DATA

UNLEASHING VALUE, EMPOWERING SECURITY AND DRIVING AI ADVANCEMENTS

Cyberday.lu | 12th October 2023

codit

telindus
CYBERSECURITY

Who we are

Eva GRAM

Head of Codit Luxembourg

codit

Cédric MAUNY

Strategic Advisor, Cybersecurity

telindus

CYBERSECURITY

Data was known to be the “new oil”

and can now even be comparable in value to Uranium

codit | telindus CYBERSECURITY

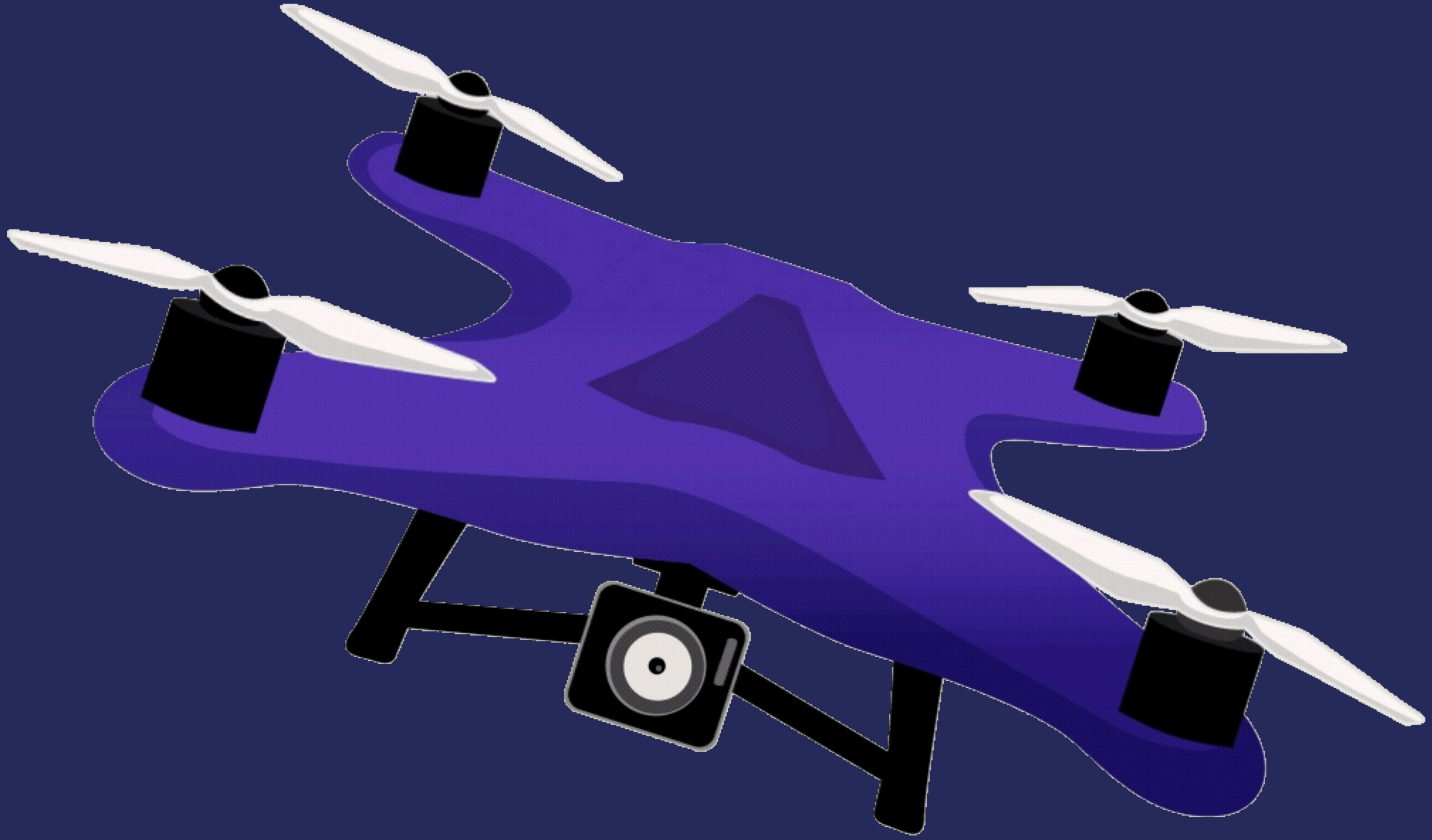
AI needs power… A lot of power

What is AI?

The importance of data

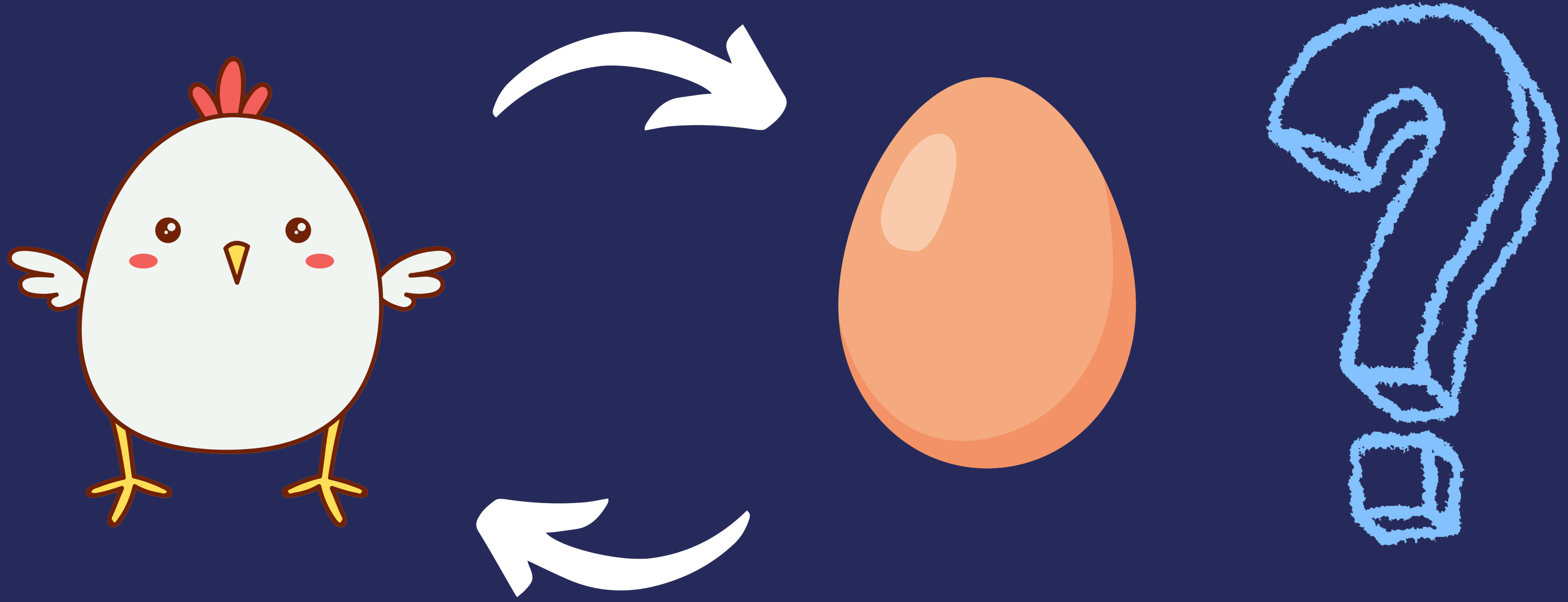
Your data is valuable: either financially…

…either for the data itself



Business produces data...

and data needs to be correctly valorized to create business value



The importance of good data

SHIT IN

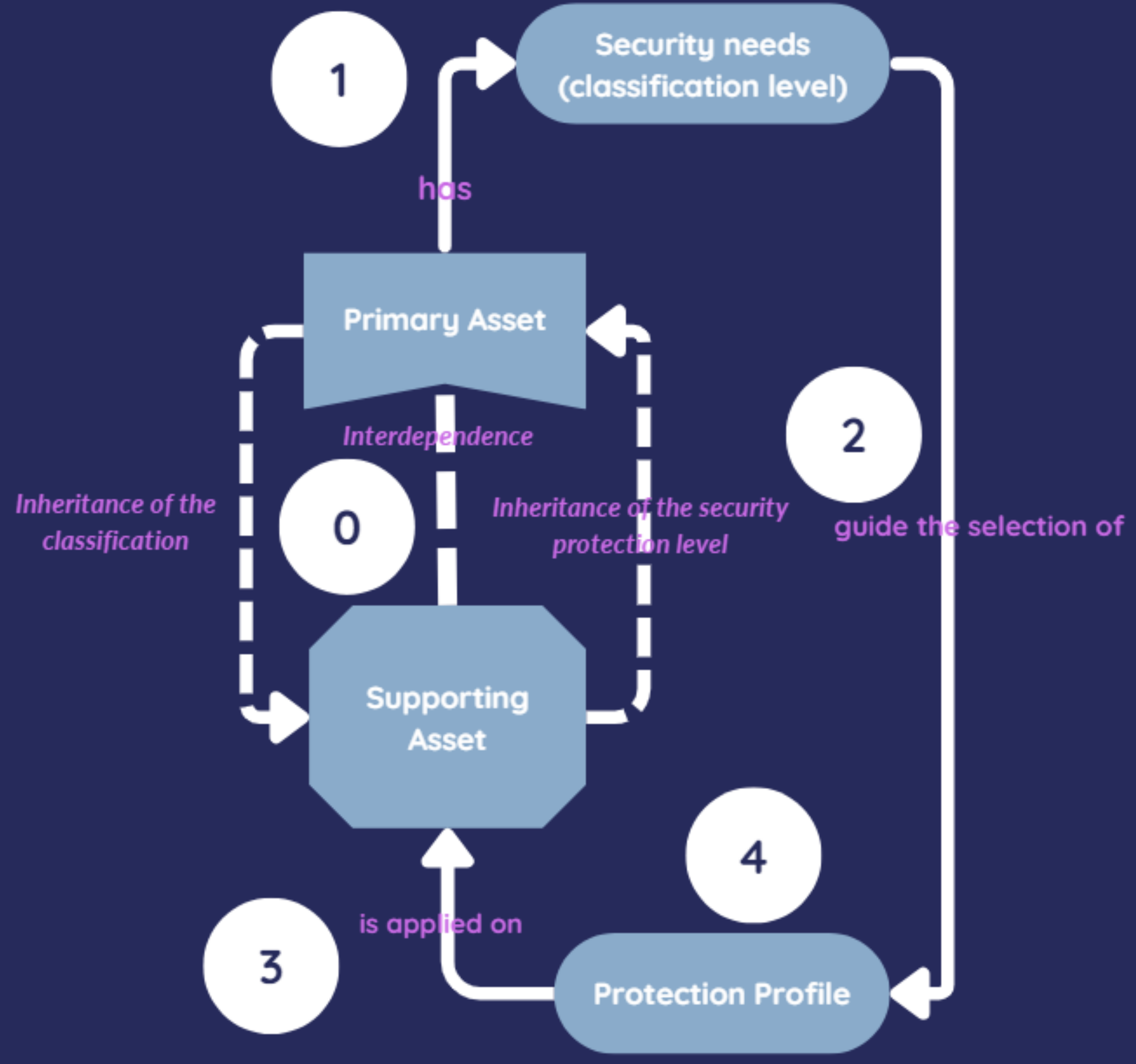
SHIT OUT

Collaboration is key

Employees become stakeholders of the data

WITH GREAT
POWER
COMES GREAT
RESPONSIBILITY
PETER PARKER is SPIDER MAN

The duty of protecting data (appropriately)



1
Security needs (classification level)
has
Primary Asset
Interdependence
0
Inheritance of the classification
Inheritance of the security protection level
2
guide the selection of
Supporting Asset
4
is applied on
3
Protection Profile

Formula of risk is known

$$Risk = Threat\ x\ Vulnerability\ x\ Impact$$

where $Impact = f(Valeur_{Data})$

We all need to keep a control over Risks

Right question is not

Am I secure?

but

Am I confident with my level of risk?

100% security does not exist

Data has security needs to be expressed in terms of confidentiality, integrity, availability (and traceability) for the business → **Security classification**

+

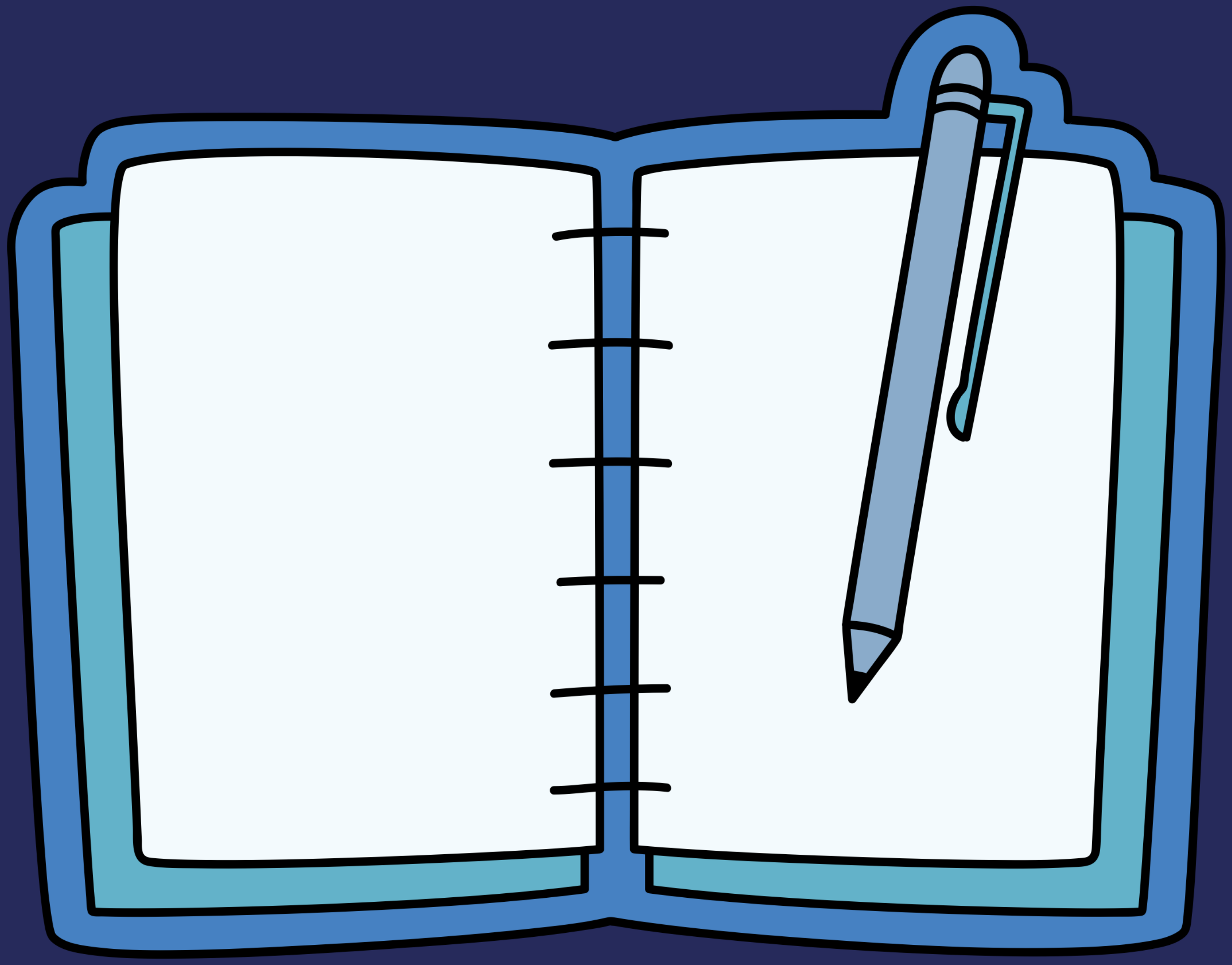
Data shall be protected commensurately to its value for the company → We need to **implement the right security protection at the right time**

codit | telindus CYBERSECURITY

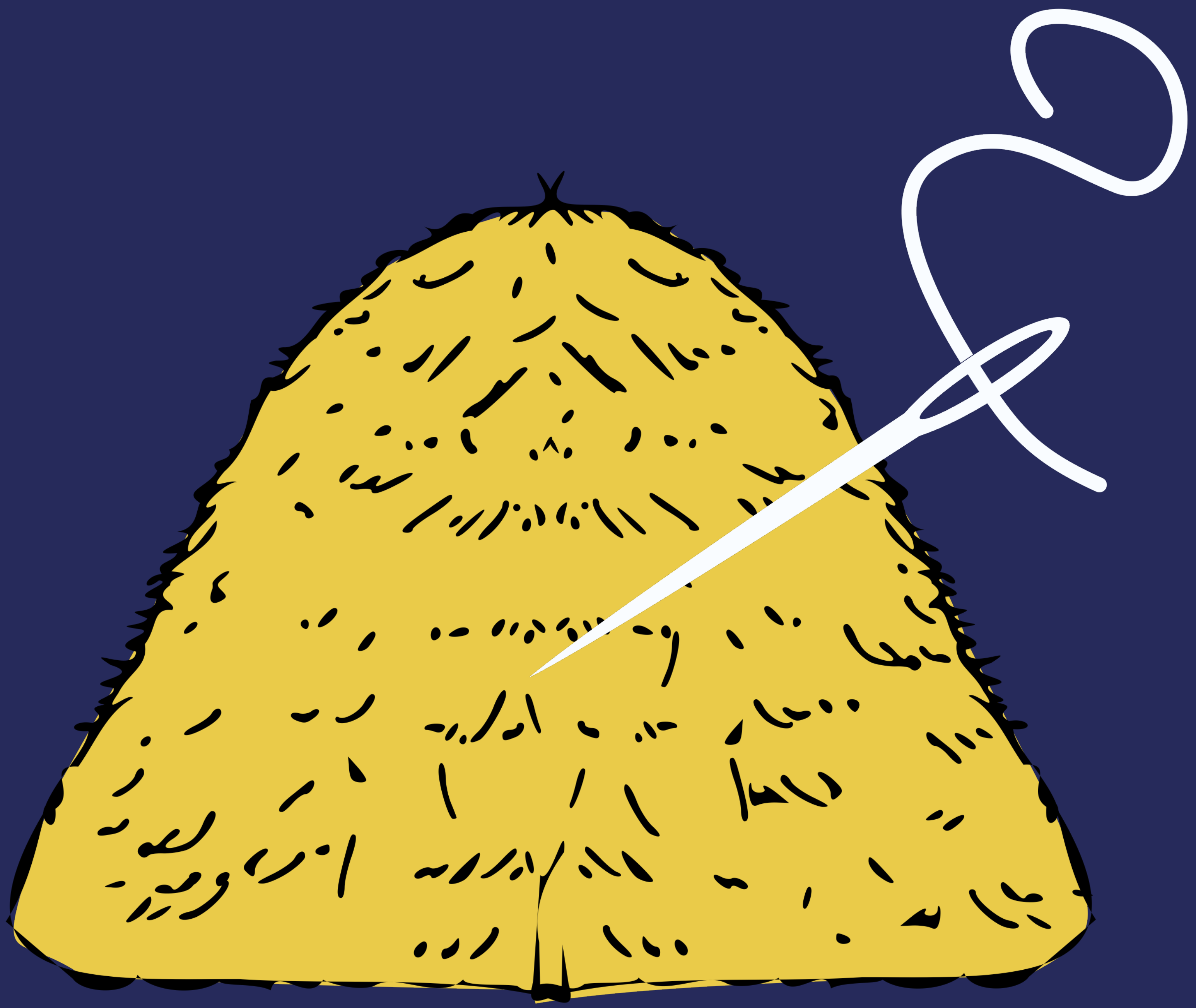
Leaks are bad

codit | telindus CYBERSECURITY

Minimise the volume of collected and processed data

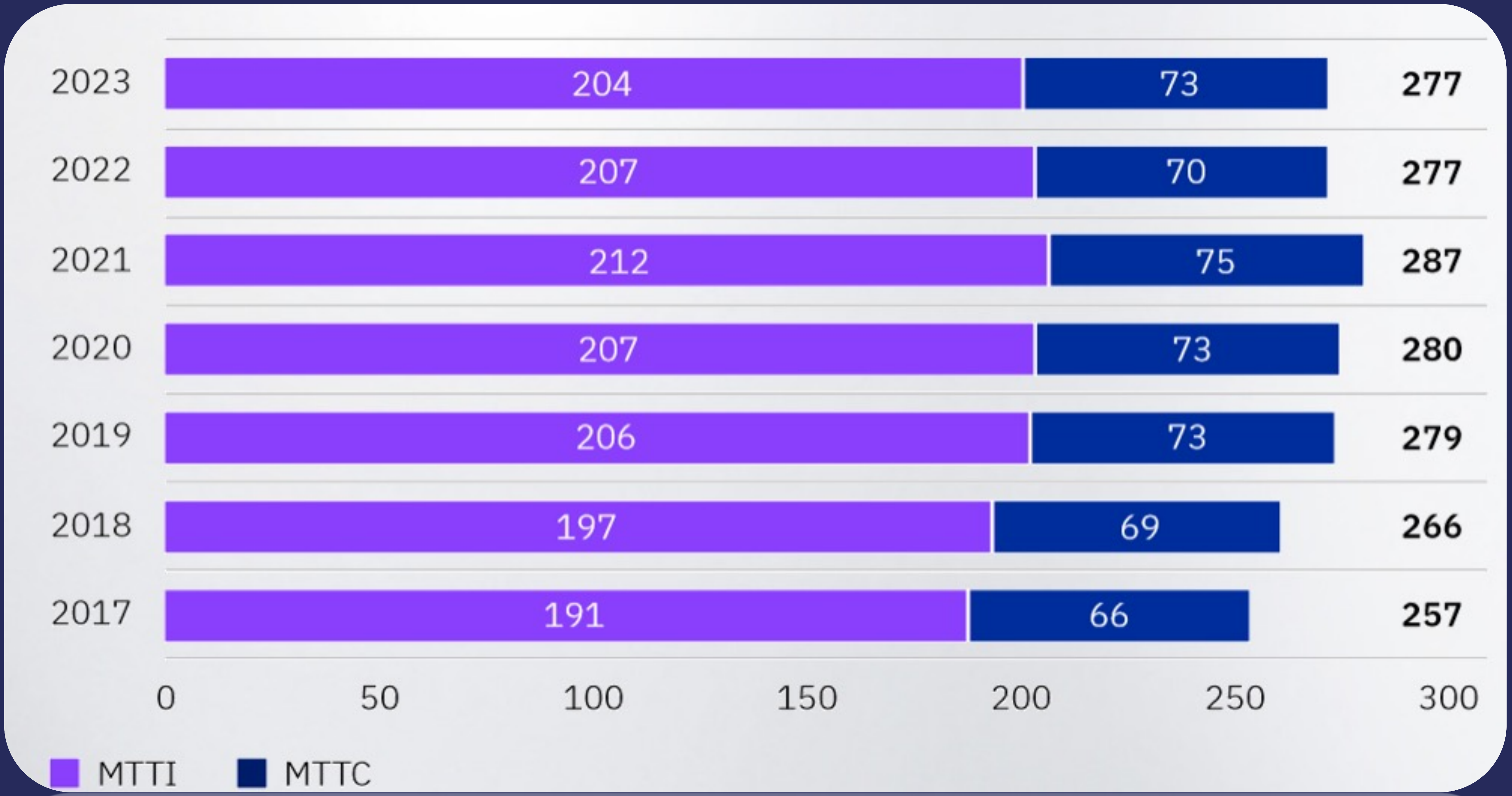


Focus on the relevant data from security perspective



codit | telindus CYBERSECURITY

Time to *uncover a security breach + to resolve it* is still too long



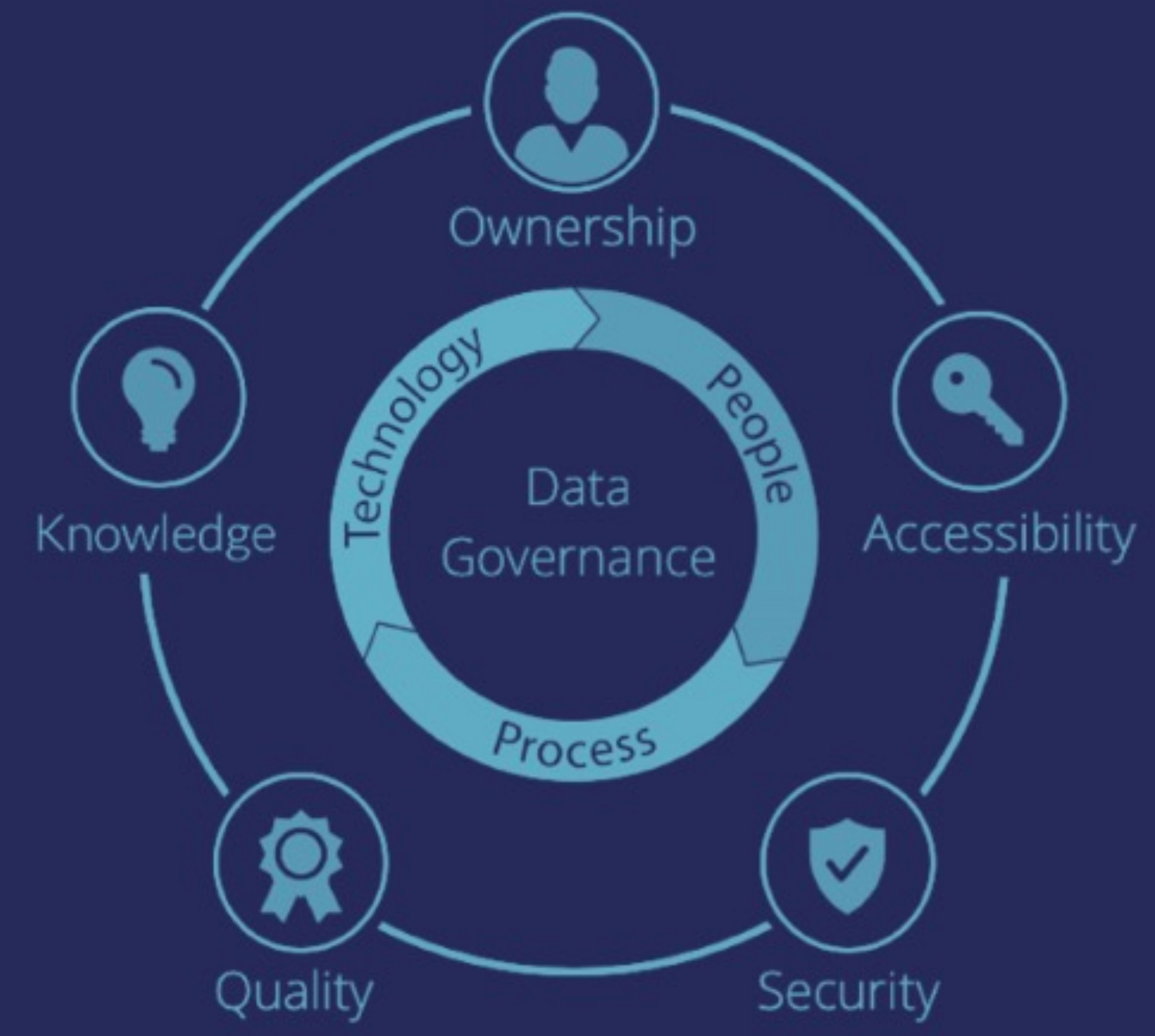
Mean Time To Identify refers to the time it takes an organization to uncover a security breach
Mean Time To Contain refers to the time required to resolve a security breach once it has been identified

We are counting days here… not hours…

IBM **Security**

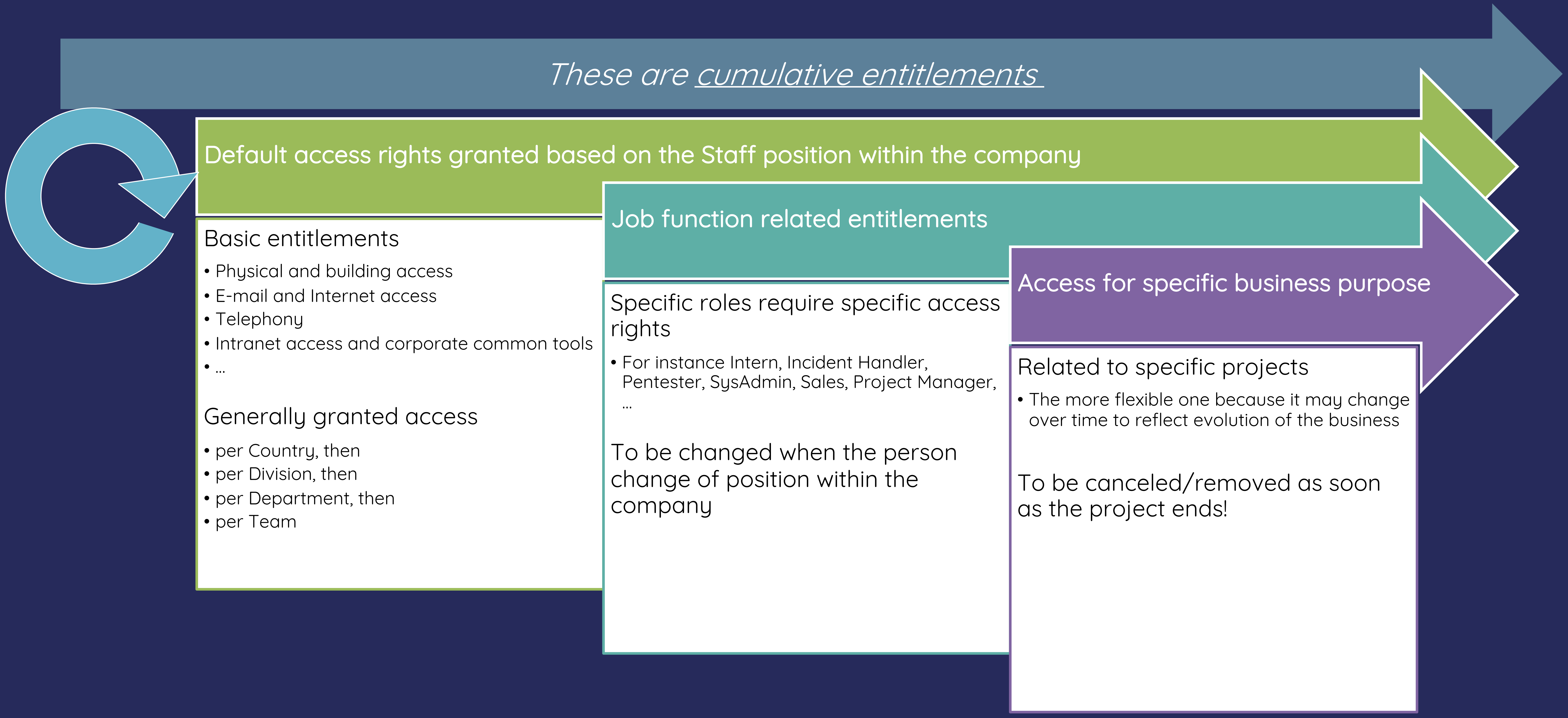
Cost of a Data Breach Report 2023

Data maturity model



Address the risk of inheritance of access rights

A data governance framework that establishes data ownership, roles and responsibilities is enforced with the right control of the access rights to data



These are <u>cumulative entitlements</u>

Default access rights granted based on the Staff position within the company

Basic entitlements

- Physical and building access
- E-mail and Internet access
- Telephony
- Intranet access and corporate common tools
- …

Generally granted access

- per Country, then
- per Division, then
- per Department, then
- per Team

Job function related entitlements

Specific roles require specific access rights

- For instance Intern, Incident Handler, Pentester, SysAdmin, Sales, Project Manager, …

To be changed when the person change of position within the company

Access for specific business purpose

Related to specific projects

- The more flexible one because it may change over time to reflect evolution of the business

To be canceled/removed as soon as the project ends!

Being data driven is mandatory

The preliminary step for driving AI

codit | telindus CYBERSECURITY

Conclusion

Don’t underestimate the power of the data

codit | telindus
CYBERSECURITY

Eva GRAM
eva.gram@codit.eu
(+352) 691 077 164

Cédric MAUNY
cedric.mauny@telindus.lu
(+352) 621 200 707

codit

telindus
CYBERSECURITY