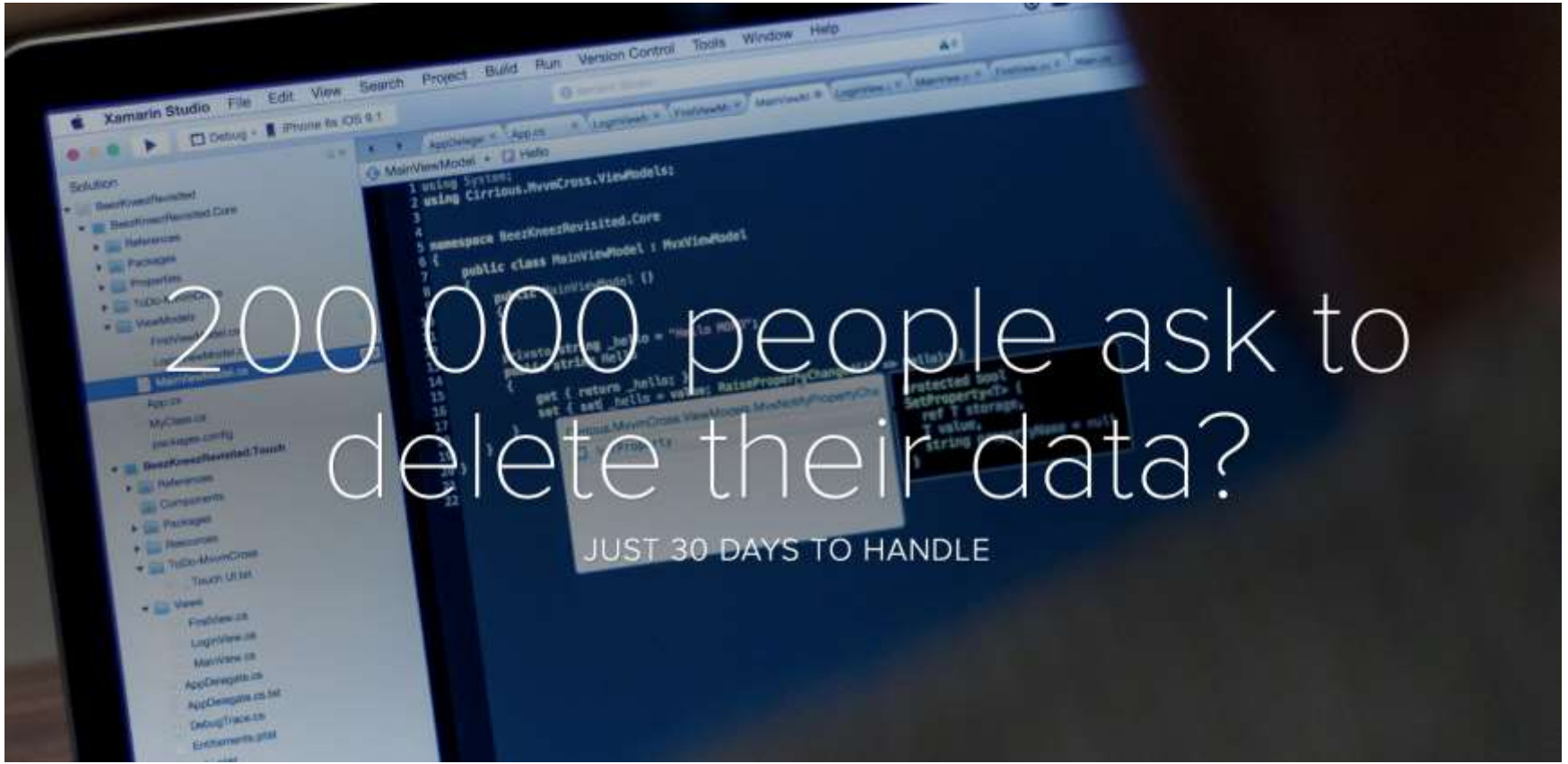
Data dynamics

Typical example: „Anna, could you quickly send me an extract of our customers emails for marketing campaign I plan to run? Oh its that late? Ok – send it to my Dropbox account.”

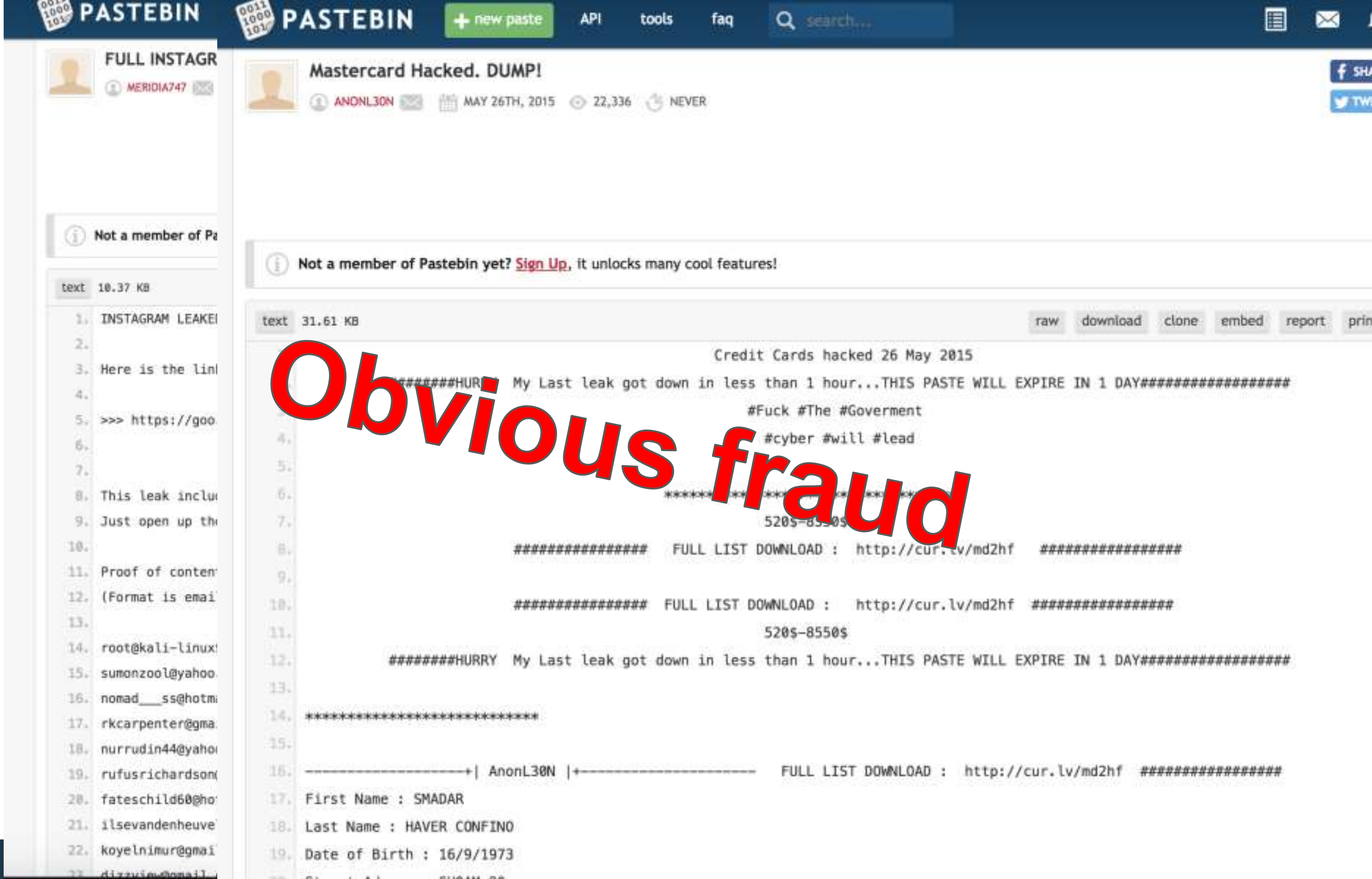
Data entropy

Nothing is typical here – yet here is the story…

Real life consequences – data access, data move

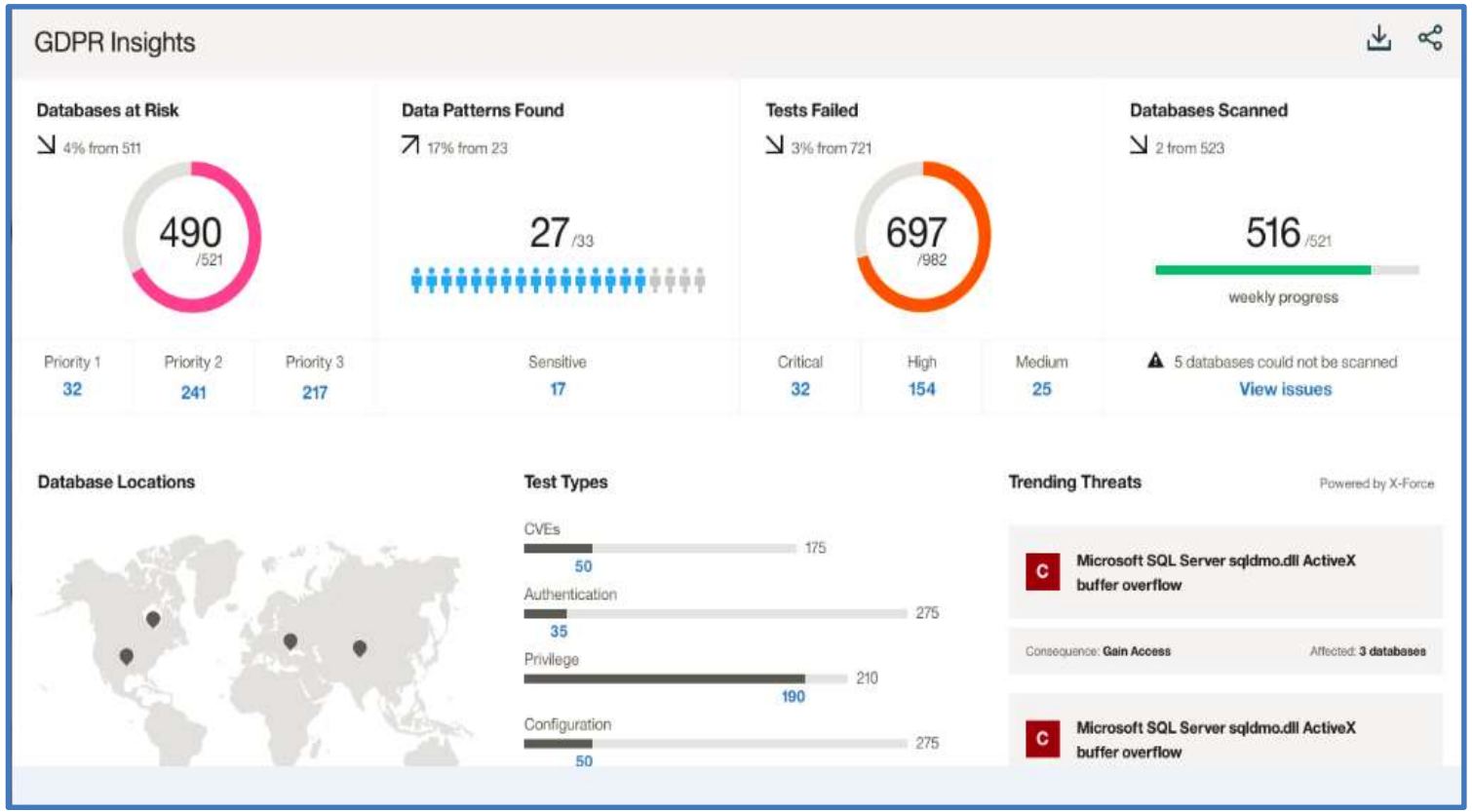


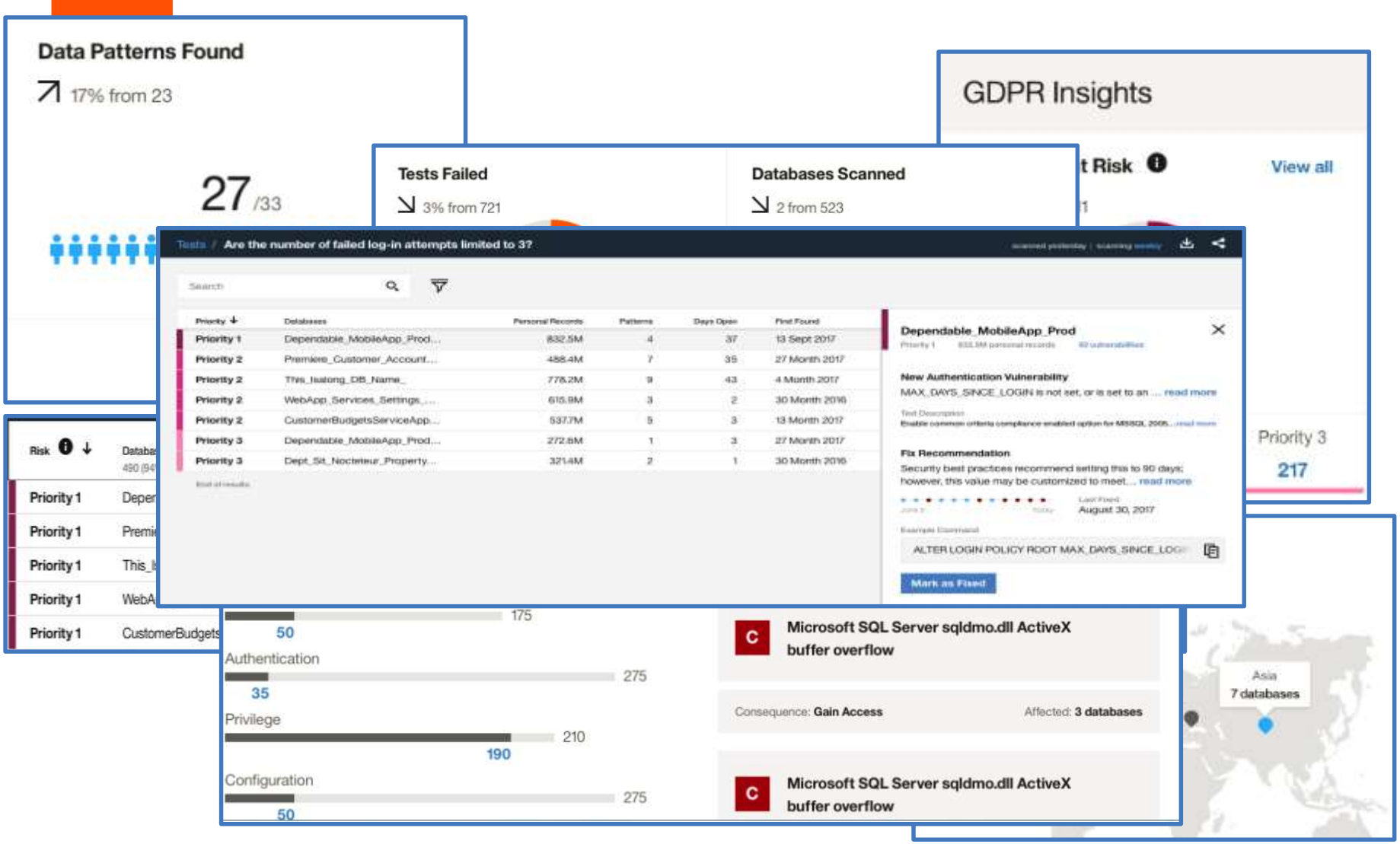
Real life consequences – data exfiltration


Obvious fraud
PASTEBIN
PASTEBIN
new paste
API
tools
faq
FULL INSTAGR
MERIDIA747
Mastercard Hacked. DUMP!
ANONL30N
MAY 26TH, 2015
22,336
NEVER
SHAR
TWEE
Not a member of Pa
Not a member of Pastebin yet? Sign Up, it unlocks many cool features!
text 10.37 KB
text 31.61 KB
raw
download
clone
embed
report
print
INSTAGRAM LEAKE
Here is the lin
>>> https://goo
This leak inclu
Just open up th
Proof of conten
(Format is emai
root@kali-linux
sumonzool@yahoo
nomad___ss@hotm
rkcarpenter@gma
nurrudin44@yaho
rufusrichardson
fateschild60@ho
ilsevandenheuve
koyelnimur@gmai
Credit Cards hacked 26 May 2015
#Fuck #The #Goverment
#cyber #will #lead
520-8550
################ FULL LIST DOWNLOAD : http://cur.lv/md2hf ################
520-8550
#######HURRY My Last leak got down in less than 1 hour...THIS PASTE WILL EXPIRE IN 1 DAY##################
****
---------------------+| AnonL30N |+--------------------- FULL LIST DOWNLOAD : http://cur.lv/md2hf ################
First Name : SMADAR
Last Name : HAVER CONFINO
Date of Birth : 16/9/1973

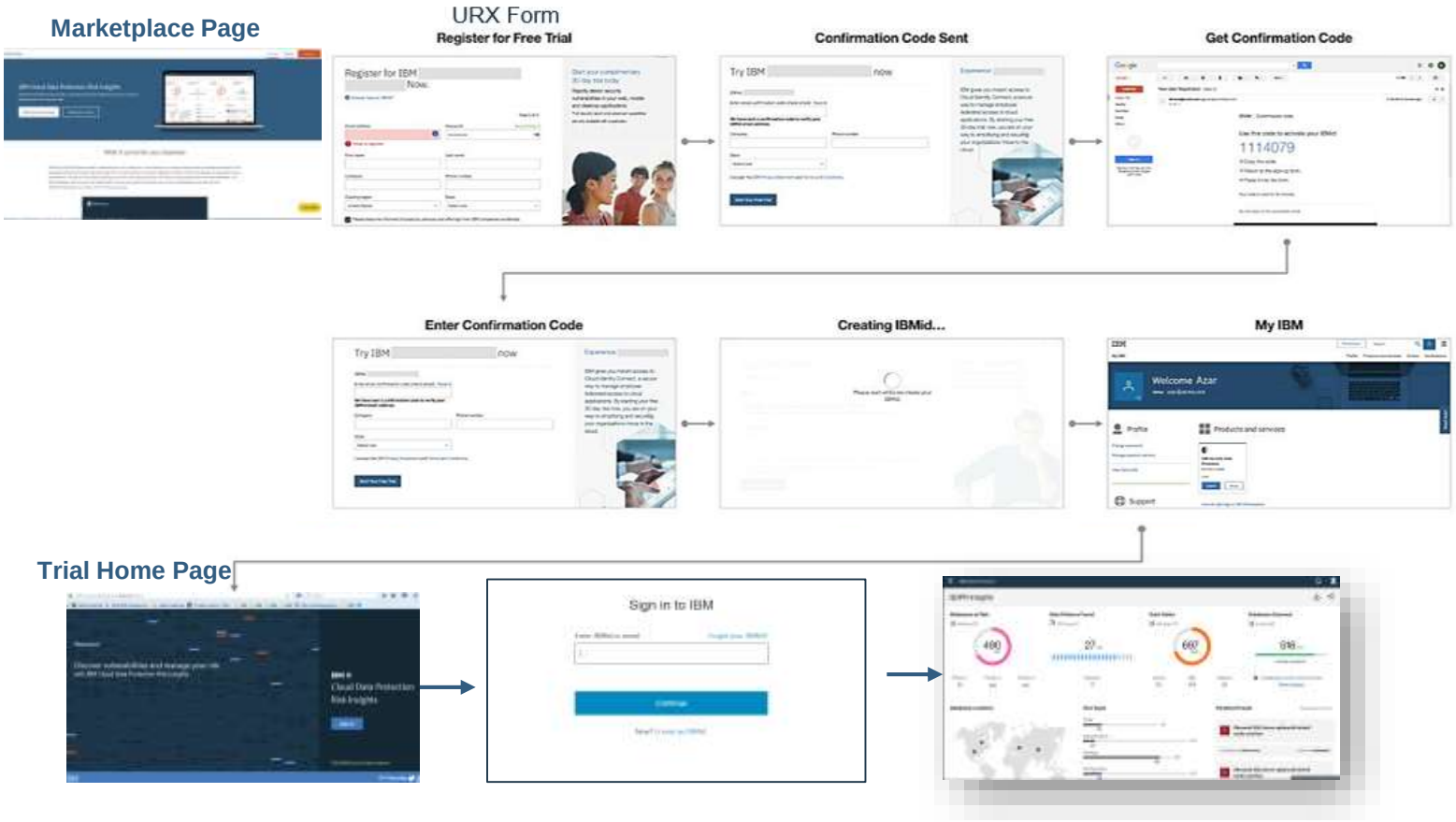
What if…

You could: Find GDPR-relevant data. Uncover risks. Take action.

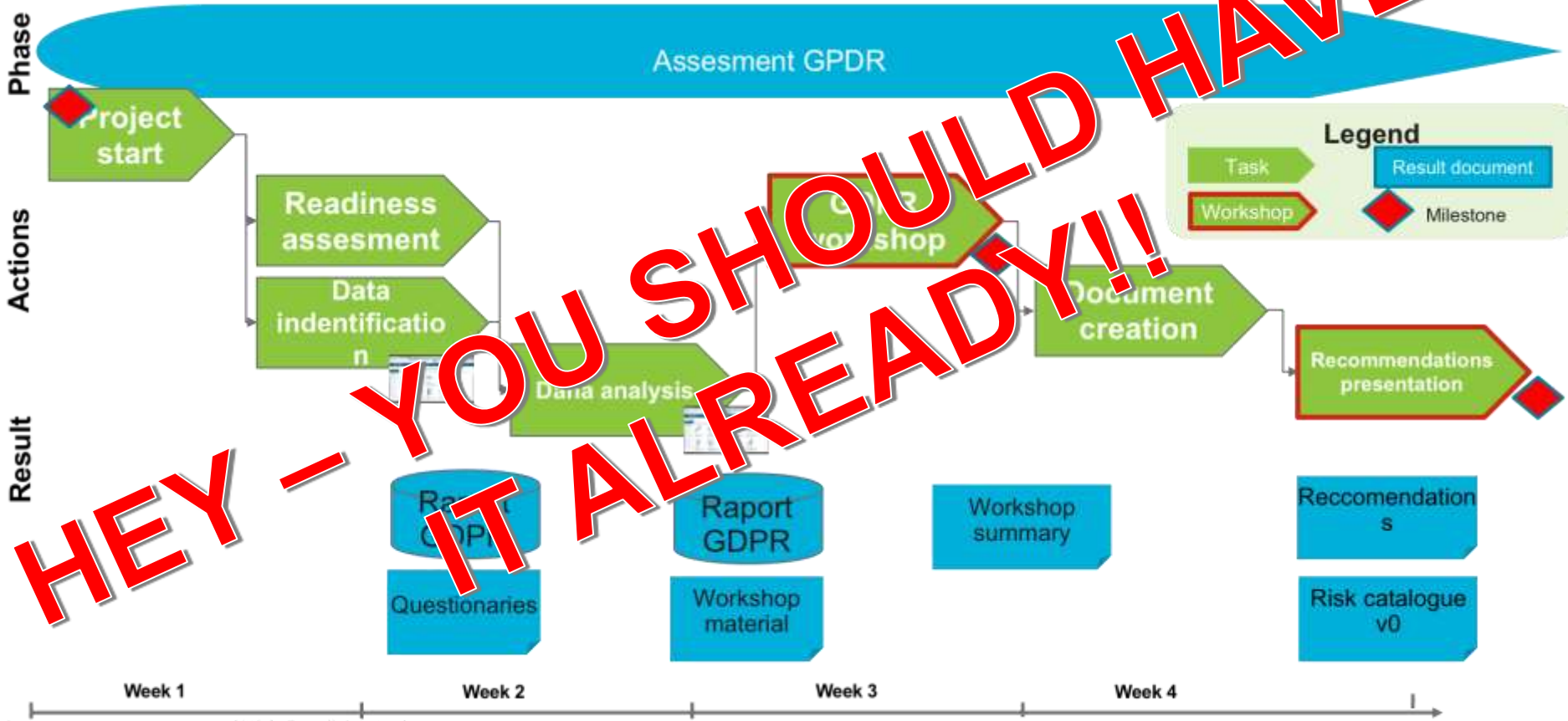



Data Patterns Found
17% from 23
27 /33
GDPR Insights
t Risk
View all
Tests Failed
3% from 721
Databases Scanned
2 from 523
Tests / Are the number of failed log-in attempts limited to 3?
Search
Priority
Databases
Personal Records
Patterns
Days Open
First Found
Priority 1 Dependable_MobileApp_Prod... 832.5M 4 37 13 Sept 2017
Priority 2 Premiere_Customer_Account... 488.4M 7 35 27 Month 2017
Priority 2 This_Isalong_DB_Name_ 778.2M 9 43 4 Month 2017
Priority 2 WebApp_Services_Settings_... 615.9M 3 2 30 Month 2016
Priority 2 CustomerBudgetsServiceApp... 537.7M 5 3 13 Month 2017
Priority 3 Dependable_MobileApp_Prod... 272.6M 1 3 27 Month 2017
Priority 3 Dept_Sit_Nocteleur_Property... 321.4M 2 1 30 Month 2016
Dependable_MobileApp_Prod
New Authentication Vulnerability
MAX_DAYS_SINCE_LOGIN is not set, or is set to an .... read more
Fix Recommendation
Security best practices recommend setting this to 90 days; however, this value may be customized to meet.... read more
August 30, 2017
ALTER LOGIN POLICY ROOT MAX_DAYS_SINCE_LOG
Mark as Fixed
Risk
Priority 1
Priority 1
Priority 1
Priority 1
Priority 1
Priority 3
217
175
50
Authentication
275
35
Privilege
210
190
Configuration
275
50
C
Microsoft SQL Server sqldmo.dll ActiveX buffer overflow
Consequence: Gain Access
Affected: 3 databases
C
Microsoft SQL Server sqldmo.dll ActiveX buffer overflow
Asia
7 databases

- How can you get started?
  Sign up for our Free 30-Day Trial *(available starting June 5, 2018)*



Alternatively…



HEY – YOU SHOULD HAVE IT ALREADY!!!

CONTACT US!

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM