e-BUSINESS & SOCIAL MEDIA WORLD CONFERENCE 2018

SECURITY, PERFORMANCE AND GDPR COMPLIANCE MANAGEMENT

Konstantinos Kanavidis, Information Security Consultant
DEVOQ TECHNOLOGY, kkan@devoq.gr

Few words about us

DEVOQ Technology

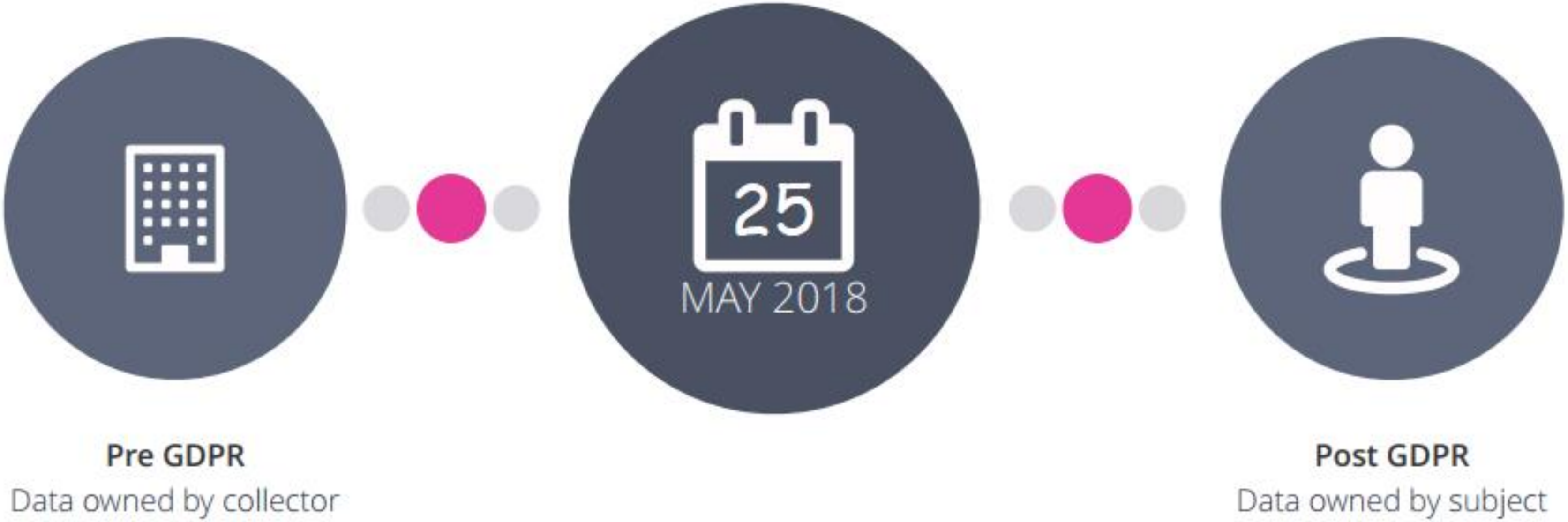
Started on 2014
Telecom background, 15 years of experience

- Cyber Security Engineering
- Security Consulting & Audits
- Penetration Testing

Small team, technically focused

General Data Protection Regulation

Fundamental change of data ownership



25

MAY 2018

Pre GDPR
Data owned by collector

Post GDPR
Data owned by subject

GDPR: Technical and organizational measures

- Organizational: e.g. limiting the number of people who can access personal data
- Technical: e.g. use encryption to protect accidental data loss

GDPR: Technical and organizational measures

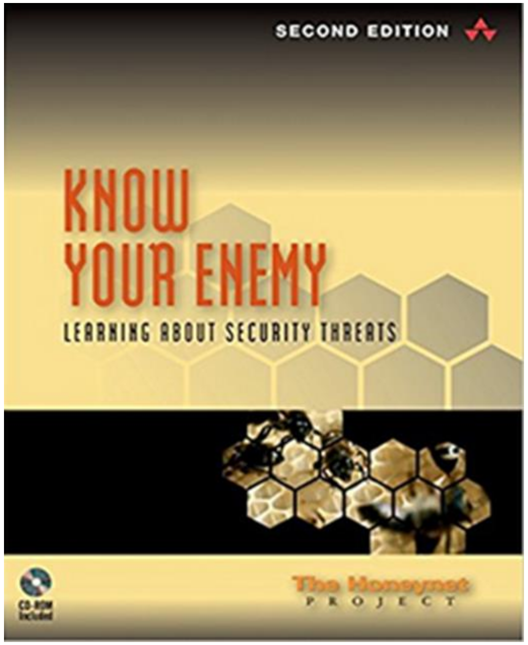
- Ensure that the chance of a data breach is minimized
- Ensure that data is kept safe

Does not mandate the exact security measures

Problem definition – Data breach

Hacking for:

- Fun
- Profit
- Vandalism
- Information leakage
- State sponsored



Know your enemy

How is a data breach possible?

Vulnerabilities: A weakness allowing an attacker to reduce a system's information assurance.

Human error

Usually a software bug:

Software bugs

- Not a new problem

- 1996: European Space Agency’s 1 Billion USD prototype rocket “Ariane 5” crashed because of a software bug on the onboard computer.
- 2014 Toyota recalls 600K Prius cars because of a software bug shutting down the engine.

Vulnerabilities exploit software bugs

Data Breach Examples

Yahoo (2013): 3 billion user accounts (was thought initially to be 1 billion)

- Names
- Dates of birth
- Email addresses
- Security questions and answers
- Weakly protected passwords

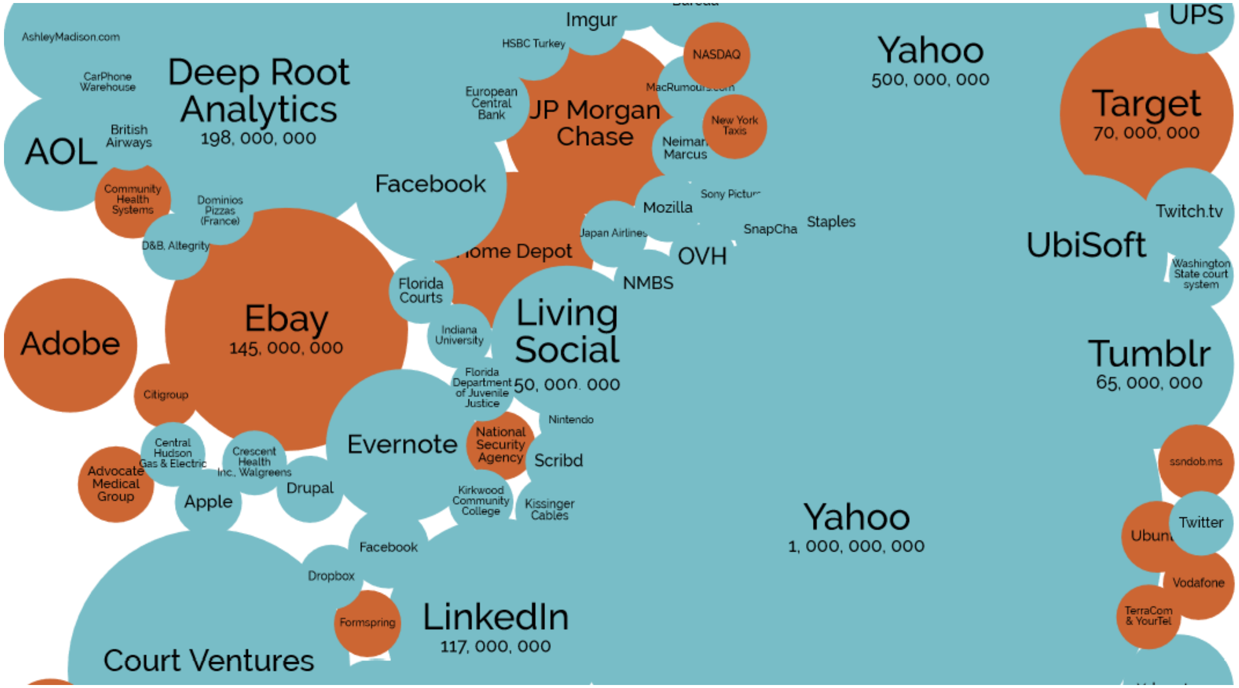
Took years to discover!

Data Breach Examples

- FriendFinder (2016): 412 million accounts
- MySpace (date unknown): 360 million accounts
- LinkedIn (2012): 165 million accounts
- Playstation Network (2011): 102 million accounts
- Dropbox (2012): 68 million accounts

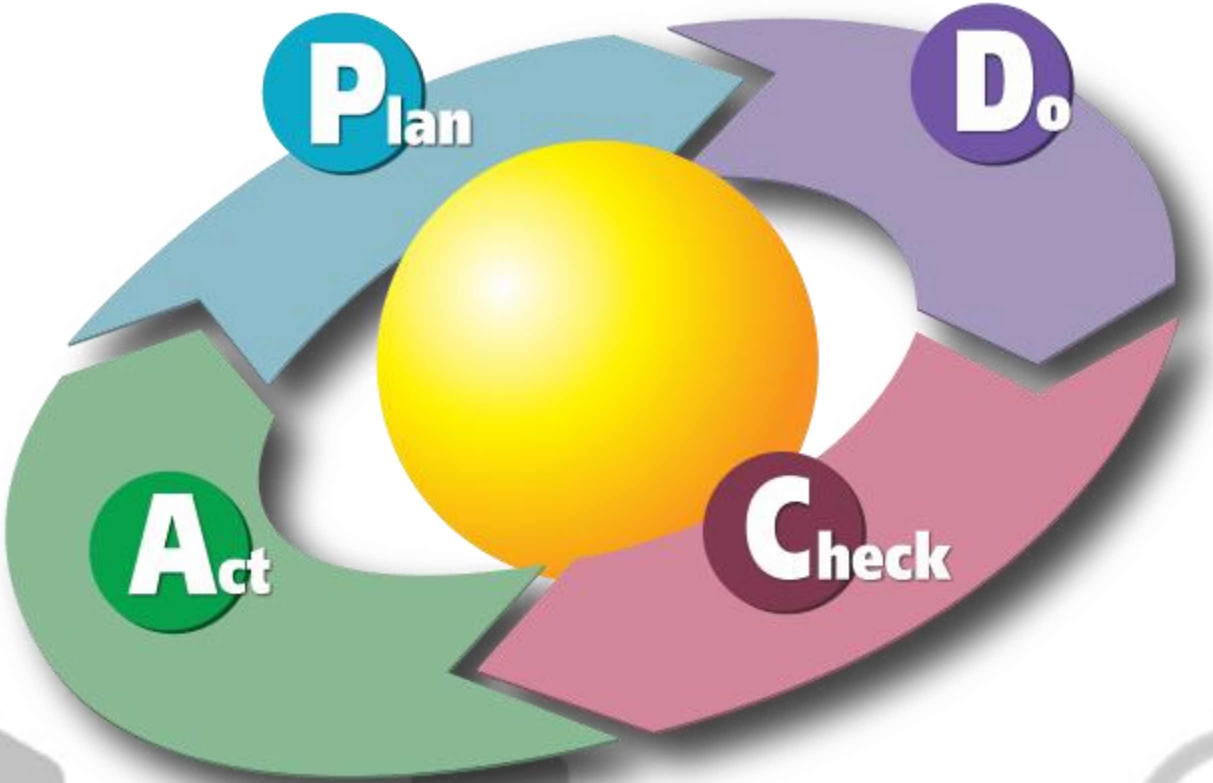
LinkedIn breach prompted Netflix to take actions (change matching passwords)

Data Breach Examples



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

What to do



Plan

- Security policies and procedures
- Architecture diagrams
- IT inventory
- Workflows & ticketing

Do

- Physical access (e.g. access cards)
- Logical access (e.g. user directory)
- Remote access (e.g. VPNs)
- Network security/Firewalls
- Antivirus/Sandbox
- Redundant systems
- Hardening
- Backups
- Data Classification, Data Loss Prevention
- Logging & monitoring

Check

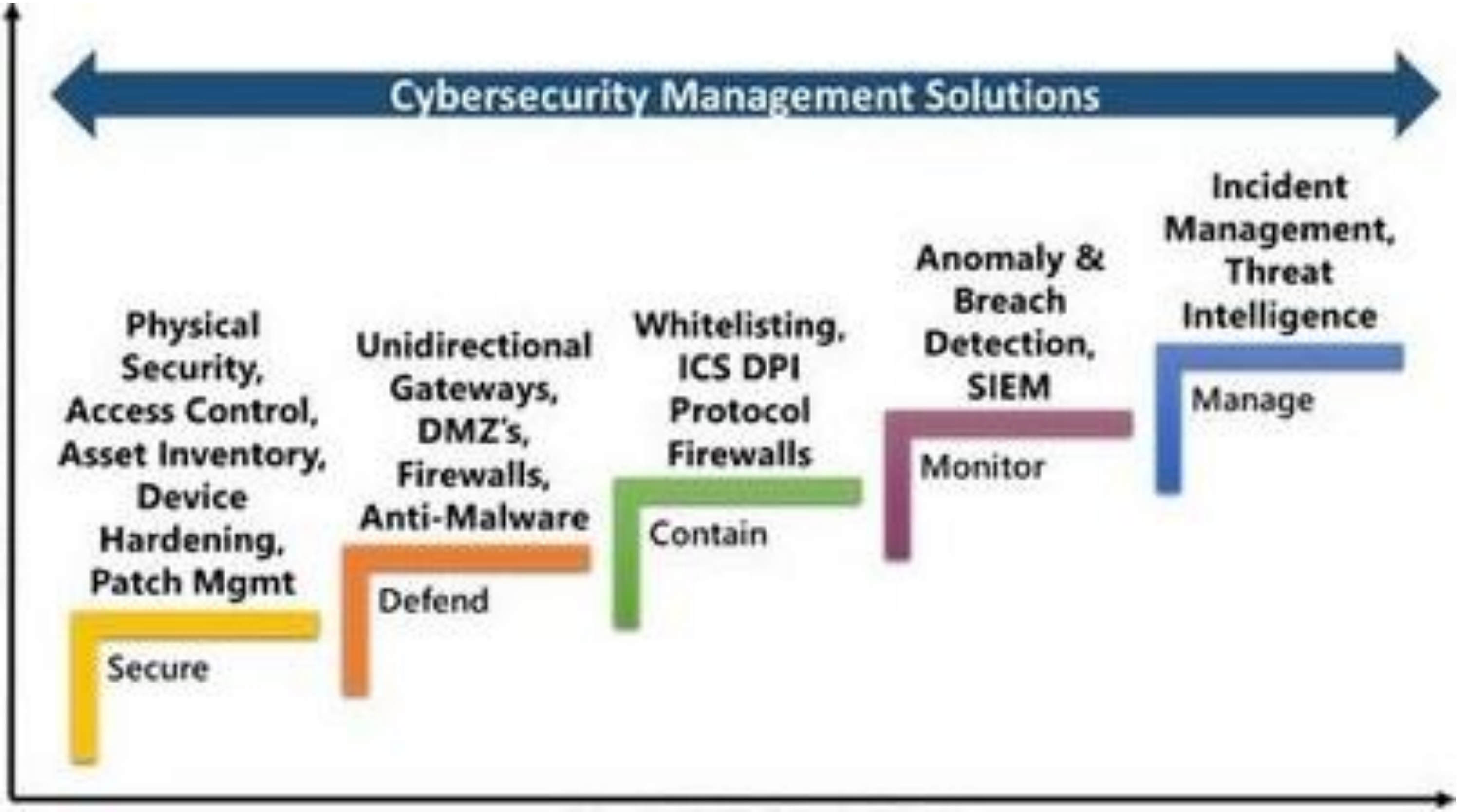
- Regular audits
- Gap analysis
- Vulnerability/penetration tests

Act

- Information security officer
- Information security department
- External consultants / experts

… and Data Protection Officer

Organization maturity



Cybersecurity Management Solutions

Physical Security, Access Control, Asset Inventory, Device Hardening, Patch Mgmt

Secure

Unidirectional Gateways, DMZ's, Firewalls, Anti-Malware

Defend

Whitelisting, ICS DPI Protocol Firewalls

Contain

Anomaly & Breach Detection, SIEM

Monitor

Incident Management, Threat Intelligence

Manage

Incident handling

- Communication plan (72 hours or without undue delay)
- Policies, procedures, key personnel
- Diagnosis, Escalation, Investigation, Resolution
- Automated system if possible

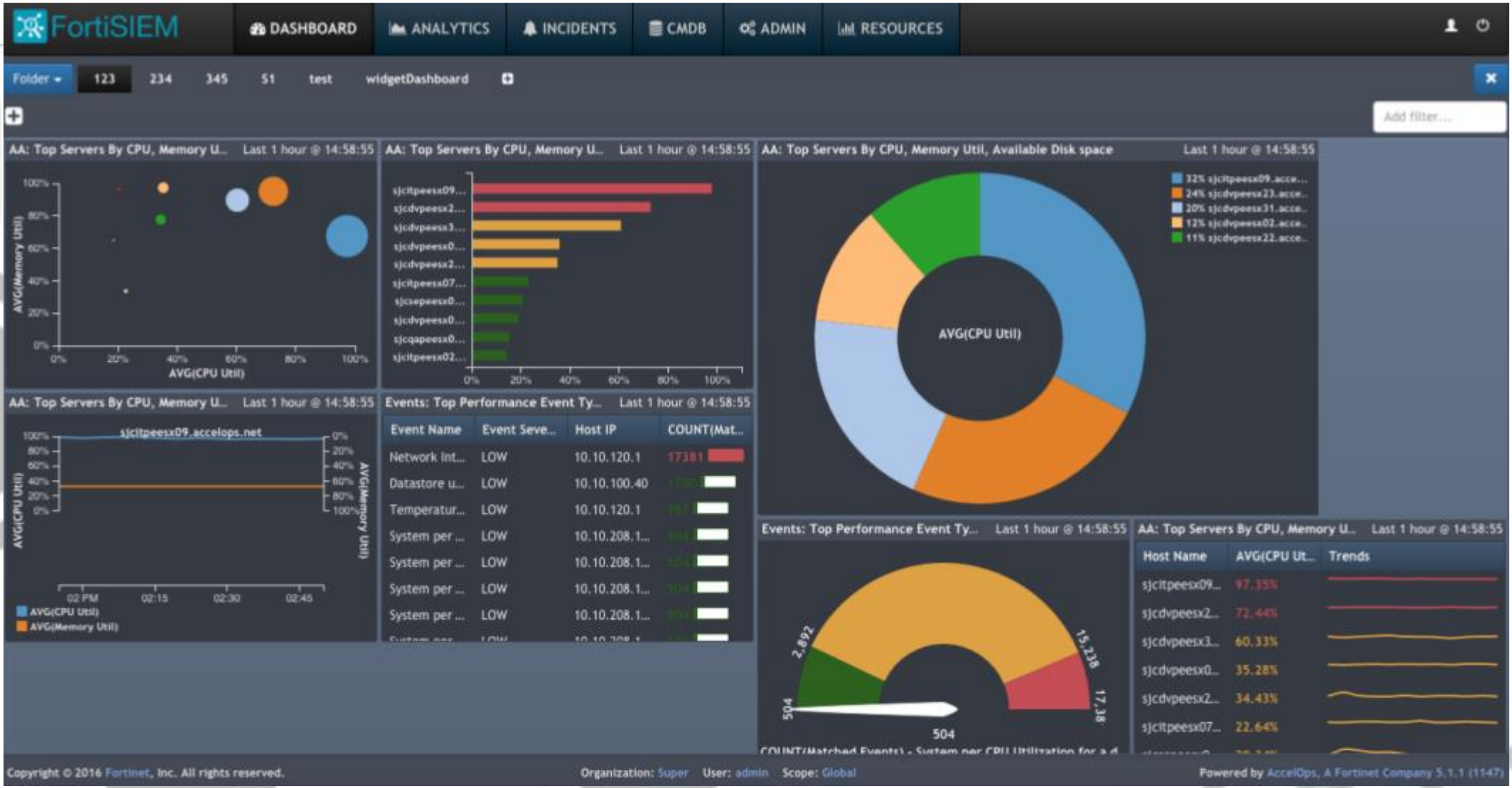
Be able to demonstrate that appropriate security controls were in place

Incident handling

- Quick response can limit the exposure
- Unified threat detection controls can provide the speed required
- Infrastructure & Security monitoring is important

Audit logs and investigation will determine if reporting is required under GDPR

Infrastructure & Security monitoring



Events: Top Performance Event Ty... Last 1 hour @ 14:58:55

Event Name	Event Seve...	Host IP	COUNT(Mat...
Network Int...	LOW	10.10.120.1	17381
Datastore u...	LOW	10.10.100.40	[illegible]
Temperatur...	LOW	10.10.120.1	[illegible]
System per ...	LOW	10.10.208.1...	504
System per ...	LOW	10.10.208.1...	504
System per ...	LOW	10.10.208.1...	504
System per ...	LOW	10.10.208.1...	504

AA: Top Servers By CPU, Memory U... Last 1 hour @ 14:58:55

Host Name	AVG(CPU Ut...	Trends
sjcitpeesx09...	97.35%	
sjcdvpeesx2...	72.44%	
sjcdvpeesx3...	60.33%	
sjcdvpeesx0...	35.28%	
sjcdvpeesx2...	34.43%	
sjcitpeesx07...	22.64%	

Copyright © 2016 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global Powered by AccelOps, A Fortinet Company 5.1.1 (1147)

Infrastructure & Security monitoring

- Real-Time Analytics
- Security and Compliance
- Single Pane of Glass
- Performance monitoring

Automation

Best practices

- ISO 27000, international standard with worldwide recognition, applies to any organization
- PCI-DSS, data security for the credit card industry, usually obligatory

Security standards already exist

ISO 27000

- International Standards Organization
- Corporate security standard
- Originally donated by Shell to a UK government initiative in the early 1990s
- C-I-A Principle
  - Confidentiality (unauthorized disclosure)
  - Integrity (accuracy of data)
  - Availability (available when needed)

ISO 27000

- Information security policies
- Asset management
- Physical security
- Communications security
- Access control
- Incident management
- Business continuity

ISO 27000

- Operational security
  - Change management
  - Malware protection
  - Backup
  - Logging
  - Monitoring
  - Vulnerability management

PCI-DSS

- Payment Card Industry Data Security Standard
- Five different policies aligned to create 2004 PCI version 1.0
  - VISA cardholder information security program
  - MasterCard site data protection
  - American Express data security operating policy
  - Discover information security and compliance
  - JCB data security program

PCI-DSS

- Build and maintain a secure network and systems
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

Many similarities with ISO 27000

DEVOQ
TECHNOLOGY

IT Manager: Do you know a good GDPR specialist?
IT Consultant: Yes, in fact I do!
IT Manager: Can you give me his email?
IT Consultant: No…

Thank you