



DATA LOSS RISK REDUCTION WITH DLP

Marcel van den Broek
Marcel.vandenbroek@e3benelux.eu
06-15827932
www.e3benelux.eu



- DLP Y/N
- Intellectual Property
- Patient data
- Client data
- Financial data



e³ REPRESENTATIVES



Marius van der Valk

Marius.vandervalk@e3benelux.eu

06-29526437

www.e3benelux.eu



Marcel van den Broek

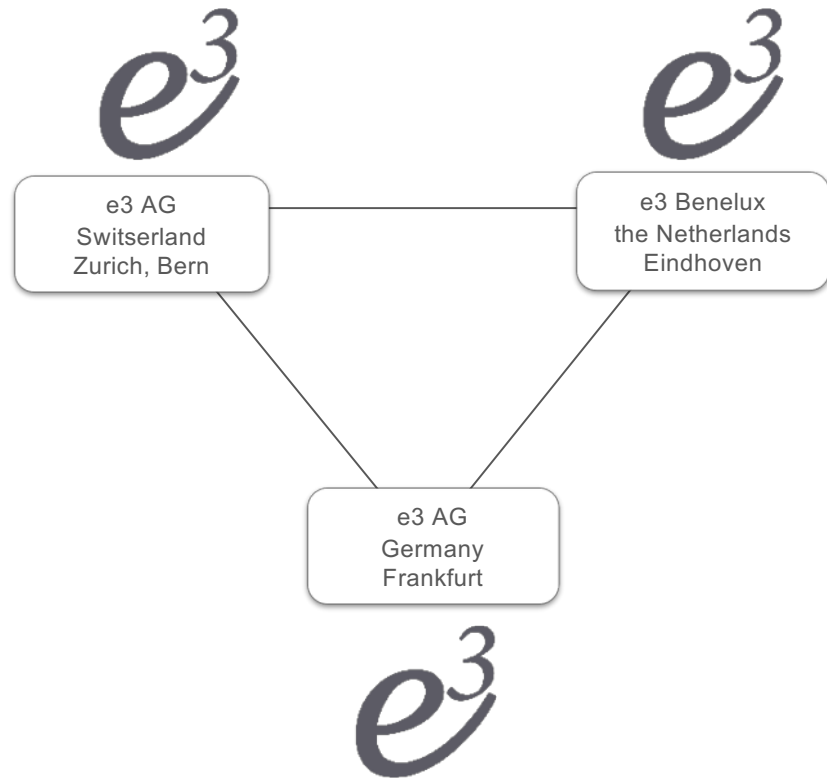
Marcel.vandenbroek@e3benelux.eu

06-15827932

www.e3benelux.eu

Marcel van den Broek, Marcel.vandenbroek@e3benelux.eu, 06-15827932, www.e3benelux.eu

e³ ORGANIZATION



e3 Benelux
Torenallee 20
5617 BC Eindhoven
Tel: +31 (0)85 0655 254
eMail: info@e3benelux.eu
Web: www.e3benelux.eu

Located at Strijp-S VideoLab



Mature DLP delivers Business Value
“ DLP as a Business Security Service”

Marcel van den Broek, Marcel.vandenbroek@e3benelux.eu, 06-15827932, www.e3benelux.eu

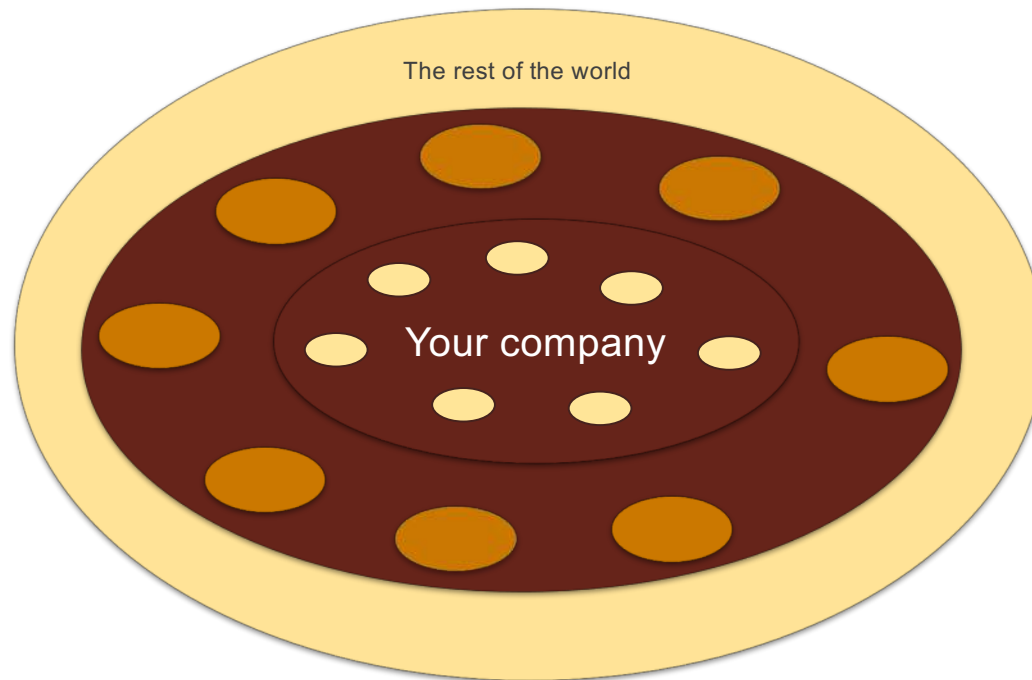
e³ OUR EXPERIENCE



- e3 is delivering DLP solution since 2009. Since then, we had the privilege to provide DLP solution to a growing number of smaller companies and global enterprise.
- According to recent Gartner analysis, *“it is time to redefine DLP”* by Brian Reed. Well not our clients, because none of them has one of the “problems”:

	Gartner’s Challenges	e3 Approach
1	Technology instead of business driven approach	1 of 4 area’s addressed in e3 DLP initiatives is technology. 3 are business and governance focussed
2	Unrealized potentials of DLP solutions	We take the solution to the limit and in collaboration with existing and new other systems beyond the original purpose
3	High maintenance / incomplete deployments	Our goal is minimal TCO for maximal functionality

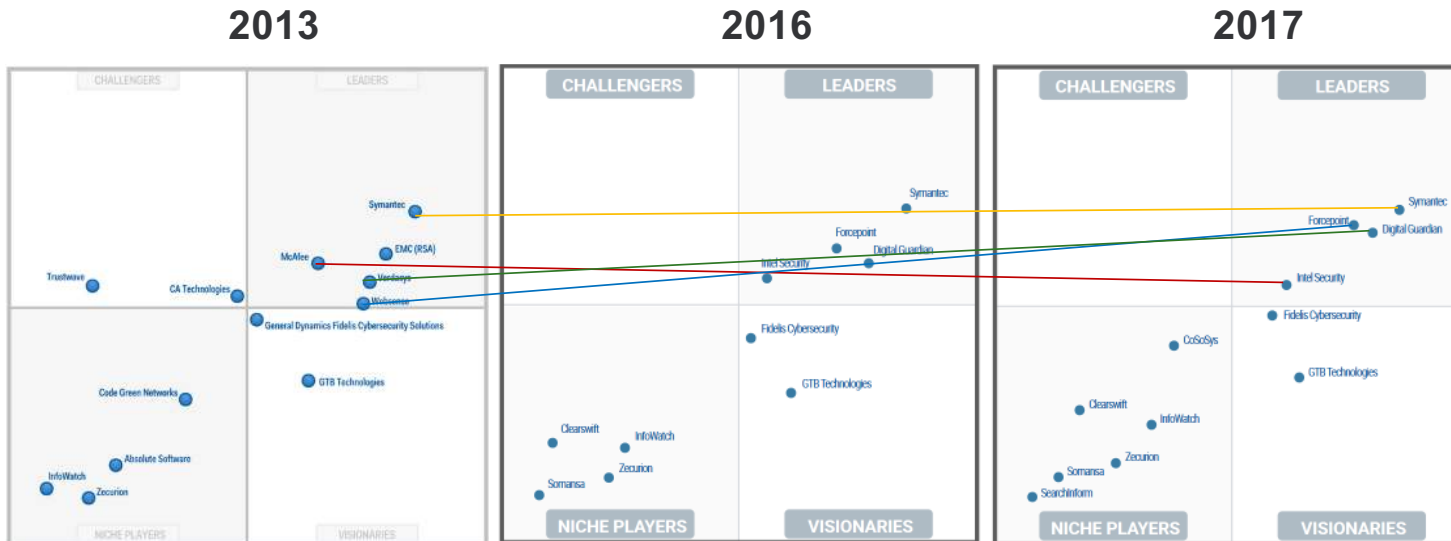
e³ THE STRENGTH OF (MATURE) DLP



DLP allows you to control where your sensitive data is allowed to go to.

- Within your company
- Towards your business partners
- Towards the rest of the world

e³ VENDORS OVER THE YEARS



Symantec's positioning is stable. Strong detection capabilities. High End solution, ideal for Banking/Insurance/Intellectual property.

McAfee's main challenge is the lack of experienced implementation specialist. Ideal for Manufacturing/Industry though also seen in other sectors.

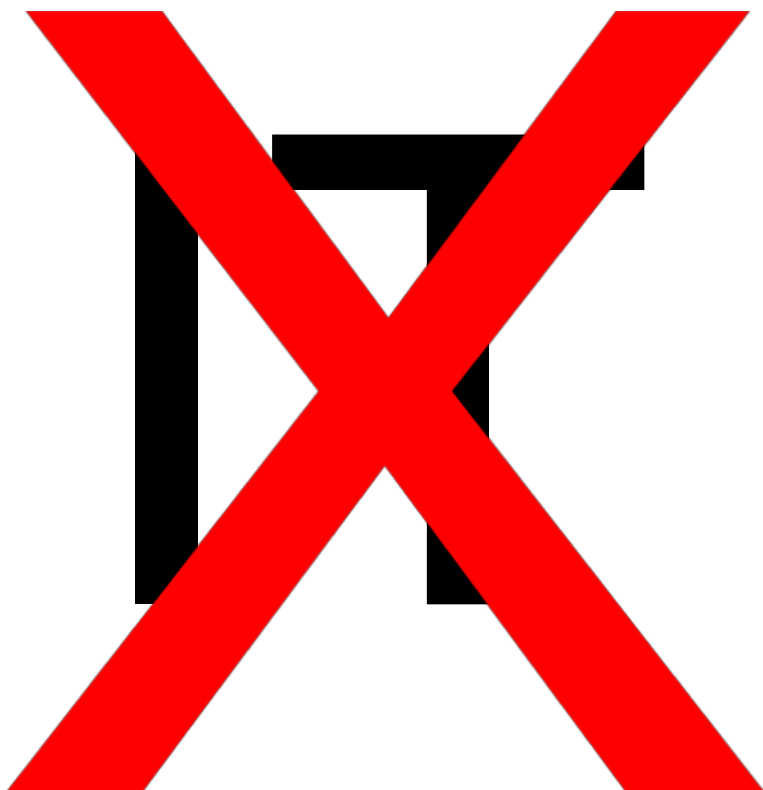
With RSA and CA, two major vendors gave up on DLP. Increased gap between leaders and niche players.

Microsoft AIP is currently biggest challenge in the enterprise world. Due to political sales strength not functionality. Channel DLP only.

Digital Guardian (Verdasys) also improved slightly. Currently not very visible in the market. Primarily Endpoint focused.

Forcepoint (Websense) improved significantly in quadrant. Acquired by Raytheon (close to US military). Potential conflict between GDPR and their user behavioural approach identified.

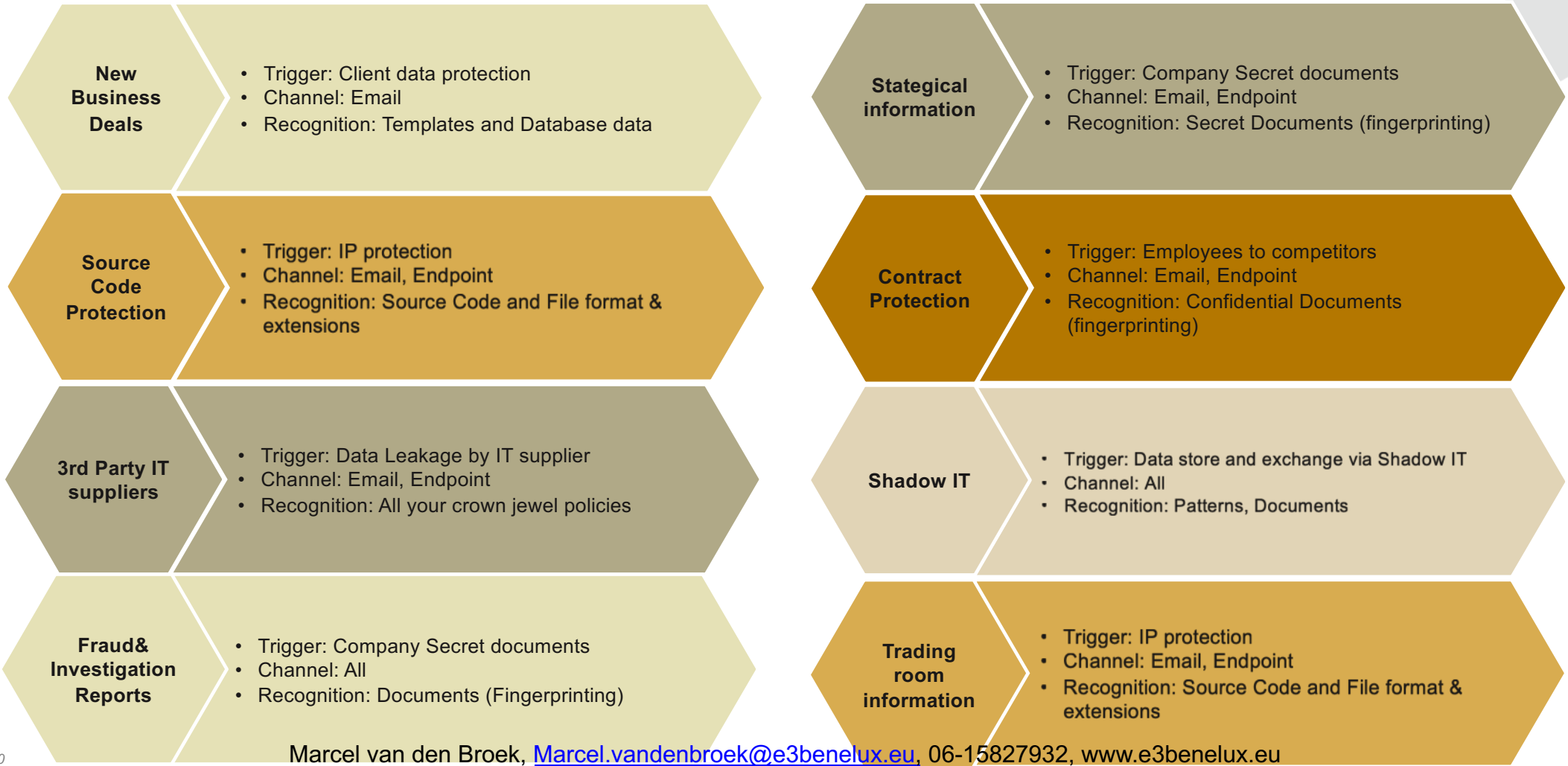
e³ LETS BE CLEAR.....



e³ AND.....



e³ MATURE DLP ADDS VALUE TO THE BUSINESS

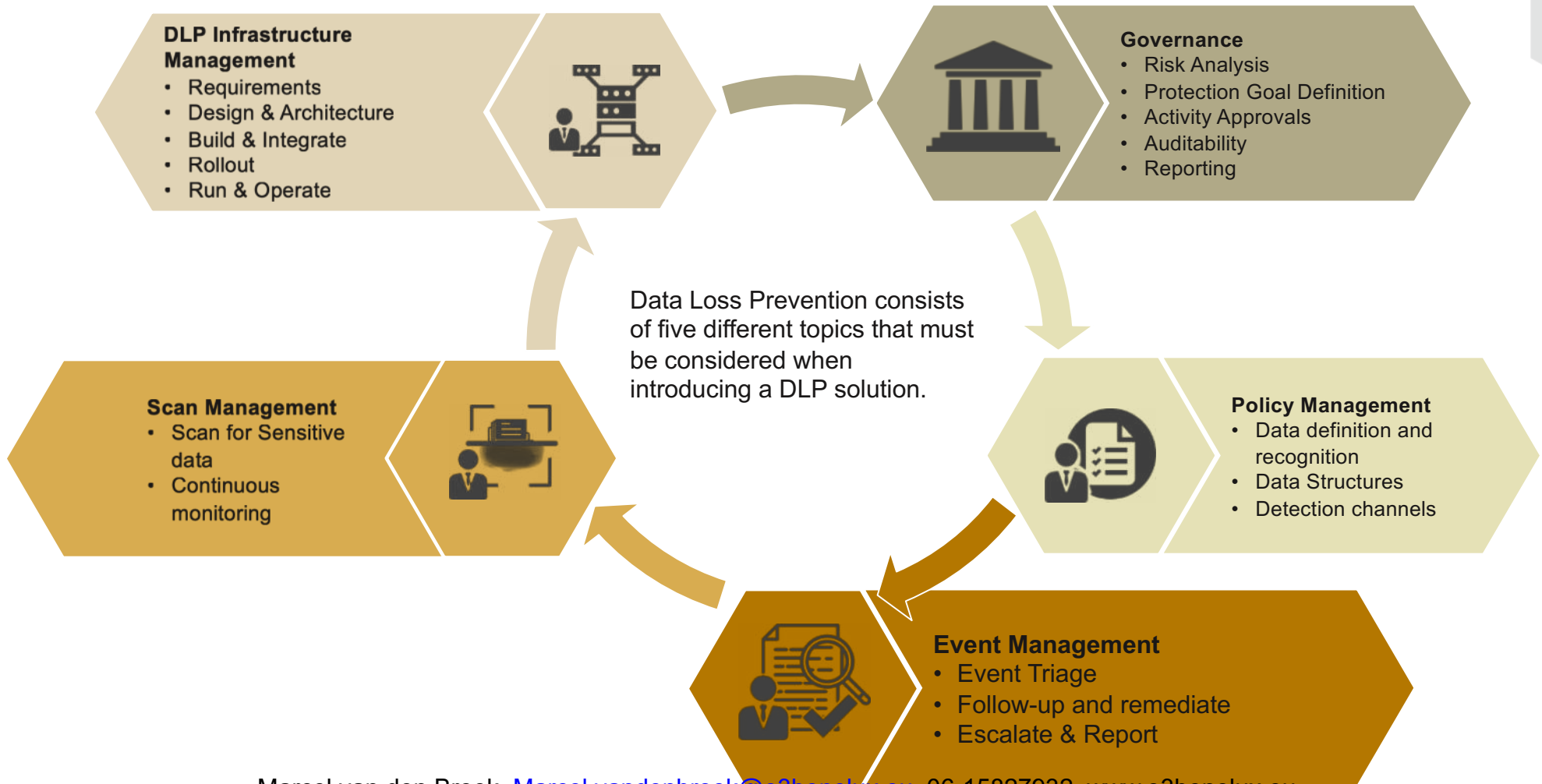


e³ DLP, A BUSINESS SECURITY SERVICE

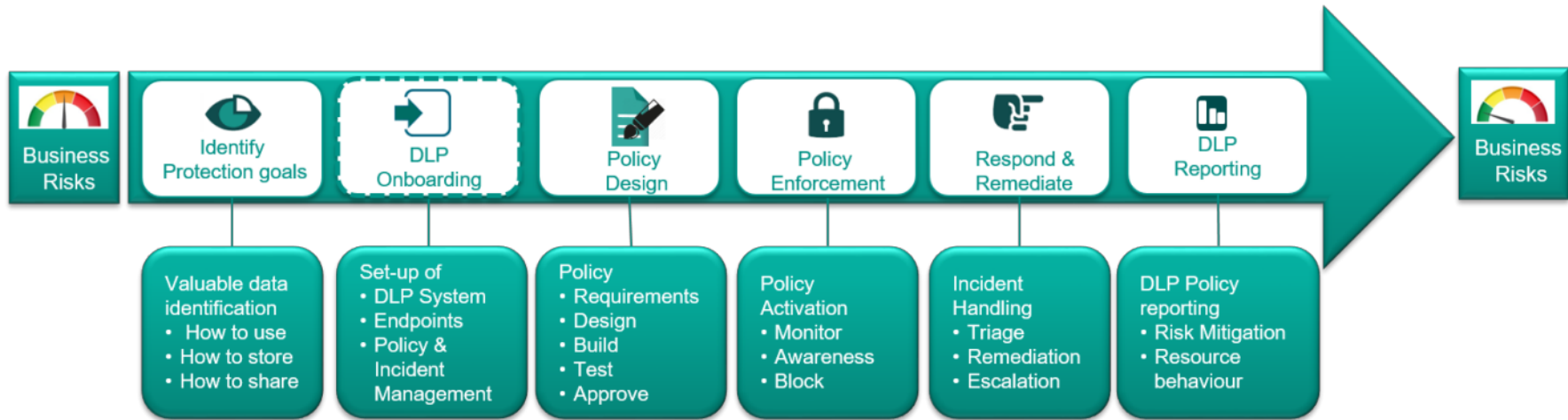


- DLP is able to Reduce Business Risks to an acceptable level
- DLP can not reduce Business risks completely
- DLP act as a security control together with other security controls

e³ WHAT IS MATURE DLP ABOUT



e³ DLP APPROACH



Roles

Business Owner
 Business Policy Owner
 Business Deployment Coordinator
 Business Incident Handler
 DLP Policy Consultant
 DLP Product Owner
 DLP DEVOPS

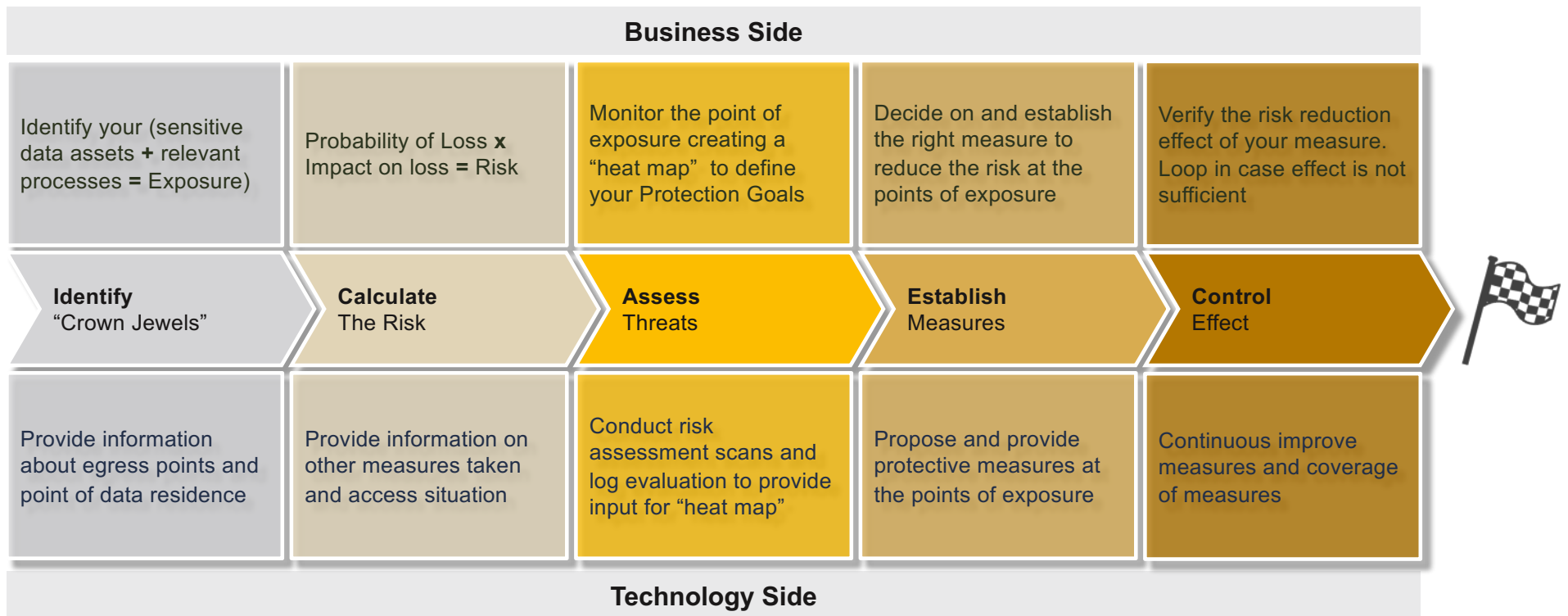
Accountability

Owner of the Business Protection Goals
 Owner of the DLP Policy, responsible for the DLP Policy requirements
 Responsible for the local DLP deployment
 Validates and Remediate DLP incidents
 DLP counterpart for the Business Policy Owner
 DLP Service responsible
 DLP Change and Operations team

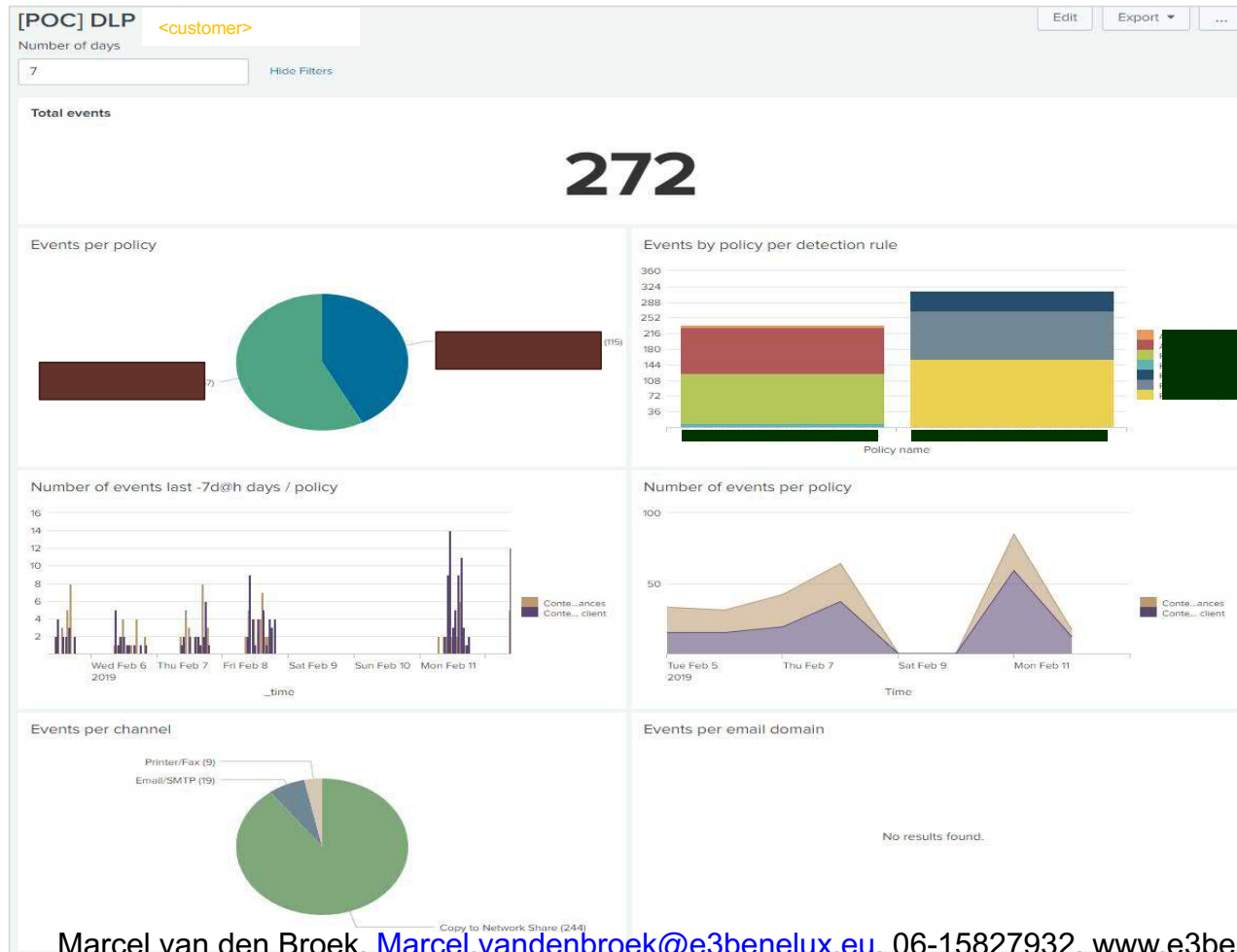
e³ PROTECTION GOAL



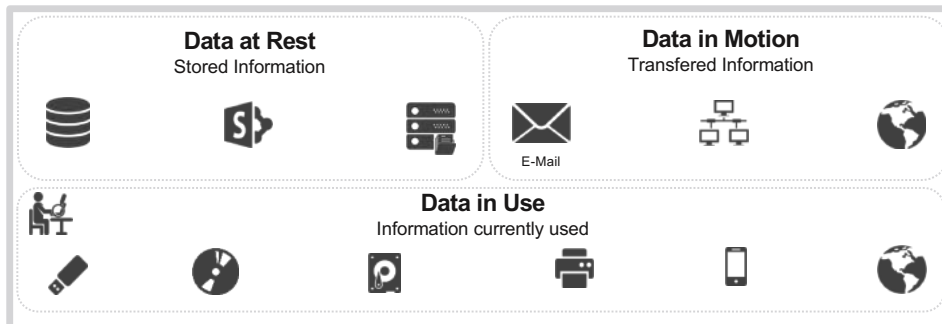
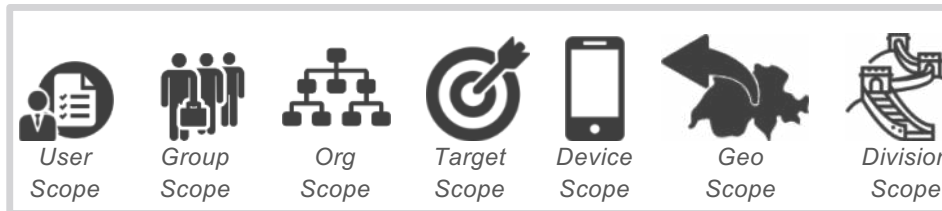
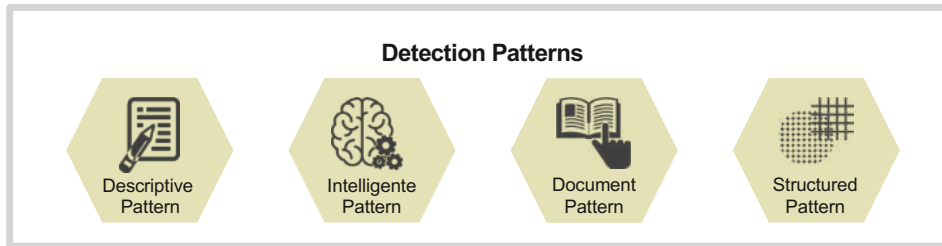
The goal of protection is to control sensitive data. This demands efforts on the business side as well as on the technology side.



e³ IDENTIFICATION OF THE PROTECTION GOAL BY DLP



e³ TRANSLATION INTO DLP POLICIES



What to look for?

Detection patterns derived from your protection goal process. Often tuning is required

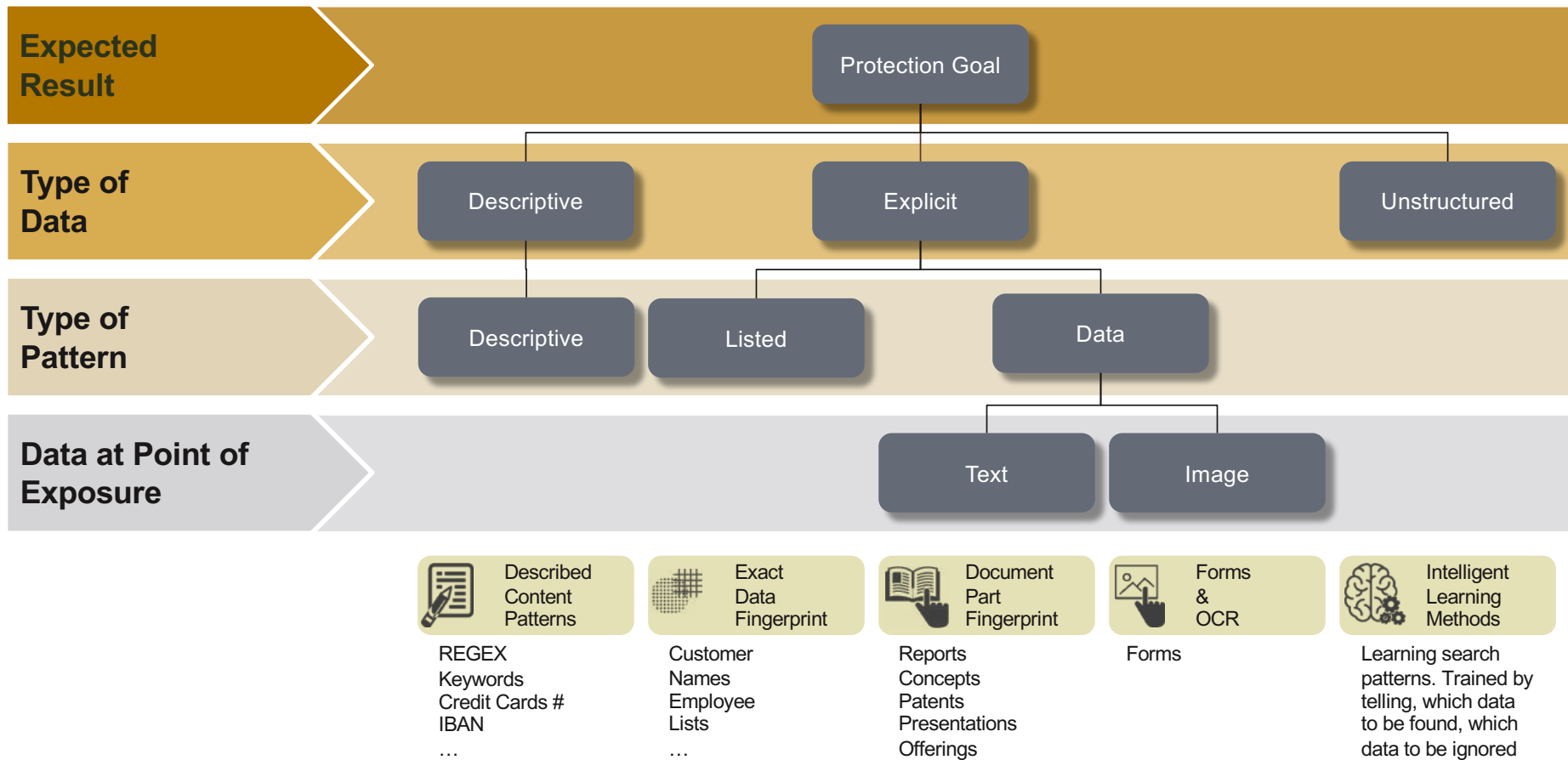
Scope definition restrict the policies are of operation (only certain user groups, only for certain target, ...)

Reactions are mostly preventive actions like blocking an eMail, quarantining a file etc.

e³ SEARCH PATTERNS



Getting the right search pattern for the policies requires an analysis of the data that should be protected.



e³ THE DILEMMA AROUND A DLP POLICY



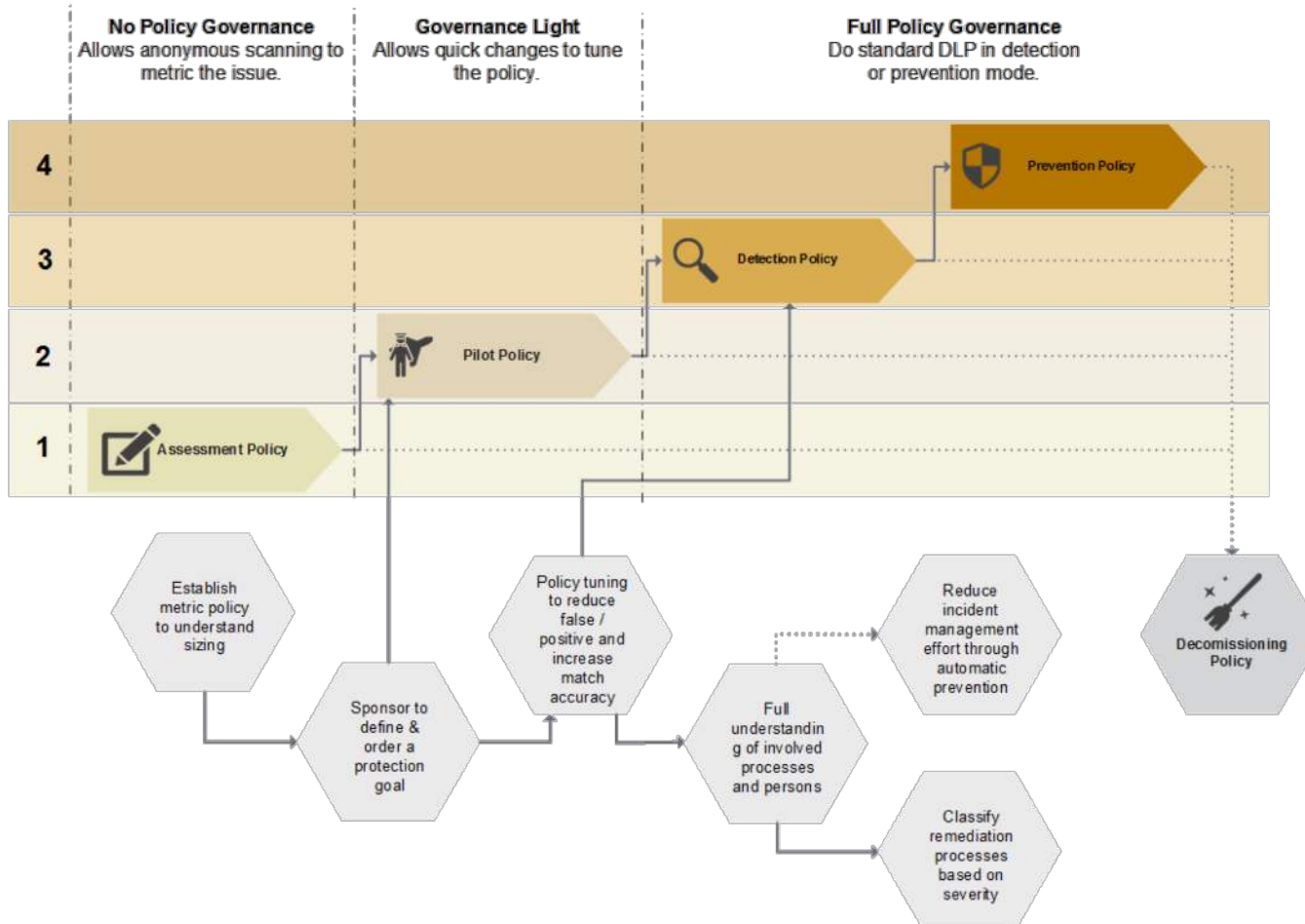
- Is not Infrastructure
- Is not an application
- And is not recognized as an Information Asset
- But the impact can be destructive in many ways
- How to ensure that DLP Policies are released with the right approvals against the right quality and comply to the associated rules and regulations?



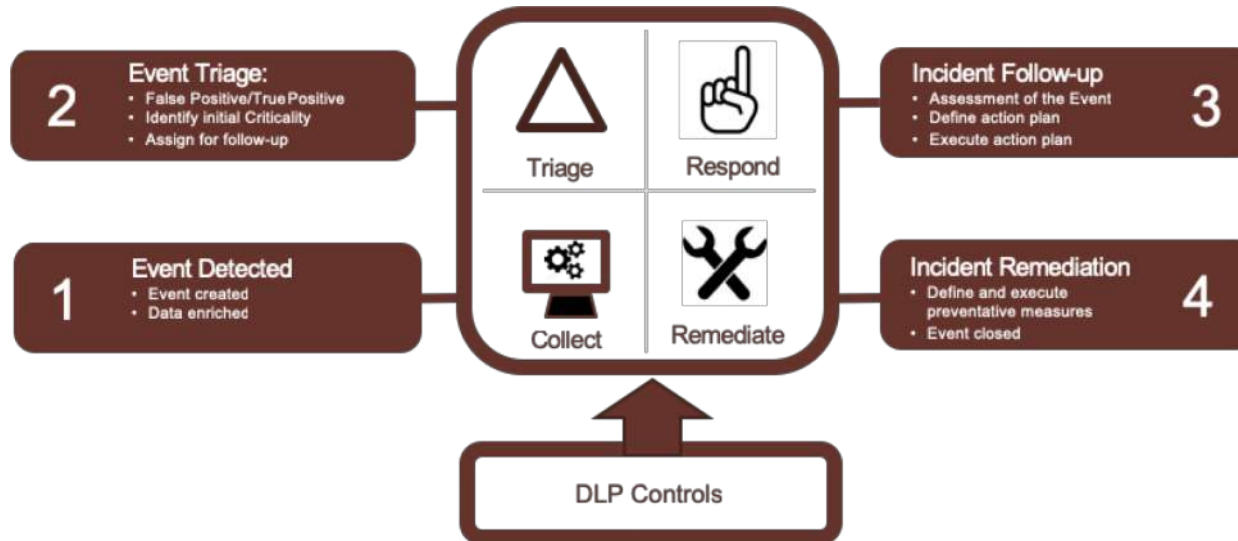
e³ POLICY LIFE CYCLE



To reduce risks, policies have to be introduced following a well-defined process.



e³ DLP EVENTS HANDLING



Behavioural change will not take place without Incident Follow-up and remediation

F/P should be routed back to the Policy Management process for improvement

GDPR related incidents have to be reported via Privacy Office to the AP within 72 hours

e³ EVENT TRIAGE



- The main output from the triage is:
 - The DLP event is assigned to the Incident handler
 - The DLP event is validated into a real incident (True Positive) or not (False Positive)
 - In case of a False Positive two situations could be identified:
 1. A shadow process is identified, which could be addressed as a process improvement by the business owner, the Policy could be tuned to allow this way of working



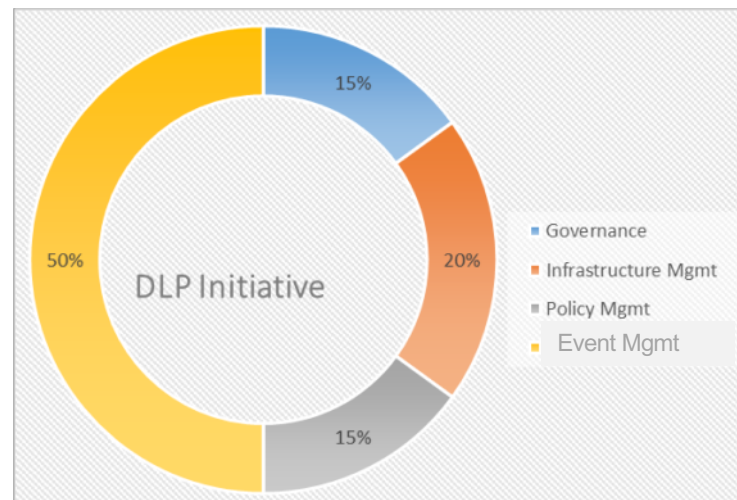
2. The Policy generates events which should not be generated
False Positives can also be identified by the Policy Owner out-off the reporting

In all cases the Policy Owner should be requested to tune the DLP Policy and reduce these False Positives.

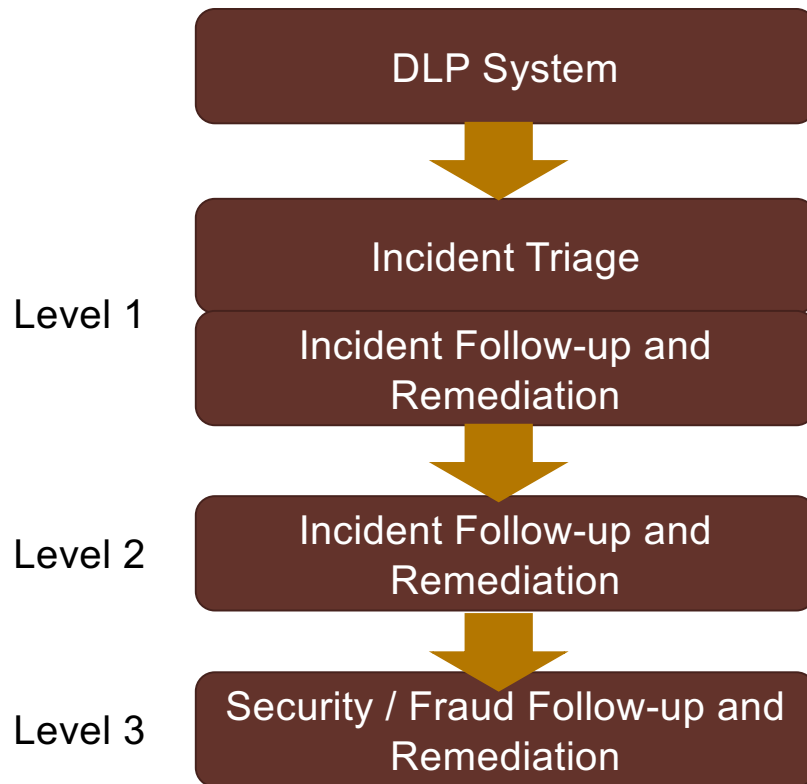
e³ WHY IS EVENT MANAGEMENT A BIG ITEM IN DLP?



- 50% of the effort is related to DLP Event Management
- Effort that needs to be planned, budgetted and allocated
 - Business effort especially
 - Generally this is not expected and not part of the business case



e³ EVENT HANDLING MODELS



example

The Event management can differ from on policy to the other

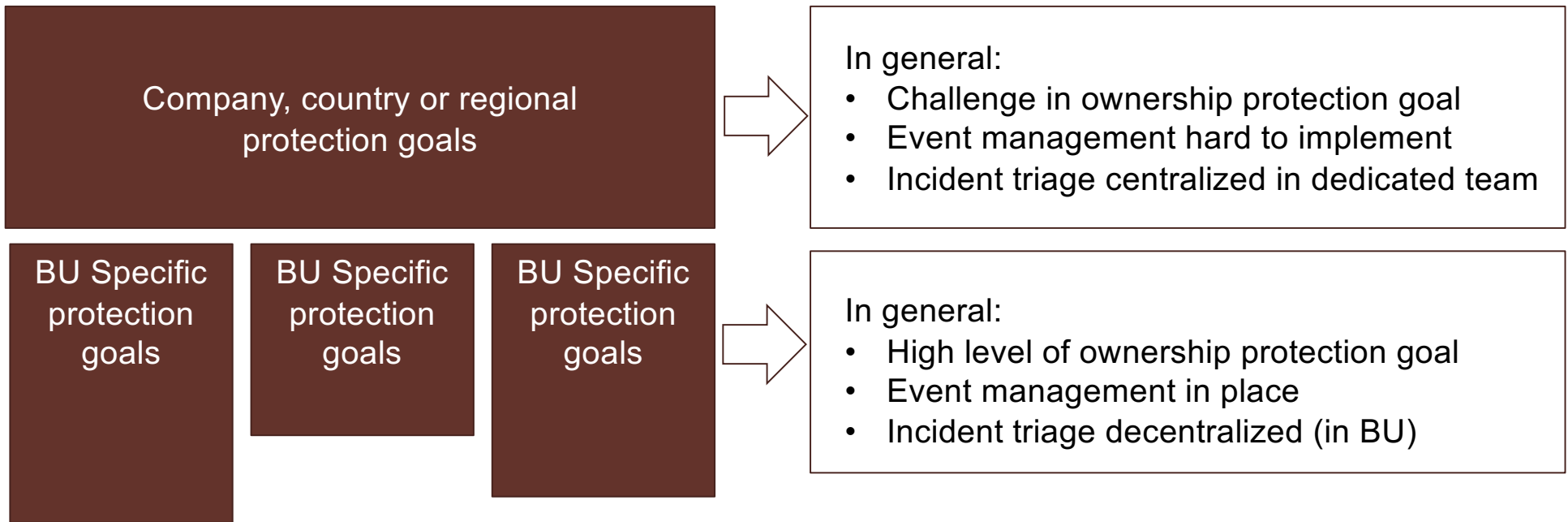
Depending on :

- Your organization
- Scope of the DLP Policy
- Sort of data sensitivity
- Sort of end-users
- Etc

Multiple models will run next to each other



RELATED TO CENTRAL AND DECENTRAL PROTECTION GOALS



e³ 10 MAIN ITEMS TO COVER



Country vs BU
Deployments

Privacy Officer

Business
Impact Analyses

Privacy Impact
Analyses

Local
legislation

Workers
Council

Governance

Communication

Business
Resources

It takes time



e³

THE END

Marcel van den Broek
Marcel.vandenbroek@e3benelux.eu
06-15827932
www.e3benelux.eu

Marius van der Vak
Marius.vandervalk@e3benelux.eu
06-29526437
www.e3benelux.eu