THE GENERAL DATA PROTECTION REGULATION AND WHAT IT MEANS FOR YOUR BUSINESS

metaphorit

AGENDA

- Welcome!
- Introductions
- Metaphor IT – What is GDPR?
- Thales e-security – Encryption
- LogRhythm – Security Information and Event Management
- Q&A

GDPR – THE DETAILS AND SCOPE

The EU *General Data Protection Regulation* was agreed upon on April 14th, 2016

Demands compliance by May 25th 2018

Simplifies regulatory environment for organisations in the EU

Designed to strengthen and unify data protection for individuals in the EU

GDPR – THE DETAILS AND SCOPE

This means that no matter where an organisation is based…

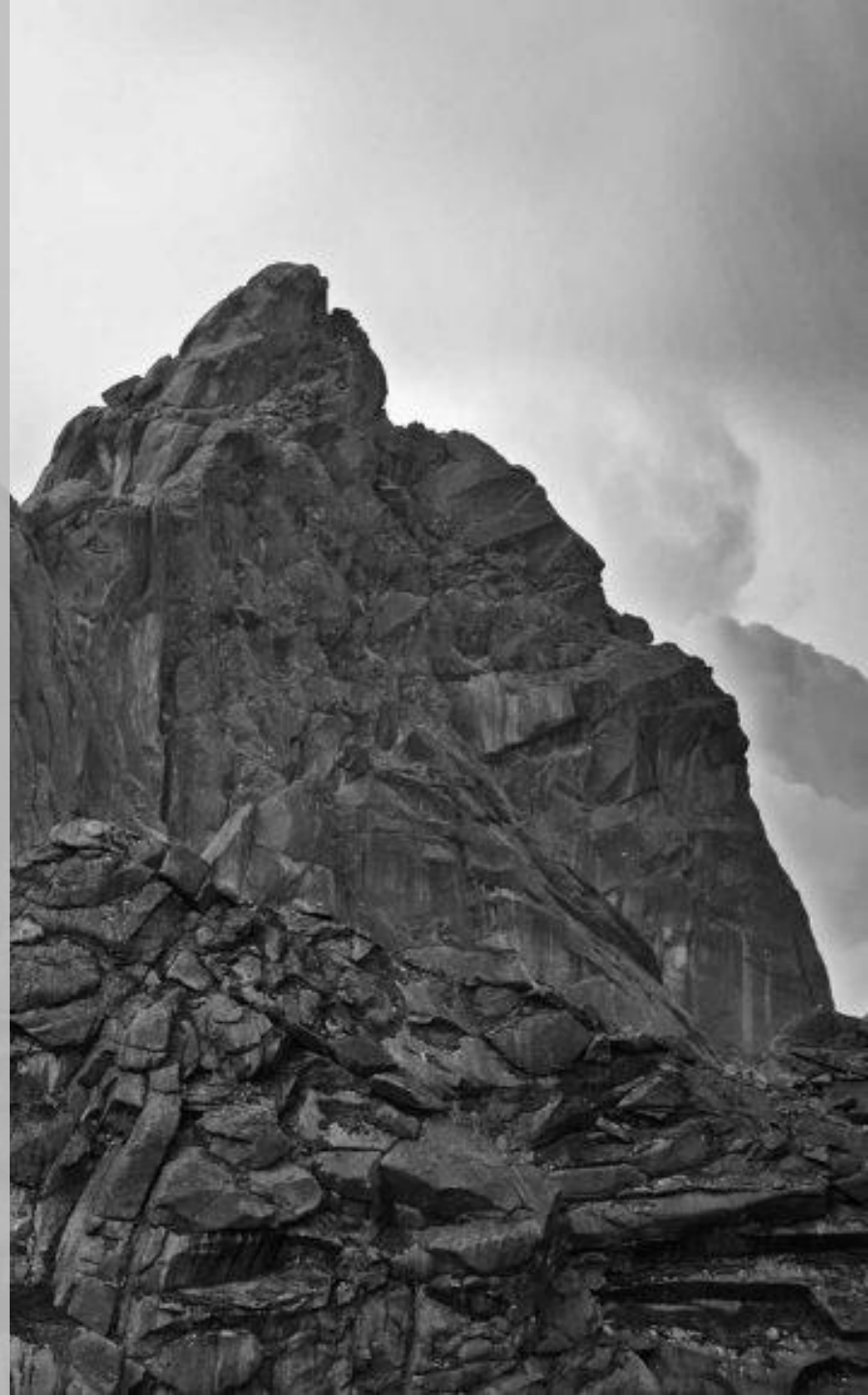
…if you do business **in the EU**, you are subject to GDPR.

GDPR – THE DETAILS AND SCOPE

According to the European Commission "personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

WHY THE CHANGE IN LEGISLATION?

- The IT Landscape has changed drastically since 1995
- Mobile Devices for corporate email and data
- BYOD – Work from anywhere at any time
- Erosion of traditional IT security perimeter
- Increase of cyber criminals



What are people talking about?

Fines of £16million or 4% of your global turnover

WHAT ARE COMPANIES DOING?

PREPARING FOR GDPR – THE 12 STEPS

ico. Information Commissioner's Office

1 Awareness

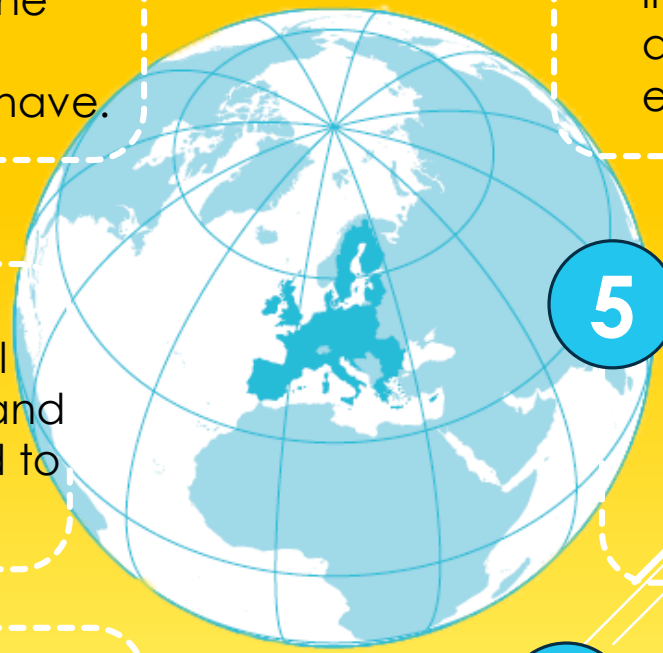
Decision makers and key people in your organisation need to be aware that the law is changing to the GDPR and appreciate the impact this is likely to have.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.



4 Individuals' rights

Procedures to ensure they cover the rights individuals have, including how you would delete personal data or provide it electronically, in a commonly used format.

5 Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

PREPARING FOR GDPR – THE 12 STEPS

ico. Information Commissioner's Office

7 Consent

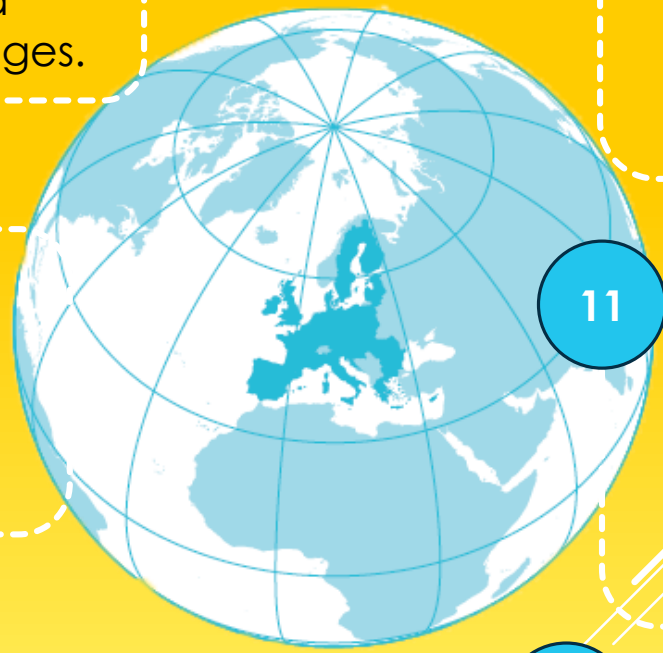
You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8 Children

Start thinking now about putting systems in place to verify individuals' ages and to gather consent for the data processing activity.

9 Data Breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.



10 Data Protection by Design and Data Protection Impact Assessments

Familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11 Data Protection Officer

Designate a DPO, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

12 International

If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

WHAT SHOULD WE BE DOING?

Ownership

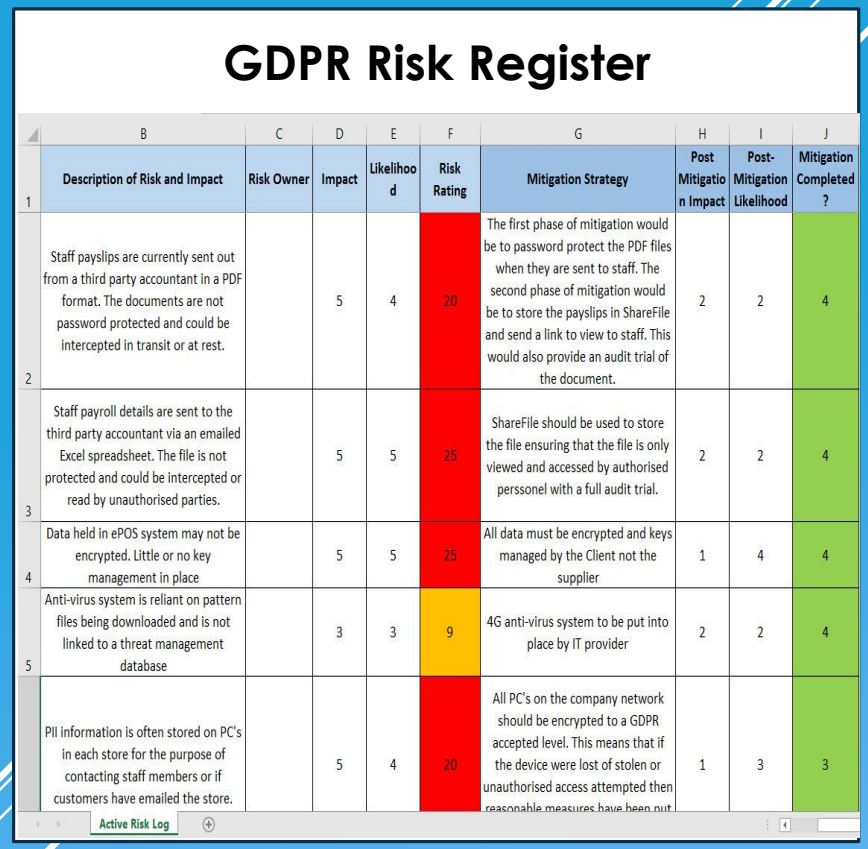
- Appoint a DPO
- Create a GDPR board who meet regularly

Analyse

- Start with your DPA processes and procedures
- Gap analysis/Readiness Assessment
- Create a risk register
- Where is data, how is it controlled?

Design

- Create a design of where you need to be
- Create the roadmap to get there with milestones
- Emphasis on protection by design – Encrypt everything
- Put tools in place to detect potential breaches
- Processes and procedures - MIT



GDPR Risk Register

	B	C	D	E	F	G	H	I	J
1	Description of Risk and Impact	Risk Owner	Impact	Likelihood	Risk Rating	Mitigation Strategy	Post Mitigation Impact	Post-Mitigation Likelihood	Mitigation Completed ?
2	Staff payslips are currently sent out from a third party accountant in a PDF format. The documents are not password protected and could be intercepted in transit or at rest.		5	4	20	The first phase of mitigation would be to password protect the PDF files when they are sent to staff. The second phase of mitigation would be to store the payslips in ShareFile and send a link to view to staff. This would also provide an audit trial of the document.	2	2	4
3	Staff payroll details are sent to the third party accountant via an emailed Excel spreadsheet. The file is not protected and could be intercepted or read by unauthorised parties.		5	5	25	ShareFile should be used to store the file ensuring that the file is only viewed and accessed by authorised perssonel with a full audit trial.	2	2	4
4	Data held in ePOS system may not be encrypted. Little or no key management in place		5	5	25	All data must be encrypted and keys managed by the Client not the supplier	1	4	4
5	Anti-virus system is reliant on pattern files being downloaded and is not linked to a threat management database		3	3	9	4G anti-virus system to be put into place by IT provider	2	2	4
	PII information is often stored on PC's in each store for the purpose of contacting staff members or if customers have emailed the store.		5	4	20	All PC's on the company network should be encrypted to a GDPR accepted level. This means that if the device were lost of stolen or unauthorised access attempted then reasonable measures have been put	1	3	3

Active Risk Log

WHAT SHOULD WE BE DOING?

Deploy
- Allocate tasks

Awareness
- Top level
- Staff
- Clients

Review
- Constant review
- Continual Security Improvement Plan

Documentation
- Greater emphasis on ability to demonstrate accountability

THALES

GDPR and protecting data

Ian Greenwood, Regional Sales Manager

Thales e-Security

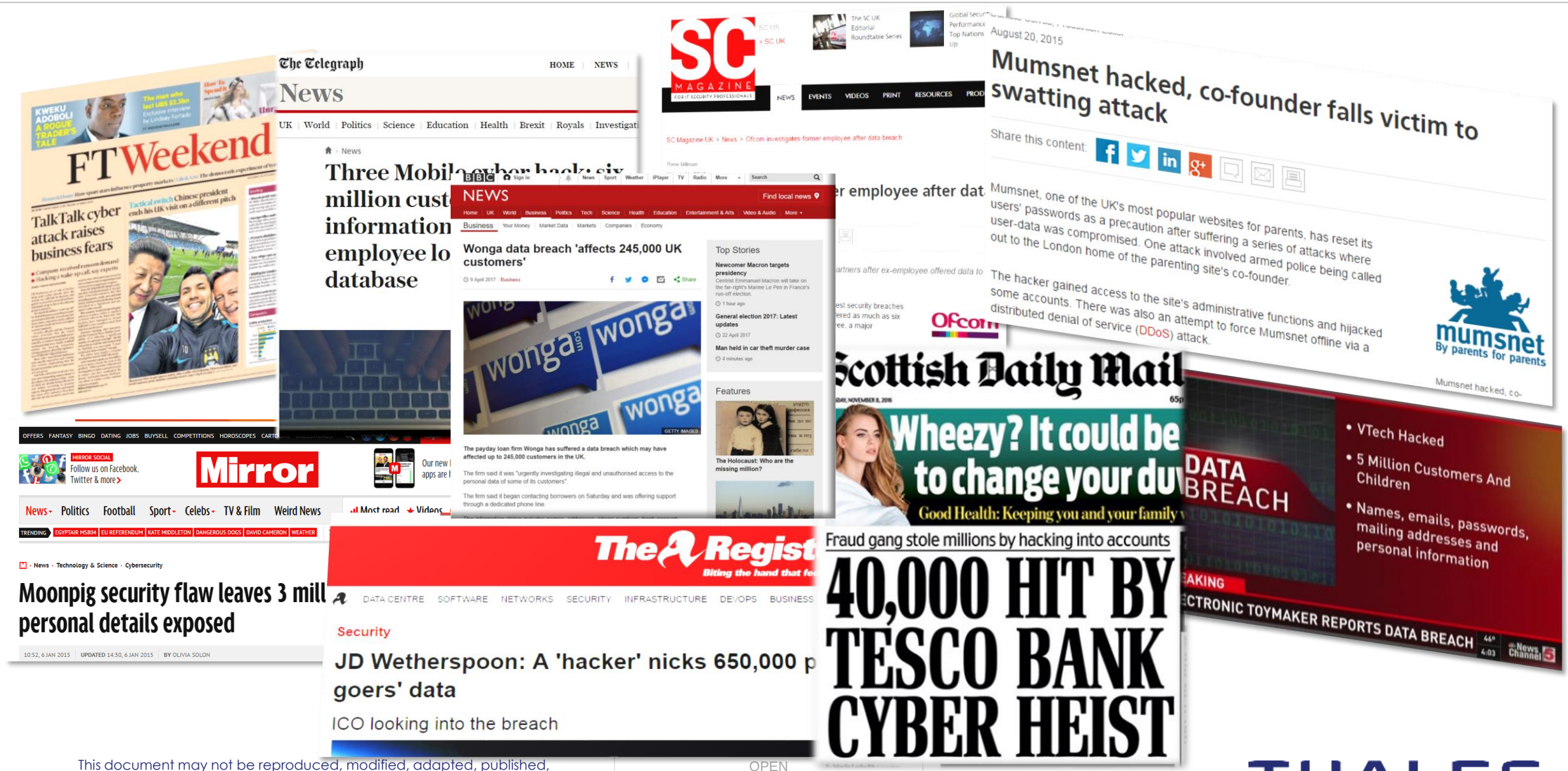
Discussion Points

- Digital Transformation – an epidemic rise
- Key security considerations for GDPR
- Customer case study
- Q&A

A CHANGE OF PARADIGM

- Threat anticipation
- Cybersecured by design
- Data is the new perimeter
- Digital Transformation

The Impact of Being Breached



THALES

Breaches and lost data

Data Lost or Stolen Since 2013

Breach Level Index as taken on 1st May 2017
(a rise of 2 billion from 23rd Feb 2017.)
www.breachlevelindex.com

Your Reputation is At Risk

Thales Survey was conducted by Wakefield Research (www.wakefieldresearch.com) among 1,023 nationally representative UK adults ages 18+, between September 22 and September 28, 2016, using an email invitation and an online survey.

GDPR Requires Stronger Data Protection

Protecting private data will be more critical than ever

- New restrictions around the collection, retention and disclosure of personal data
- More scrutiny of the users and applications that have access to private data

Substantial penalties & Requirements

- Orgs found in violation face penalties up to €20 million or 4% of annual worldwide revenues
- 72 Hours to report a data breach
- Assessment of data protection assessment

GDPR is focused on specific outcomes

How can Vormetric help?

1. GDPR Mandate: "..ensure appropriate data security through means including, among others, "pseudonymisation" and encryption of personal data."

- **Vormetric solution:** Tokenisation and Data Masking, VTE: Vormetric Transparent Encryption, Vormetric Key Management
- **Vormetric Benefit:** If the data is encrypted, it unintelligible to the cyber-criminal, therefore, a breach does not need to be notified to the authorities. In addition, with Vormetric key management, only those with appropriate authority can access the data.

2. GDPR Mandate: "all forms of data must be protected"

- **Vormetric solution:** VTE: Vormetric Transparent Encryption
- **Vormetric Benefit:** Vormetric encrypts both structured and unstructured data.

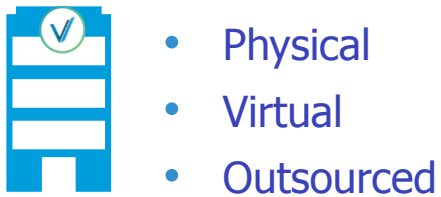
3. GDPR Mandate: "process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of data processing

- **Vormetric Solution:** Security Intelligence (e.g. LogRhythm
- **Vormetric Benefit: Produces** detailed security event logs easily integrated SIEM systems to produce security reports necessary for GDRP compliance. Logs include: an auditable trail of permitted and denied access attempts from users and processes, reports on unusual or improper data access, accelerate the detection of insider threats, hackers and the presence of advanced persistent threats (APT) that are past the perimeter security.

Slide No: 20

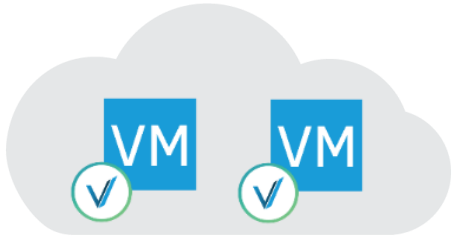
One Platform – One Strategy

Data-at-rest security that follows your data



- Physical
- Virtual
- Outsourced

Enterprise Data Centers



Private, Public, Hybrid Clouds
SaaS, PaaS, IaaS

Remote Servers

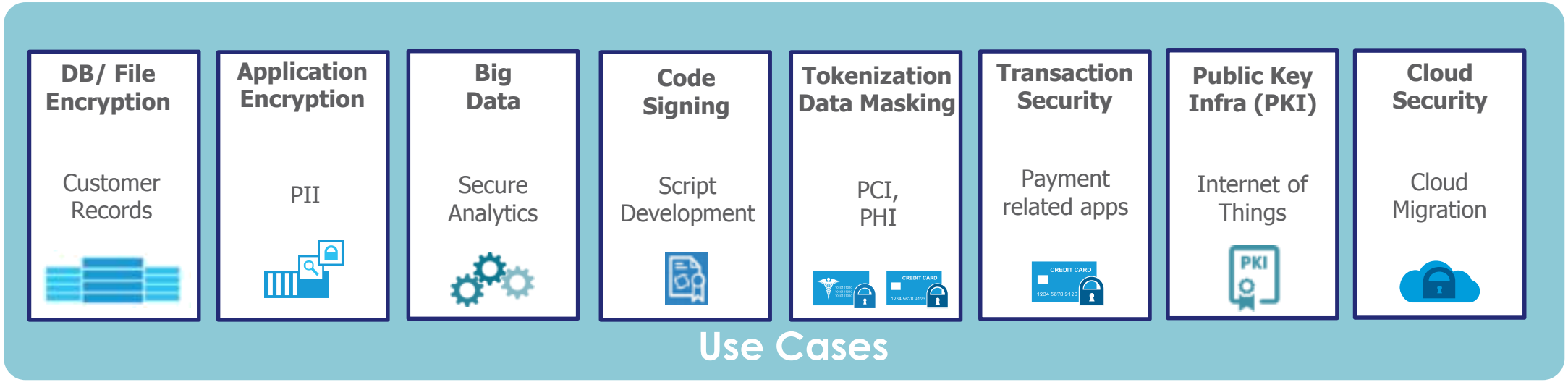
- Sources
- Nodes
- Analytics

Big Data

OPEN

THALES

This increased adoption has created encryption silos



$ + $ + $ + $ + $ + $ + $

Each use case requires individual infrastructure, management consoles and training

Complex • Inefficient • Expensive

Vormetric Transparent Encryption – How it works?

SIEM logs and alerts

Privileged Users
admin/backup

*$^!@#)(
-|"_}?$%-:>>

root SA

user

Approved Processes and
Authorised Users

John Smith
401 Main Street

Encrypted
& Controlled

Clear Text

Vormetric
File System
Agent Policy
And Key access

Allow/Block
Encrypt/Decrypt

User

Application

Database

File
Systems

Volume
Managers

Storage

Server

Policies and Keys

DSM

Vormetric
Data Security Manager
virtual or physical appliance

Big Data, Databases or Files

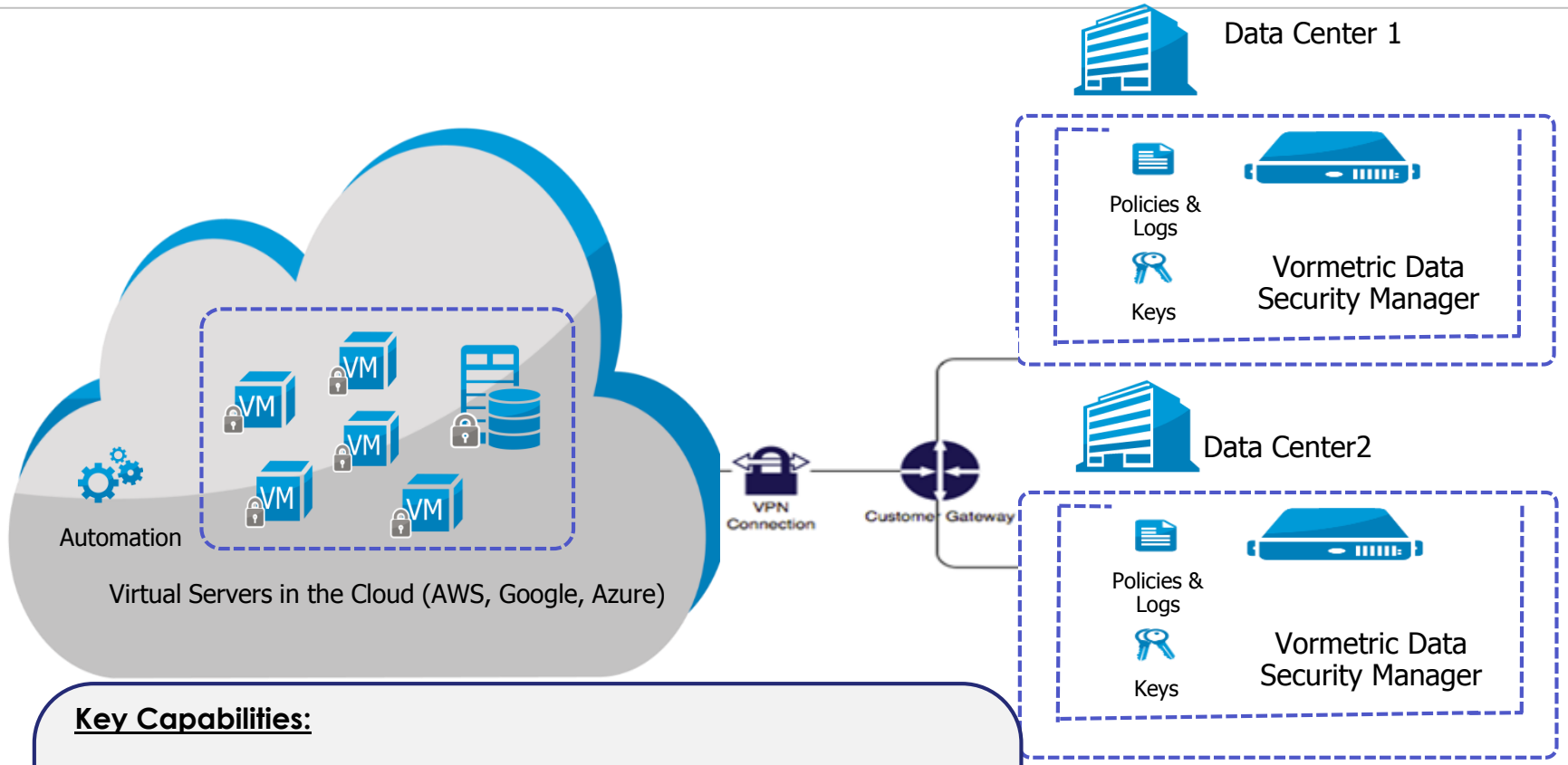
Encrypted

Cloud Admin, Storage
Admin, etc.

*$^!@#)(
-|"_}?$%-:>>

DIGITAL TRANSFORMATION – FINANCIAL SERVICES & DIGITAL PAYMENTS

Cloud Encryption Model



Key Capabilities:

- Data in cloud is "locked down" via encryption
- Ability to implement data access policies across private and hybrid cloud servers – block access or take away data visibility from cloud infrastructure admins
- Manage and control encryption keys on-premise
- Provide rich security intelligence around who/what is accessing protected data in the cloud

Summary

Digital transformation is coming

Proactive data defence must be the core of a digital transformation strategy

Best Practice approach:

- Encrypt Everything
- Establish Trust across platforms, supply chains and user
- Implement effective identity access management to data
- Ensure strong key management and protection

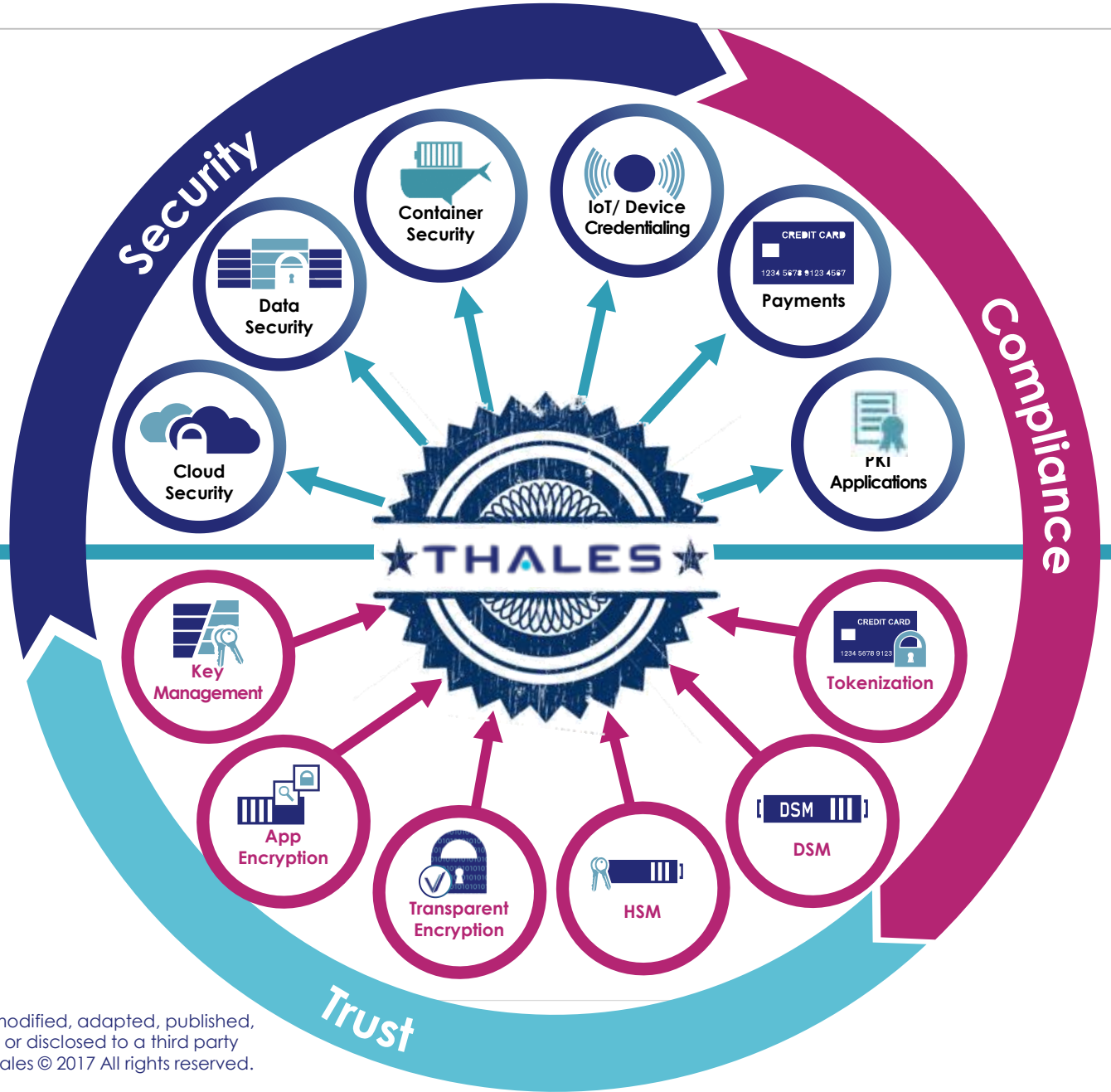
Next steps

- Free 2 hour initial consultation on your current architecture and how we can assist in meeting GDPR
- 5 day Thales GDPR assessment of your environment and report issued
- Free no-obligation POC to see how the Vormetric platform works in your environment
- Come and visit us at Infosecurity on June 6th-8th at Olympia – Stand C140

Thales eSecurity Solutions

Customer Use Cases

Thales Products/ Solutions



THALES

LogRhythm
The Security Intelligence Company

Faster Detection & Response - GDPR

RSM : Jodie Sikkel

SE : Lee Duff

How LogRhythm aligns with GDPR

- Data Breaches
  - LogRhythm has the toolset to:

Detect - SIEM

Report - Alarms and Reporting

Mitigate - SmartResponse

Investigate - Case Management and Forensics

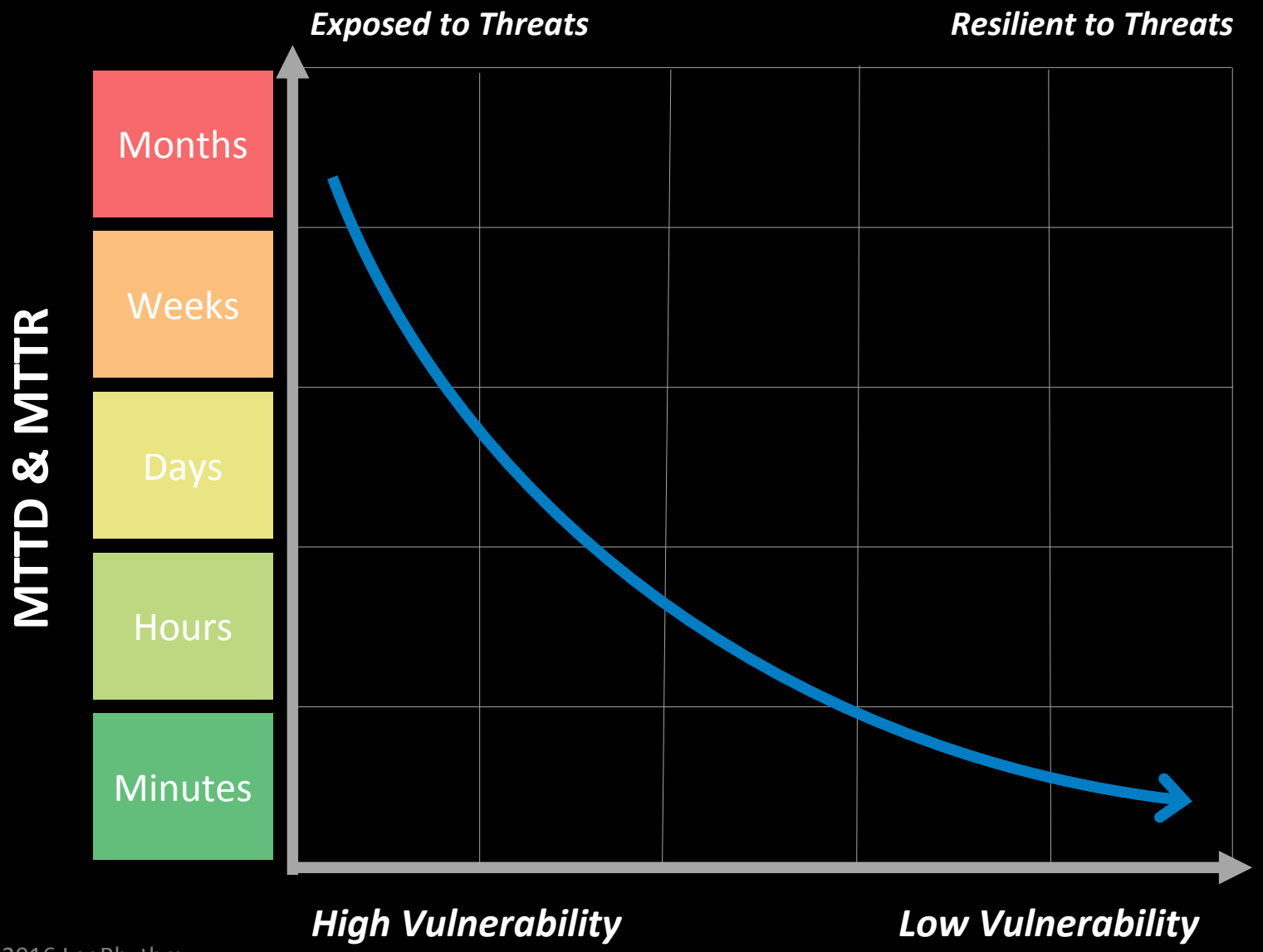
LogRhythm
The Security Intelligence Company

How LogRhythm aligns with GDPR

- Privacy By Design
  - Customers use LogRhythm to:
    - Address Proactive not reactive; Preventative not remedial requirements
    - Gain visibility into activity on corporate environment (end to end)
    - Pay particular attention to staff & systems that have access to Personally Identifiable Information (PII) data
    - Log all access to PII data
    - Demonstrate compliance with our compliance modules

LogRhythm
The Security Intelligence Company

Faster Detection & Response - GDPR



MEAN TIME TO DETECT (MTTD)
The average time it takes to recognize a threat requiring further analysis and response efforts

MEAN TIME TO RESPOND (MTTR)
The average time it takes to respond and ultimately resolve the incident

As organizations improve their ability to quickly detect and respond to threats, the risk of experiencing a damaging breach is greatly reduced

LogRhythm
The Security Intelligence Company

Obstacles To Faster Detection & Response

Alarm Fatigue

Swivel Chair Analysis

Forensic Data Silos

Fragmented Workflow

Lack of Automation

Effective

Threat Lifecycle Management

- ✓ Addresses these obstacles
- ✓ Enables faster detection and response to threats

LogRhythm®

The Security Intelligence Company

Our Approach

Forensic Data Collection | Discover | Qualify | Investigate | Neutralize | Recover

Explore Workshop, 14th June 2017

In this half-day technical workshop, you will have the opportunity to design security policies in a live environment. You will experience first-hand LogRhythm's ability to gain better visibility to potential cyber activity and detect, block and respond to cyber threats.

During this half-day workshop, you will:

- Investigate compromised user accounts
- Research security events and advanced persistent threats in a SIEM environment
- Automate immediate response to cyber incidents to reduce the risk of experiencing a material breach
- Learn how to calculate critical metrics such as Mean-Time-to-Detect™ (MTTD™) and Mean-Time-to-Respond™ (MTTR™) to measure the effectiveness of an organization's security capabilities

LogRhythm®
The Security Intelligence Company

WHAT CAN YOU DO NOW?

- [x] Obtain a free EU GDPR Readiness Assessment with Metaphor IT
- [ ] Fill out LogRhythm's Security Maturity Model Tool
- [ ] Create a GDPR Board to take ownership
- [ ] Ensure that adequate technical and organisational measures are put in place to protect data

THANK YOU!

- Feedback Forms
- LogRhythm – Explore Event
- Thales e-security – Free 2 Hour GDPR Workshop
- Follow Up Emails
- Any Questions?

Linkedin.com/company/metaphor-it

0333 003 3305

www.metaphor-it.co.uk

@MetaphorIT