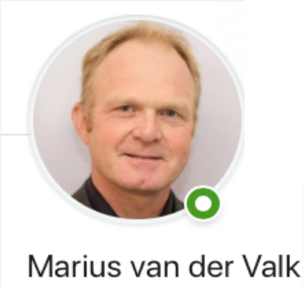
Data Los Risk reduction with DLP

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

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

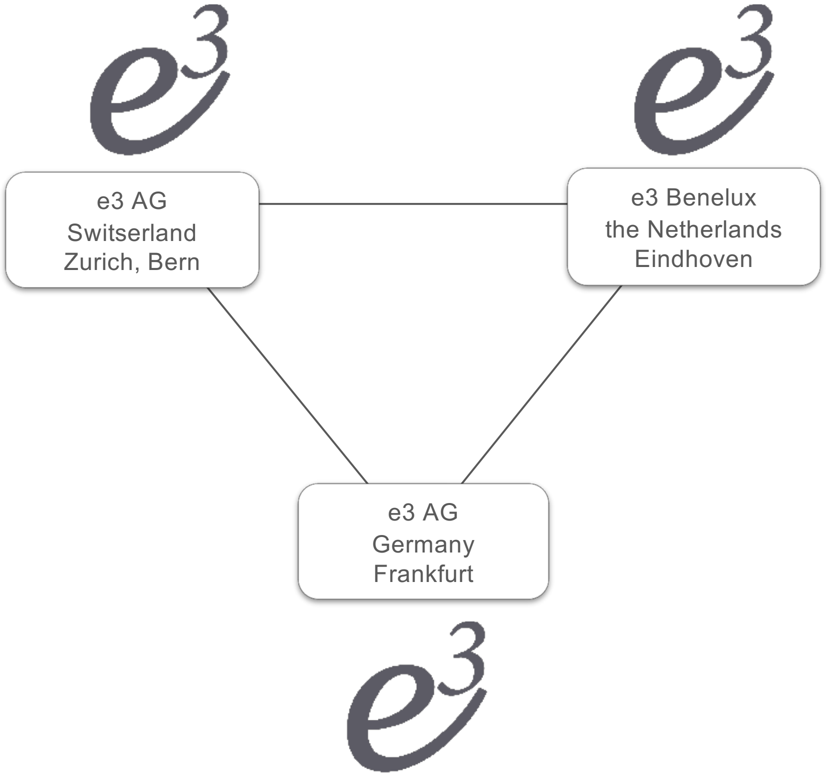
REPRESENTATIVES



Marius.vandervalk@e3benelux.eu
06-29526437
www.e3benelux.eu

Marcel.vandenbroek@e3benelux.eu
06-15827932
www.e3benelux.eu

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

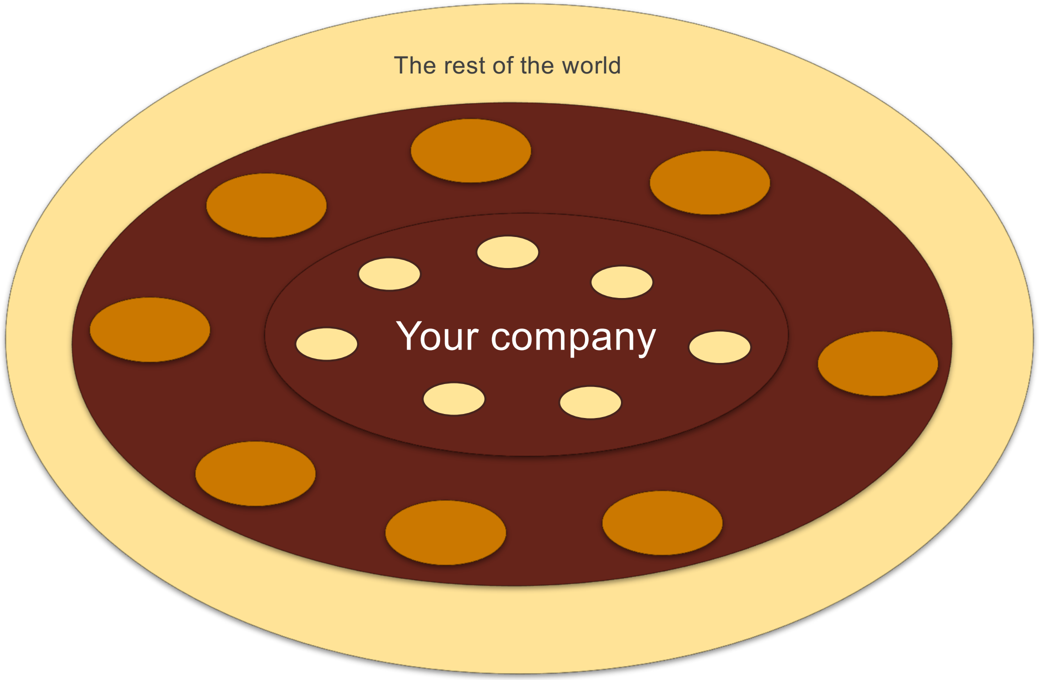
“ DLP as a Business Security Service”

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

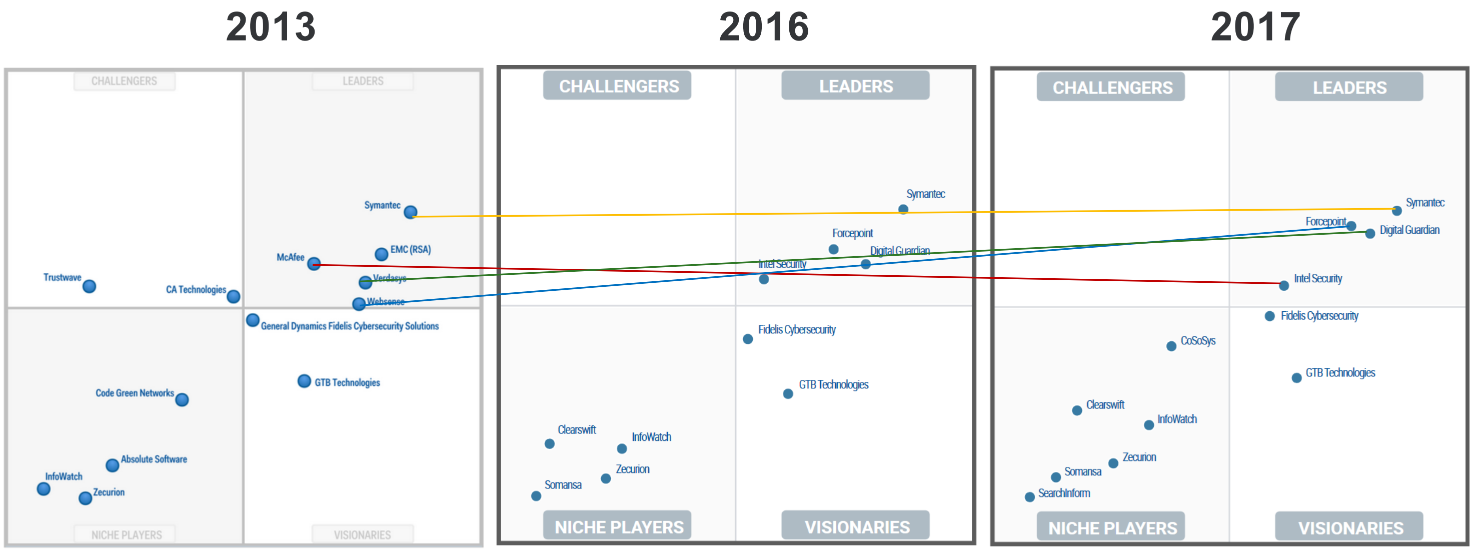
THE STRENGTH OF (MATURE) DLP



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

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.

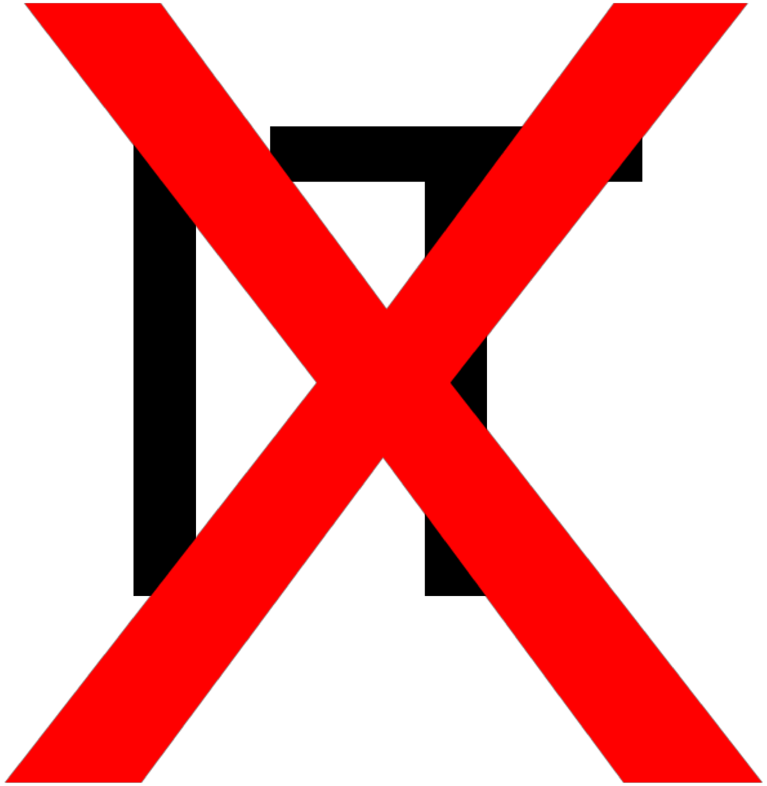
Microsoft AIP is currently biggest challenge in the enterprise world. Due to political sales strength not functionality. Channel DLP only.

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.

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

Lets be clear......



e^3 And......

MATURE DLP ADDS VALUE TO THE BUSINESS

New Business Deals

- Trigger: Client data protection
- Channel: Email
- Recognition: Templates and Database data

Source Code Protection

- Trigger: IP protection
- Channel: Email, Endpoint
- Recognition: Source Code and File format & extensions

3rd Party IT suppliers

- Trigger: Data Leakage by IT supplier
- Channel: Email, Endpoint
- Recognition: All your crown jewel policies

Fraud& Investigation Reports

- Trigger: Company Secret documents
- Channel: All
- Recognition: Documents (Fingerprinting)

Stategical information

- Trigger: Company Secret documents
- Channel: Email, Endpoint
- Recognition: Secret Documents (fingerprinting)

Contract Protection

- Trigger: Employees to competitors
- Channel: Email, Endpoint
- Recognition: Confidential Documents (fingerprinting)

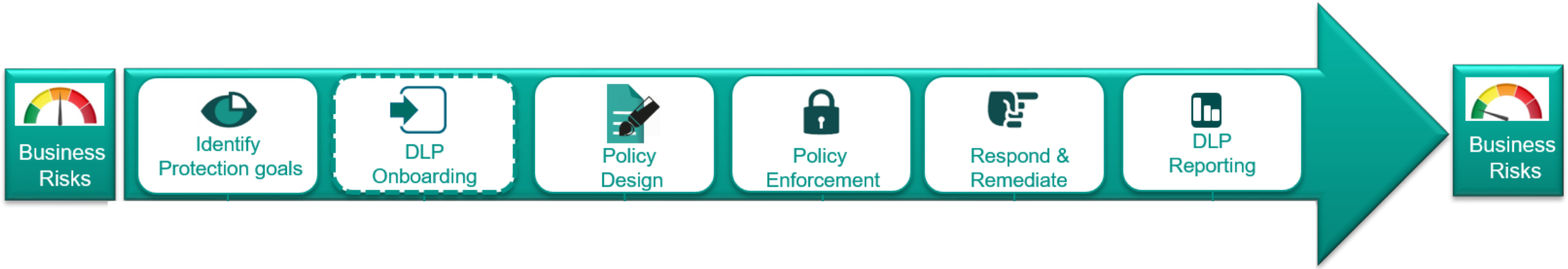
Shadow IT

- Trigger: Data store and exchange via Shadow IT
- Channel: All
- Recognition: Patterns, Documents

Trading room information

- Trigger: IP protection
- Channel: Email, Endpoint
- Recognition: Source Code and File format & extensions

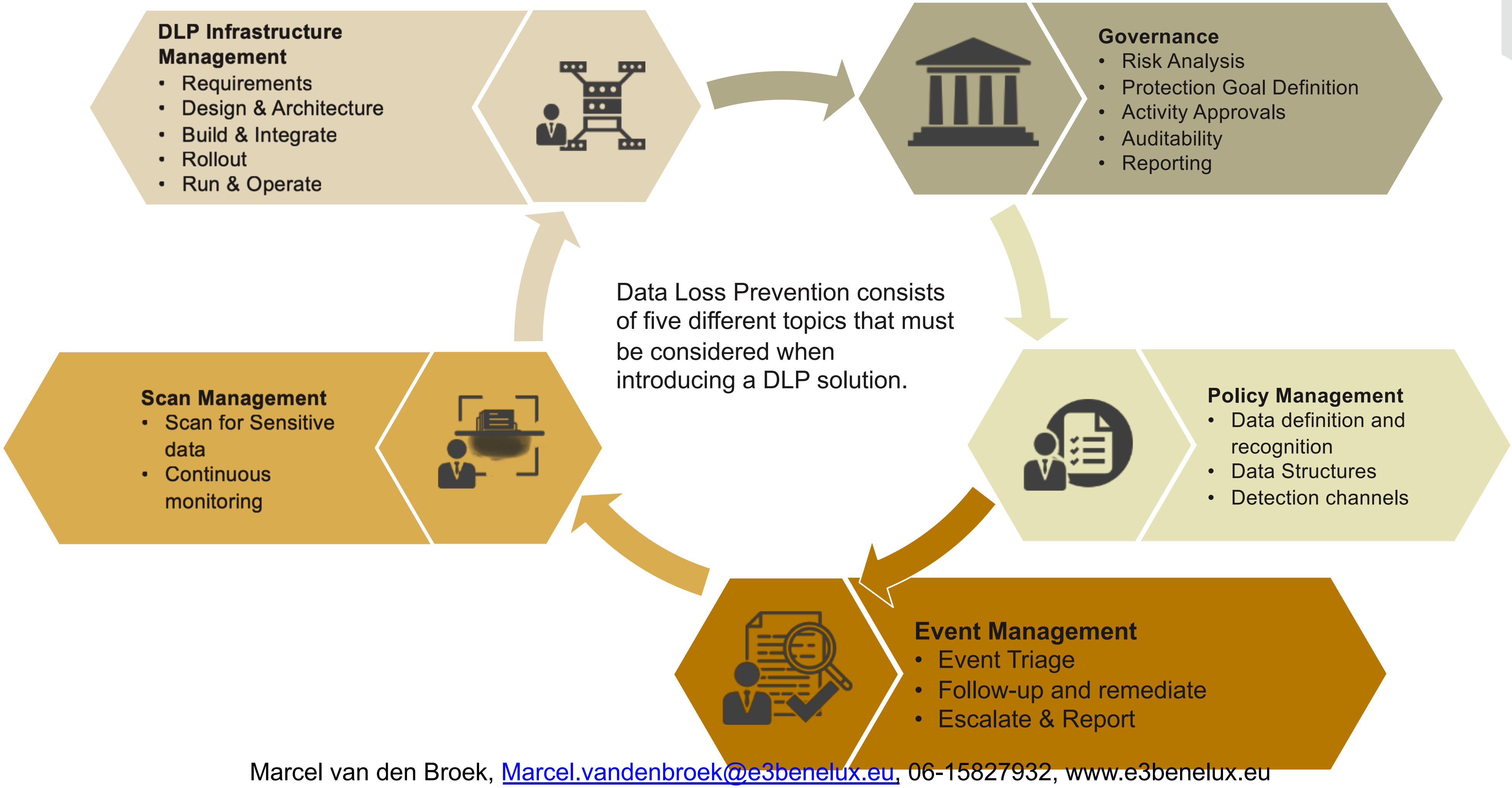
DLP, A BUSINESS SECURITY SERVICE



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

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

WHAT IS MATURE DLP ABOUT



DLP Infrastructure Management

- Requirements
- Design & Architecture
- Build & Integrate
- Rollout
- Run & Operate

Governance

- Risk Analysis
- Protection Goal Definition
- Activity Approvals
- Auditability
- Reporting

Policy Management

- Data definition and recognition
- Data Structures
- Detection channels

Event Management

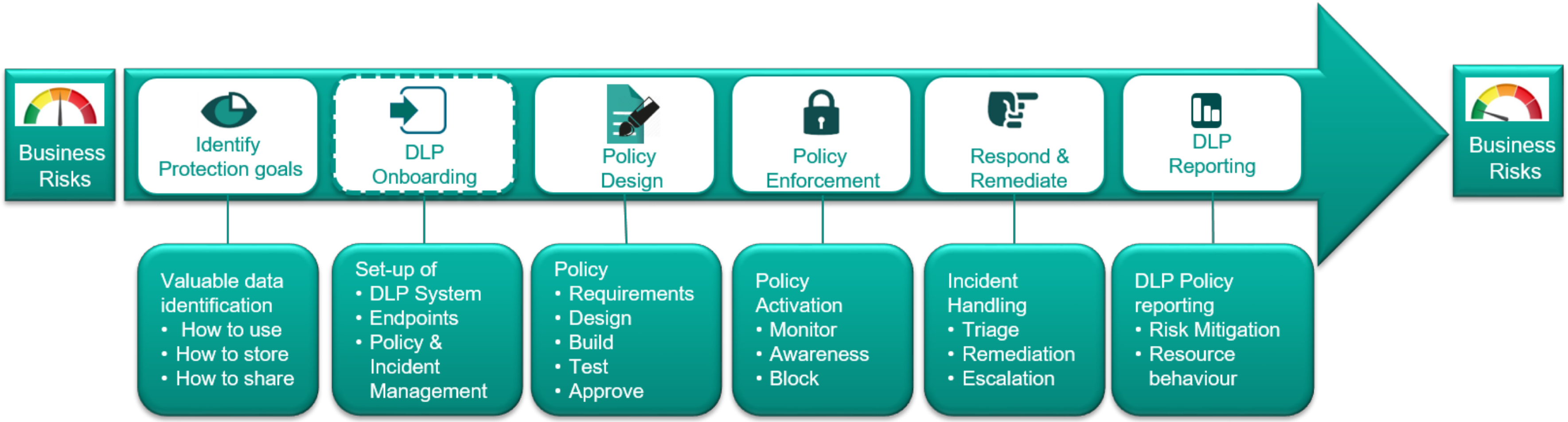
- Event Triage
- Follow-up and remediate
- Escalate & Report

Scan Management

- Scan for Sensitive data
- Continuous monitoring

Data Loss Prevention consists of five different topics that must be considered when introducing a DLP solution.

DLP APPROACH



Valuable data identification
- How to use
- How to store
- How to share

Set-up of
- DLP System
- Endpoints
- Policy & Incident Management

Policy
- Requirements
- Design
- Build
- Test
- Approve

Policy Activation
- Monitor
- Awareness
- Block

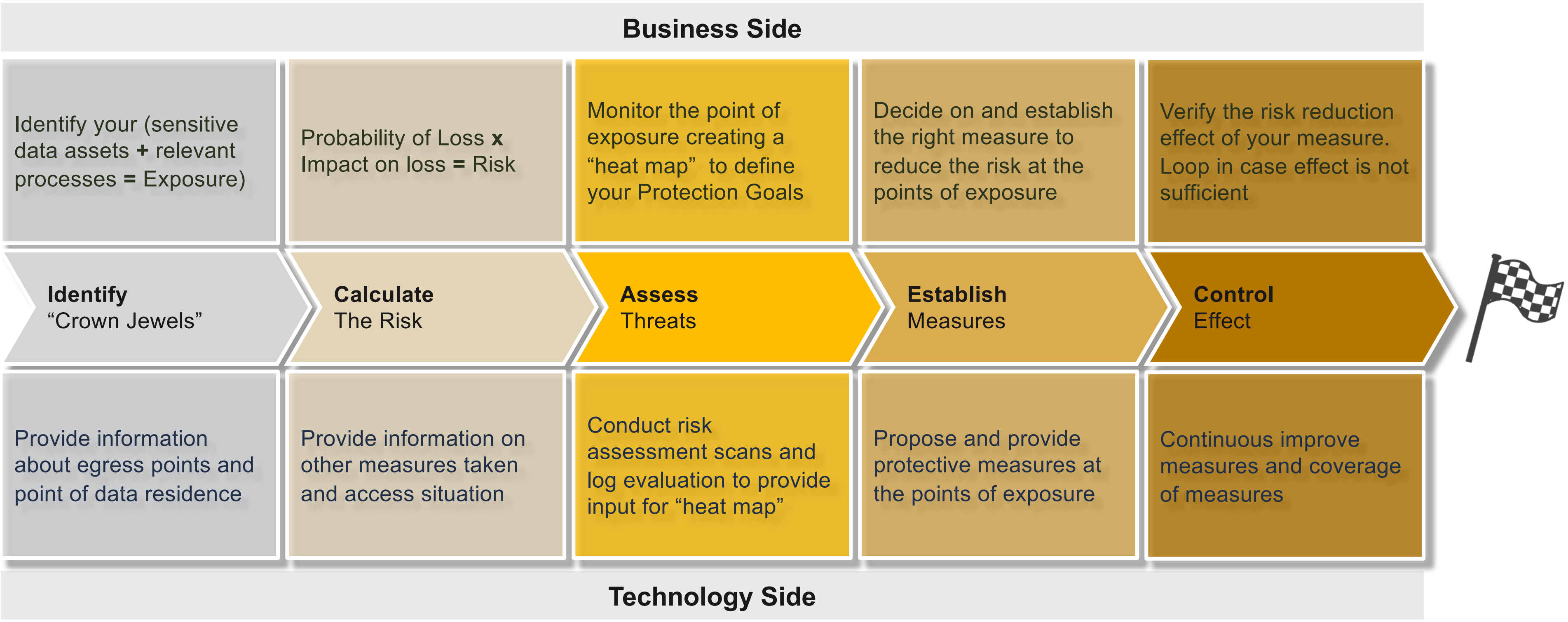
Incident Handling
- Triage
- Remediation
- Escalation

DLP Policy reporting
- Risk Mitigation
- Resource behaviour

Roles	Accountability
Business Owner	Owner of the Business Protection Goals
Business Policy Owner	Owner of the DLP Policy, responsible for the DLP Policy requirements
Business Deployment Coordinator	Responsible for the local DLP deployment
Business Incident Handler	Validates and Remediates DLP incidents
DLP Policy Consultant	DLP counterpart for the Business Policy Owner
DLP Product Owner	DLP Service responsible
DLP DEVOPS	DLP Change and Operations team

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.



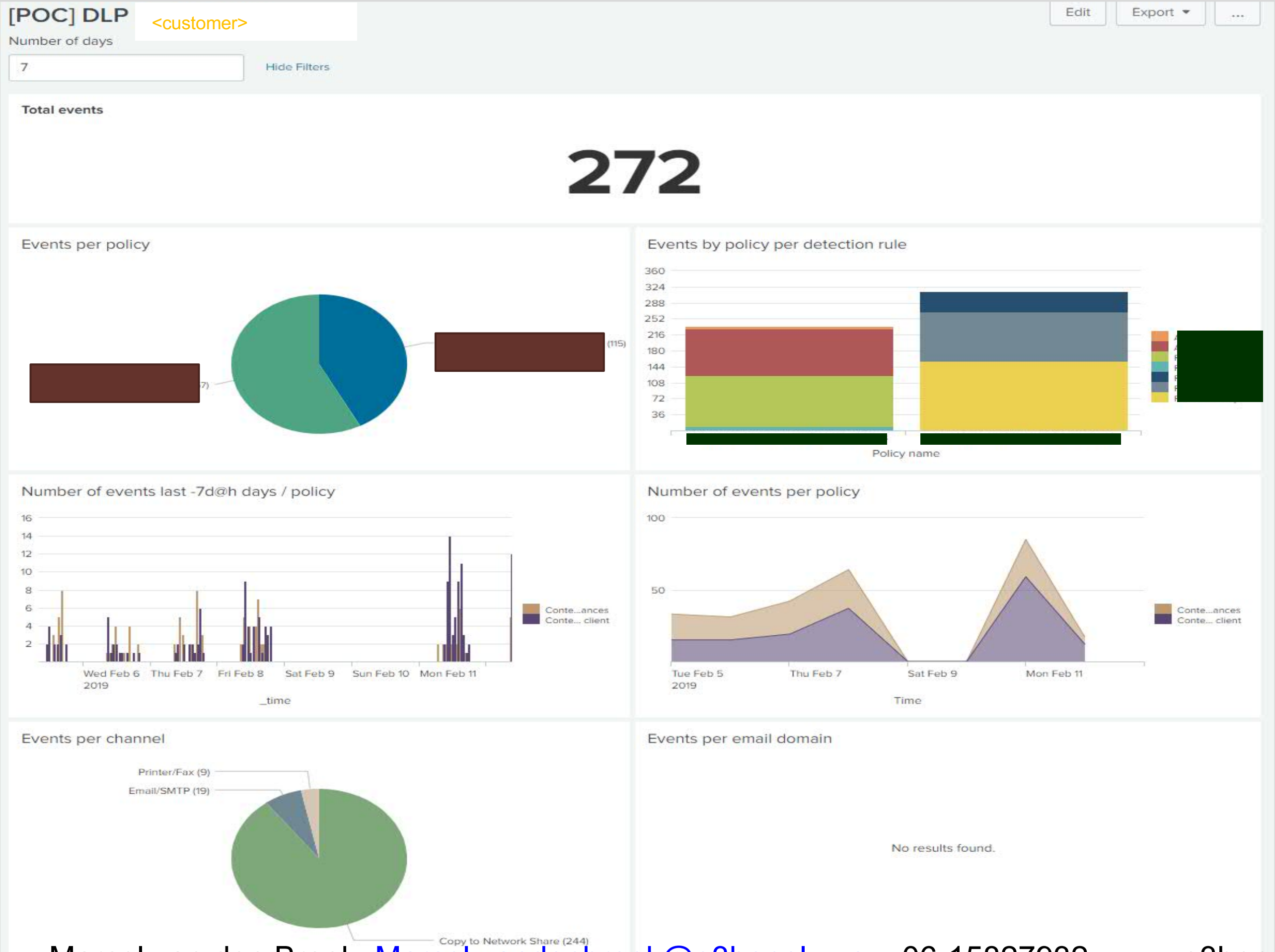
Business Side

Identify your (sensitive data assets **+** relevant processes **=** Exposure)	Probability of Loss **x** Impact on loss **=** Risk	Monitor the point of exposure creating a “heat map” to define your Protection Goals	Decide on and establish the right measure to reduce the risk at the points of exposure	Verify the risk reduction effect of your measure. Loop in case effect is not sufficient
Identify “Crown Jewels”	**Calculate** The Risk	**Assess** Threats	**Establish** Measures	**Control** Effect
Provide information about egress points and point of data residence	Provide information on other measures taken and access situation	Conduct risk assessment scans and log evaluation to provide input for “heat map”	Propose and provide protective measures at the points of exposure	Continuous improve measures and coverage of measures

Technology Side

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

IDENTIFICATION OF THE PROTECTION GOAL BY DLP



[POC] DLP <customer>

Number of days

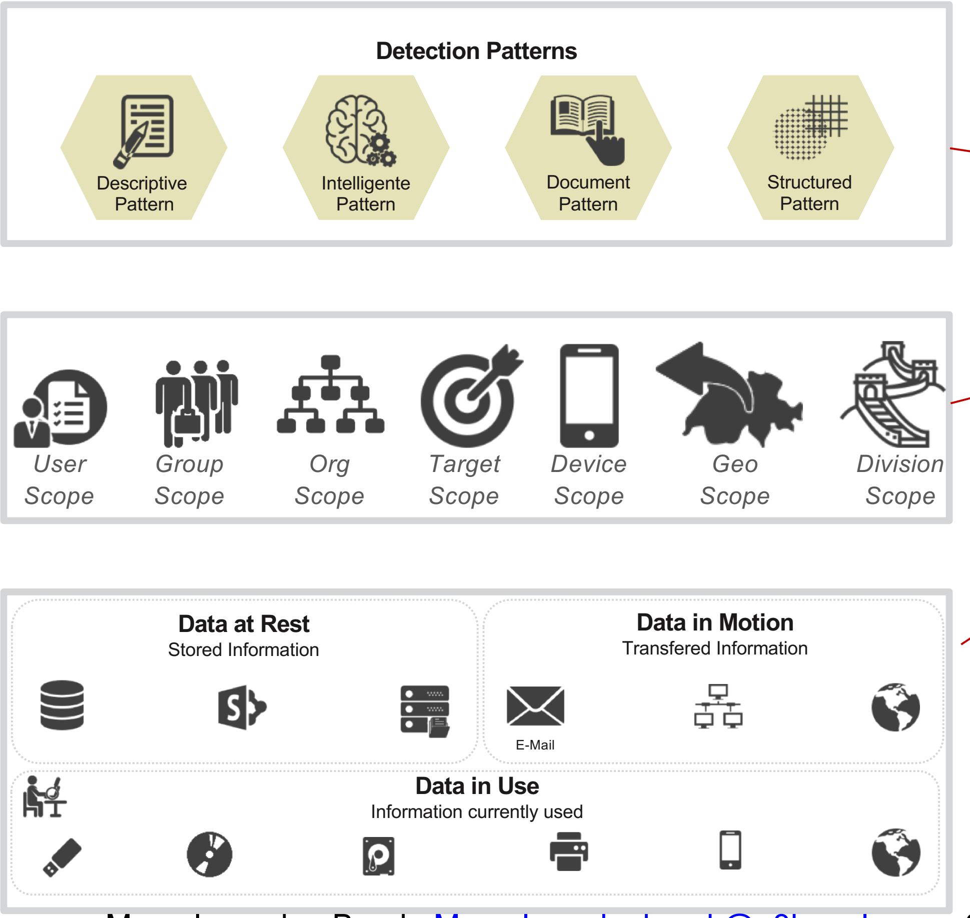
7

Total events

272

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

TRANSLATION INTO DLP POLICIES



What to look for?

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

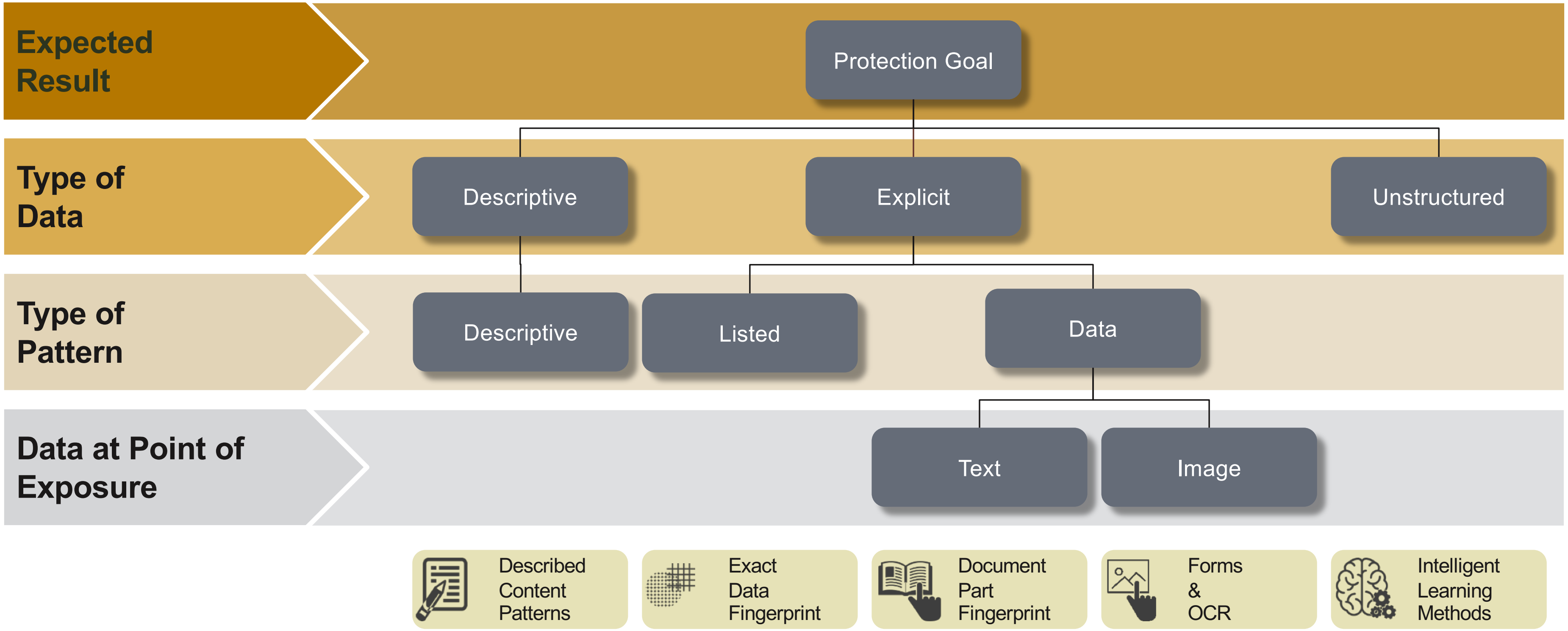
Scope definition restrict the policies are of operation (only certain user groups, only for certain target, …)

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

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

Search Patterns

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



Described Content Patterns:
REGEX
Keywords
Credit Cards #
IBAN
…

Exact Data Fingerprint:
Customer
Names
Employee
Lists
…

Document Part Fingerprint:
Reports
Concepts
Patents
Presentations
Offerings

Forms & OCR:
Forms

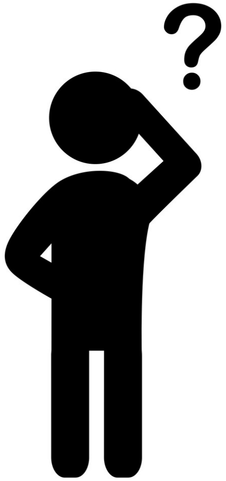
Intelligent Learning Methods:
Learning search patterns. Trained by telling, which data to be found, which data to be ignored

THE DILEMMA AROUND A DLP POLICY

- Is not Infrastructure
- Is not an application
- And is not recognized as an Information Asset

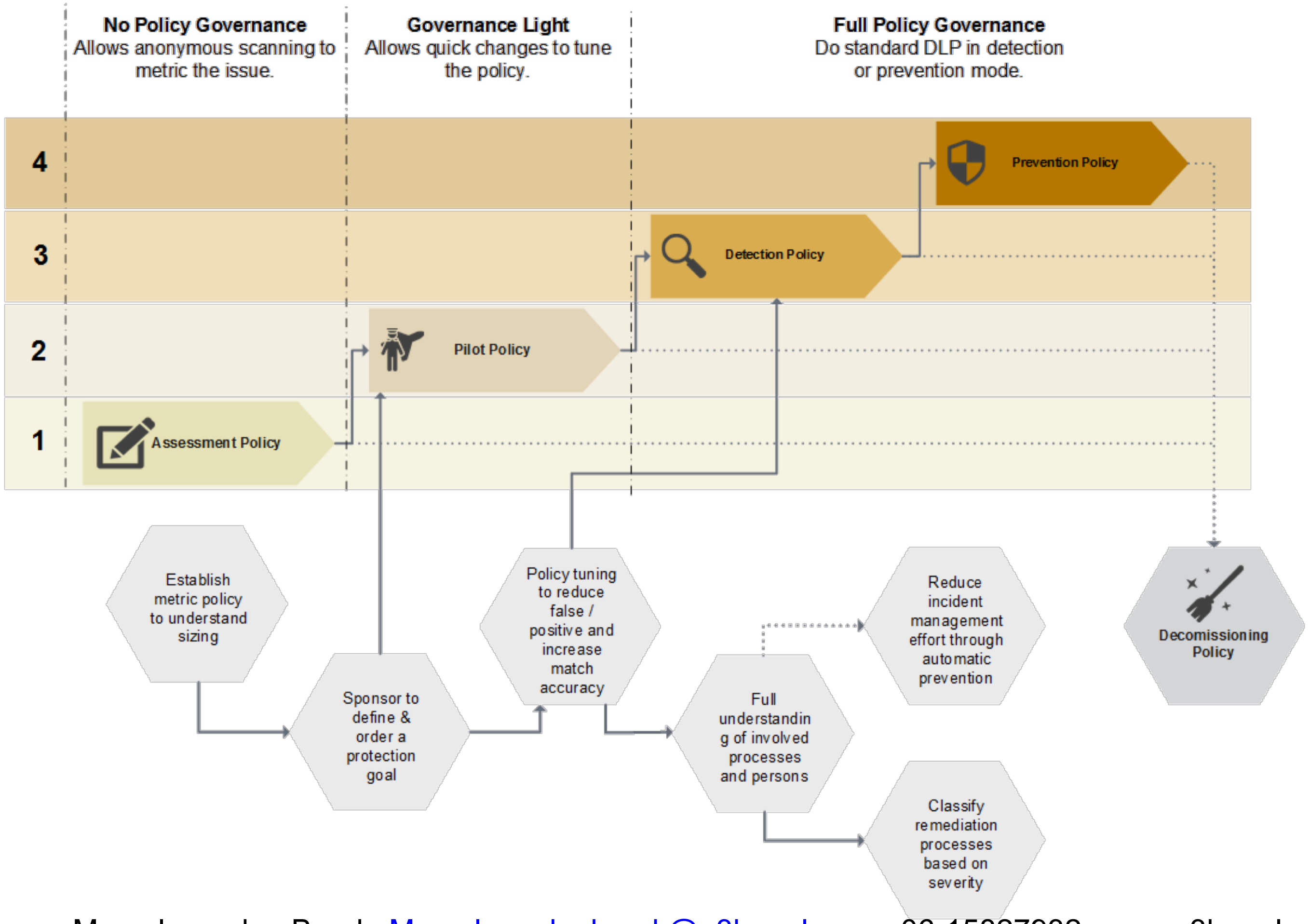
- But the impact can be destructive in many ways

- How to ensure that DLP Policies are released with the right approvals against the right quality and comply to the associated rules and regulations?



POLICY LIFE CYCLE

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



No Policy Governance
Allows anonymous scanning to metric the issue.

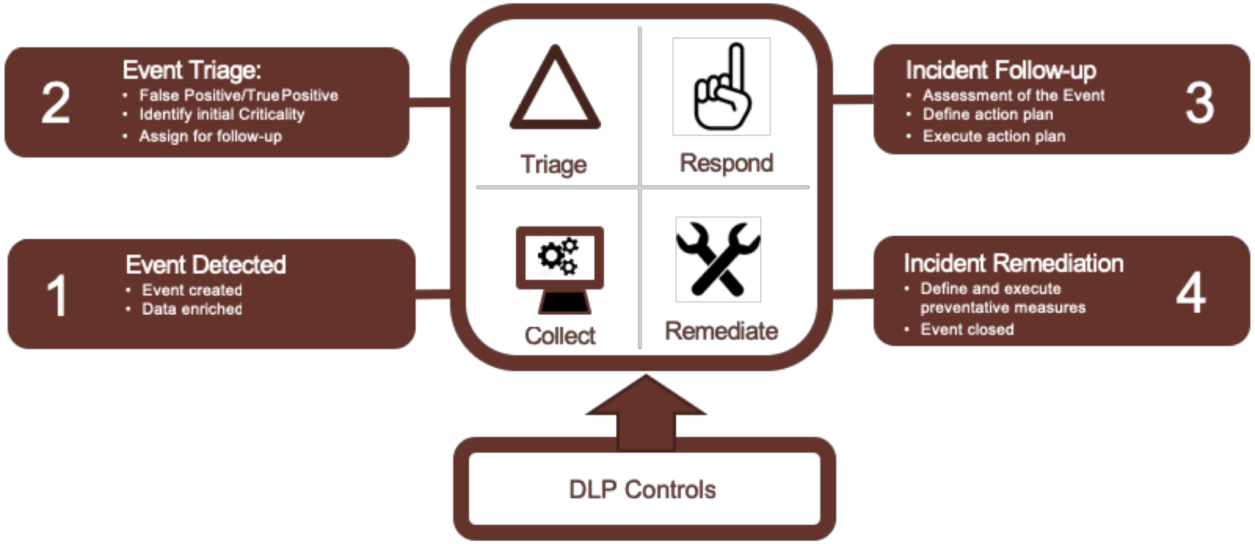
Governance Light
Allows quick changes to tune the policy.

Full Policy Governance
Do standard DLP in detection or prevention mode.

4
3
2
1
Prevention Policy
Detection Policy
Pilot Policy
Assessment Policy
Establish metric policy to understand sizing
Sponsor to define & order a protection goal
Policy tuning to reduce false / positive and increase match accuracy
Full understandin g of involved processes and persons
Reduce incident management effort through automatic prevention
Classify remediation processes based on severity
Decomissioning Policy

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

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

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

EVENT TRIAGE

- The main output from the triage is:
- The DLP event is assigned to the Incident hander
- 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

Business process

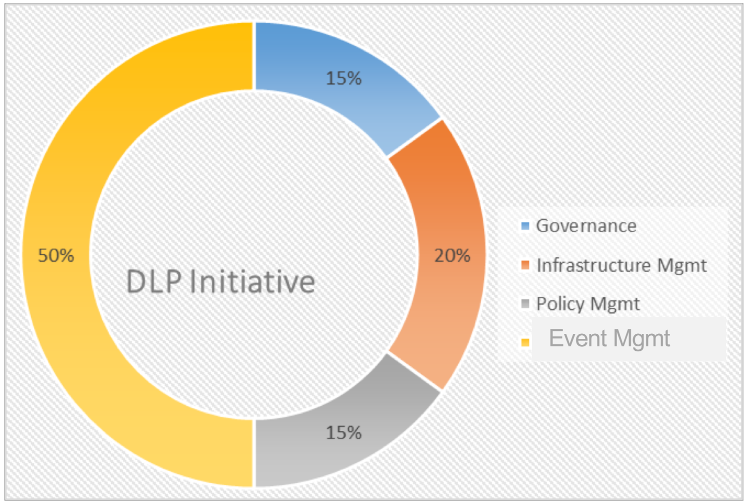
  2. The Policy generates events which should not be generated

False Positives can also be identified by the Policy Owner out-off the reporting

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

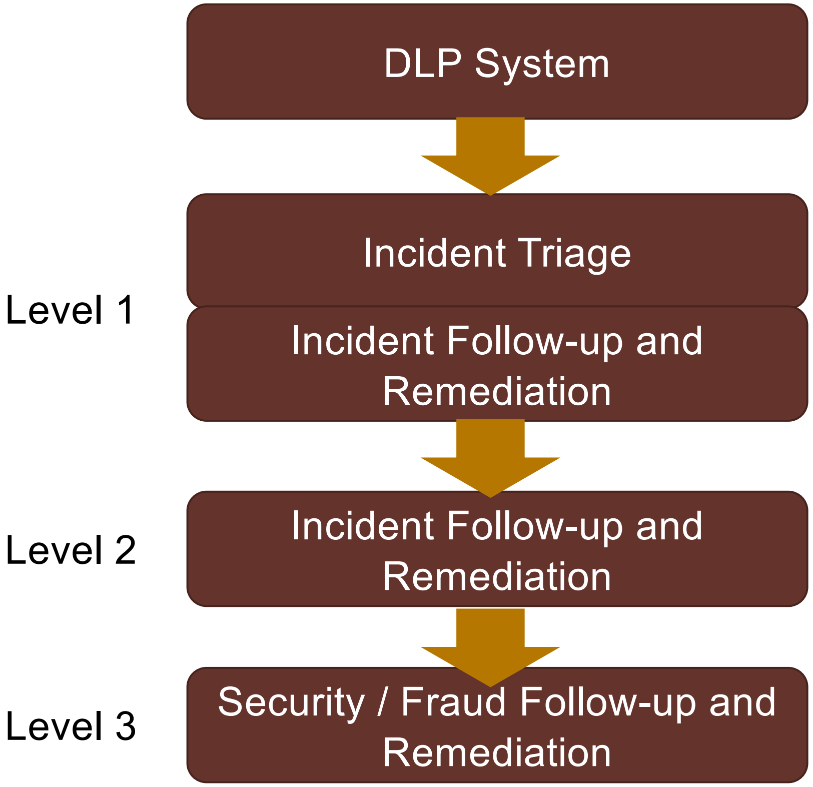
Why is Event Management a big item in DLP?

- 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



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

EVENT HANDLING MODELS


DLP System
Level 1
Incident Triage
Incident Follow-up and Remediation
Level 2
Incident Follow-up and Remediation
Level 3
Security / Fraud Follow-up and Remediation

example

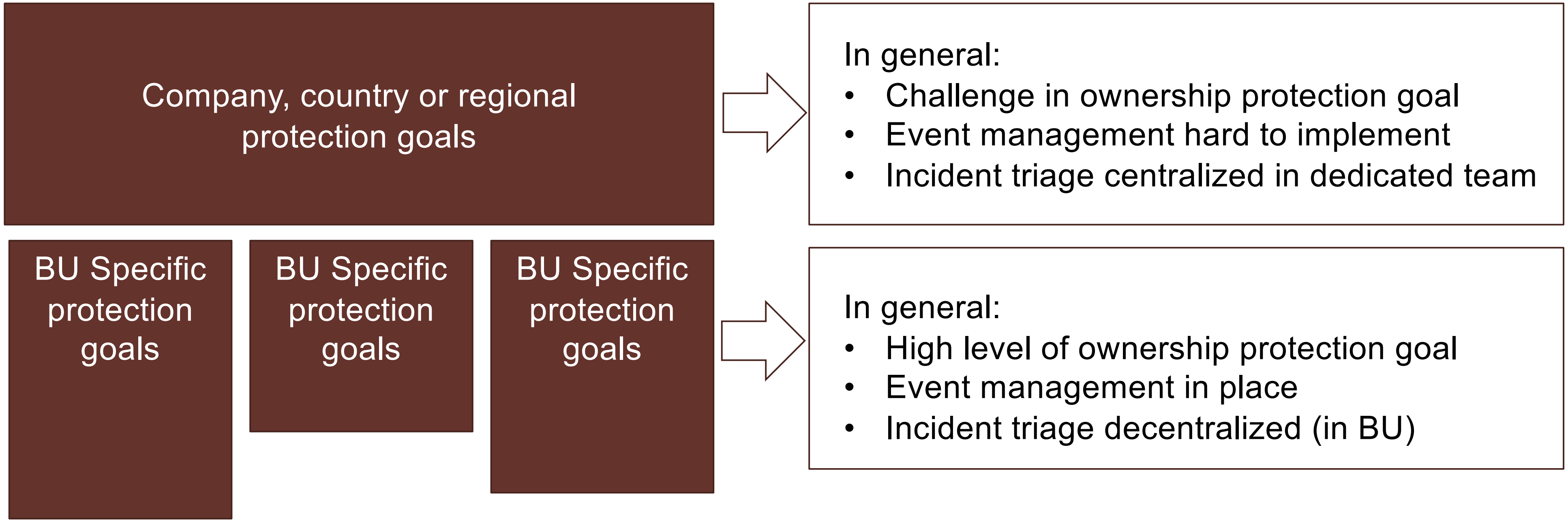
The Event management can differ from on policy to the other

Depending on :

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

Multiple models will run next to each other

Related to Central and decentral Protection Goals



Company, country or regional protection goals

In general:

- Challenge in ownership protection goal
- Event management hard to implement
- Incident triage centralized in dedicated team

BU Specific protection goals

BU Specific protection goals

BU Specific protection goals

In general:

- High level of ownership protection goal
- Event management in place
- Incident triage decentralized (in BU)

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

KEEP
CALM
AND
LET'S
RECAP

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