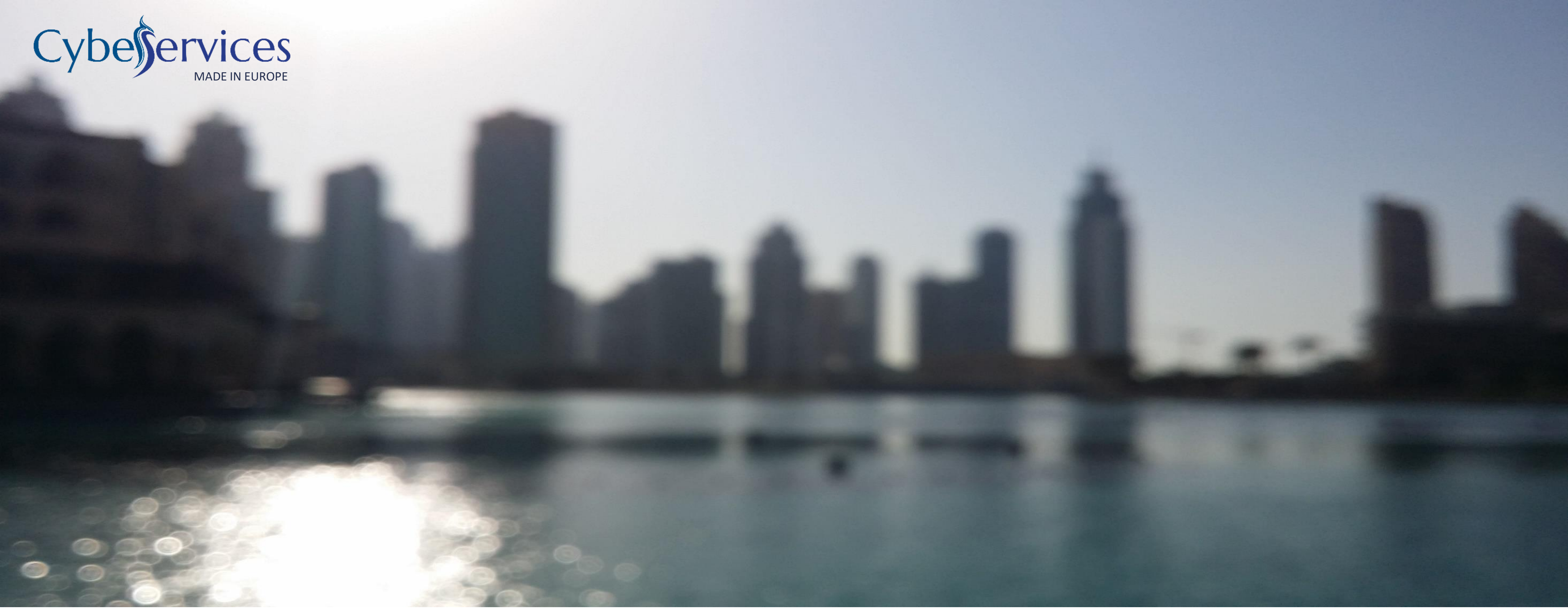


Security big data analysis – What is it really good for? The more the merrier?

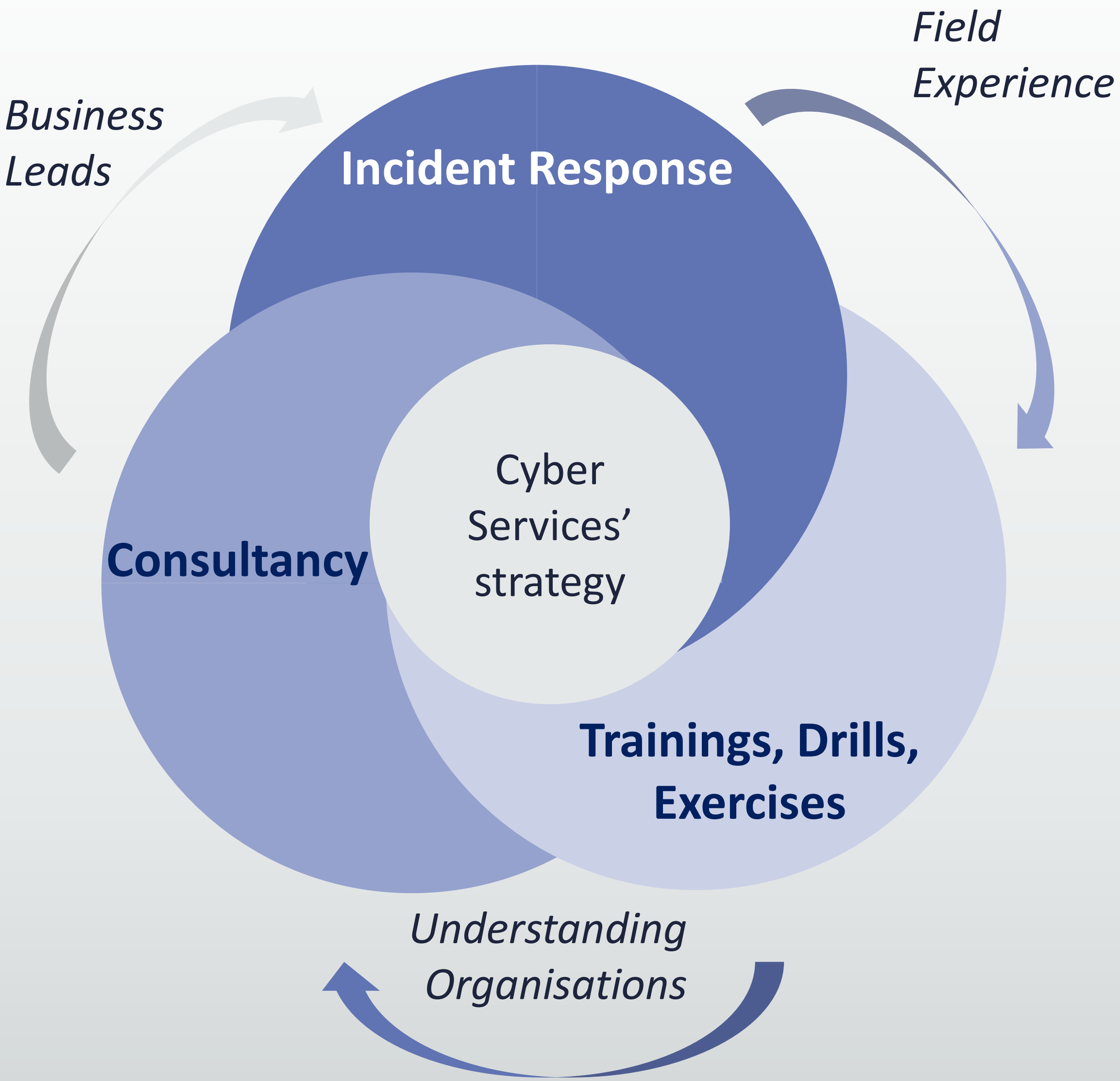
Anett Mádi-Nátor

About Cyber Services

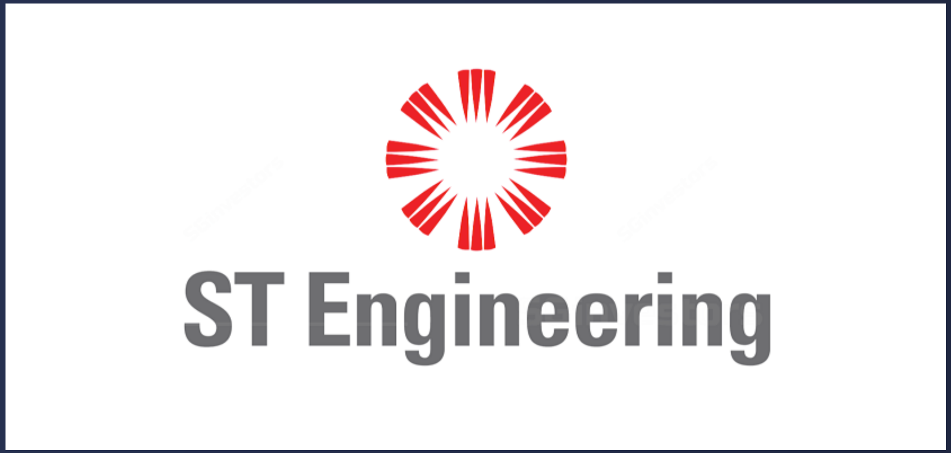
Cyber Services PLC is a knowledge based cyber security service provider active in the field of establishing controllable and predictable processes in the cyberspace.

As such, Cyber Services provides proactive cyber security primarily for larger commercial entities (critical infrastructure), multinational organisations, and governments internationally.

Partners: UN ITU, European Cyber Security Organisation, NATO Cyber Range, Hong Kong Productivity Council, Microsoft, law enforcement, national security agencies, national CERTs /CSIRTs



Our Partners



Our Collaboration

Founding Member of European Cyber Security Organisation
Member of Board, Special Advisor to Secretary General
Women4Cyber Initiative – Private lead for W4C Foundation

A PARTNERSHIP
FOR CYBER SECURITY IN EUROPE

BUILDING TOGETHER
A EUROPEAN
CYBER ECOSYSTEM

ECS
EUROPEAN CYBER SECURITY ORGANISATION

Our Hong Kong Partner

Hong Kong Productivity Council

Topics

Short overview of big data processing methods and typical areas of use, with related security problems

Understanding cyber threat and risk analysis of big data – Impact analysis

Short intro to cyber threat intelligence, overview on different levels, internal and external sources, possibilities and limitations of use of CTI

Internal sources of CTI

- How does log management support cybersecurity of big data? A use case
- How does system monitoring support cybersecurity of big data? A use case

Automated log analysis with statistical features and artificial intelligence – do these provide a feasible solution and a handy future for big data analysts to secure their systems?

Data has become a new ”natural” resource

data is the new oil

we need to find it, extract it, refine it, distribute it and monetize it.

David Buckingham

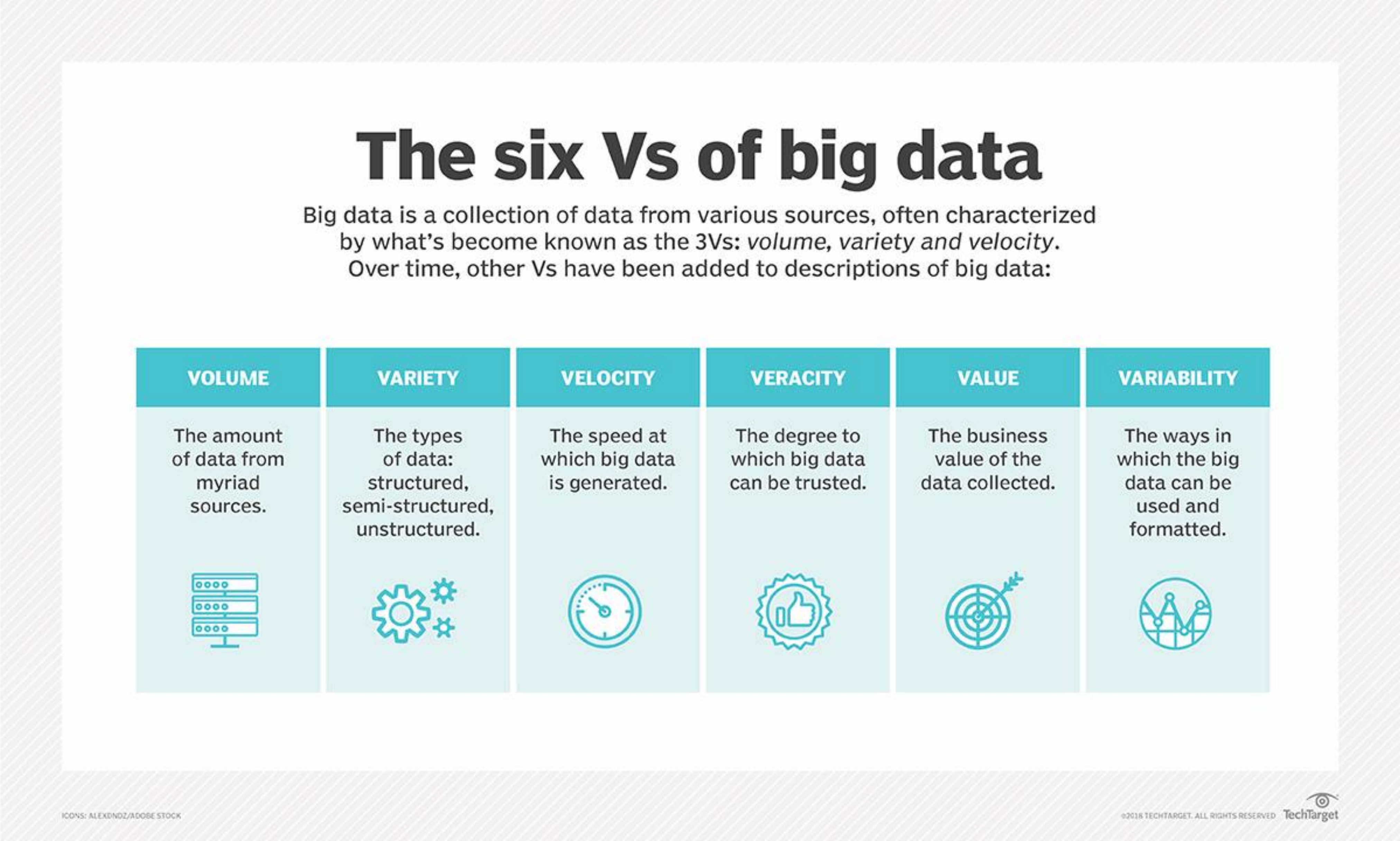
2016

Data has become RISK

2021

CyberServices
MADE IN EUROPE

What is Big Data?



The six Vs of big data

Big data is a collection of data from various sources, often characterized by what's become known as the 3Vs: *volume, variety and velocity*. Over time, other Vs have been added to descriptions of big data:

VOLUME	VARIETY	VELOCITY	VERACITY	VALUE	VARIABILITY
The amount of data from myriad sources.	The types of data: structured, semi-structured, unstructured.	The speed at which big data is generated.	The degree to which big data can be trusted.	The business value of the data collected.	The ways in which the big data can be used and formatted.

ICONS: ALEXDNDZ/ADOBE STOCK

TechTarget

Benefits and Advantages of Big Data & Analytics in Business
A General Approach

- **Cost** optimization.
- Improve **efficiency**.
- Foster **competitive pricing**.
- **Boost sales** and retain customer loyalty.
- **Innovate**.
- Focus on the local environment.
- **Control and monitor** online reputation.

MEANWHILE

CyberServices
MADE IN EUROPE

Big Data vs Cybersecurity

On February 2, 2021 user Singularity0x01 created a thread on the popular English-language cybercriminal forum RaidForums titled ‘Compilation of Many Breaches’ (COMB)

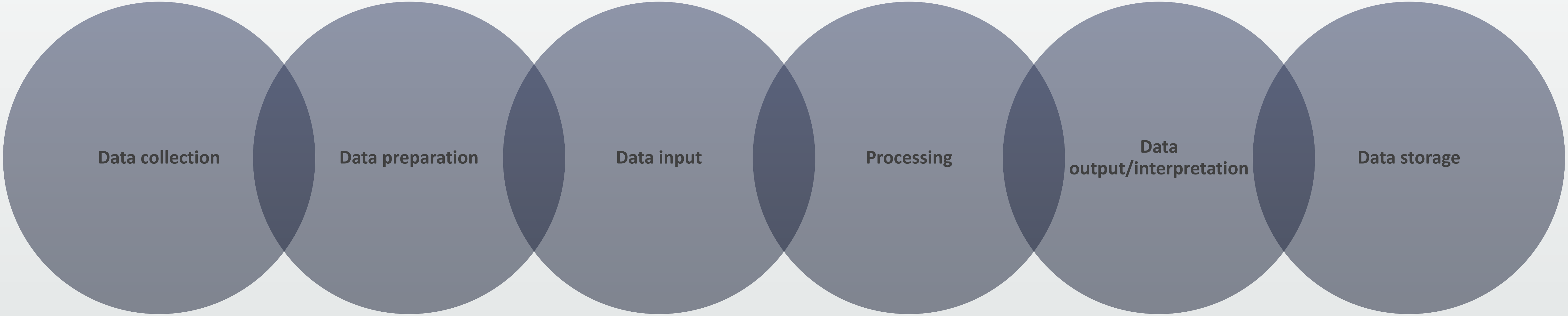
Size of Breach is 3.8 Billion

Hungary – 5 Million records

Hong Kong – 1.7M records, main target is education sector (.com domain records are not counted here)

Big Data security is the processing of guarding data and analytics processes, both in the cloud and on-premise, from any number of factors that could compromise their confidentiality.

Six stages of data processing



Data collection

Data preparation

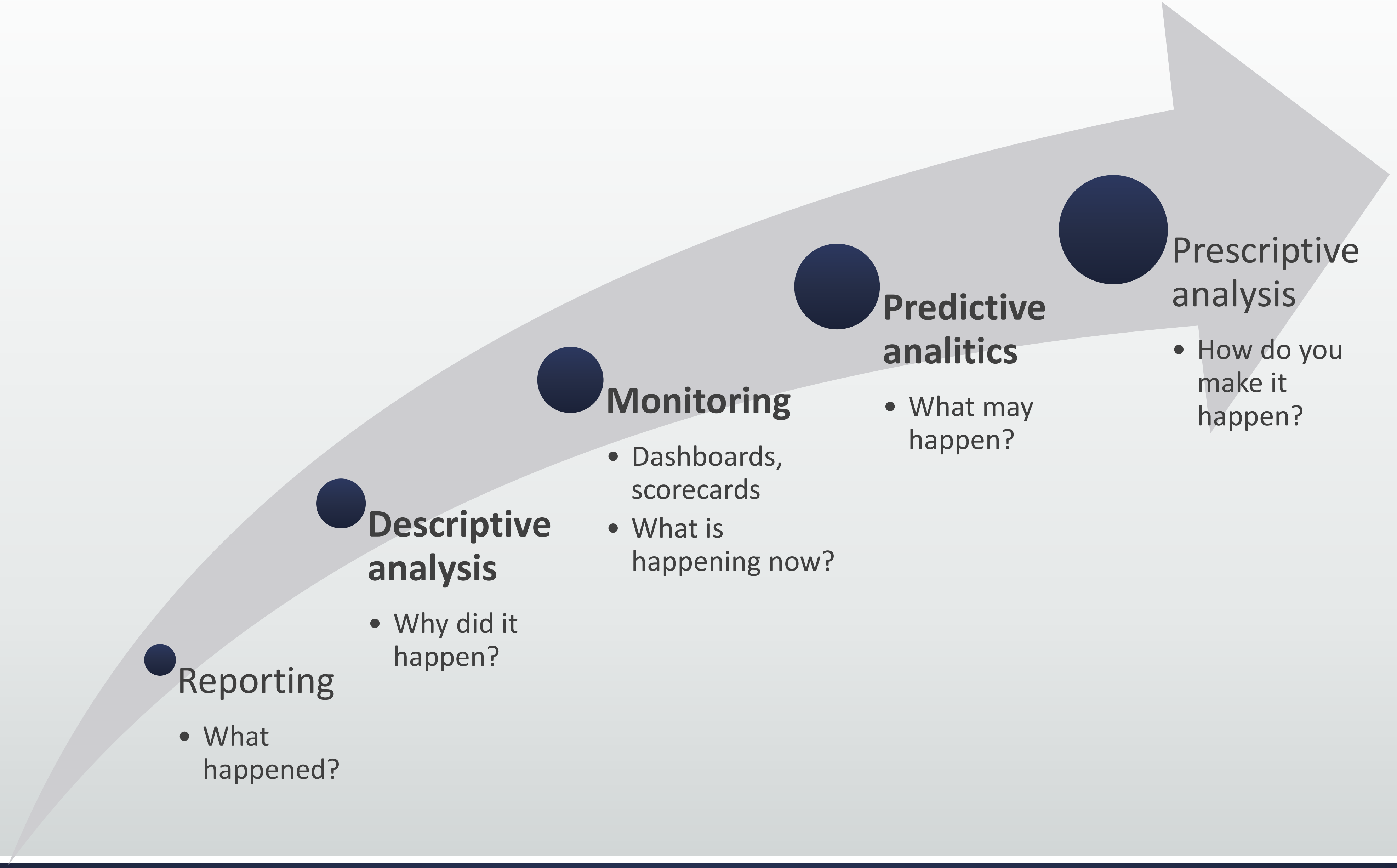
Data input

Processing

Data output/interpretation

Data storage

Evolution of analysis



Reporting

- What happened?

Descriptive analysis

- Why did it happen?

Monitoring

- Dashboards, scorecards
- What is happening now?

Predictive analitics

- What may happen?

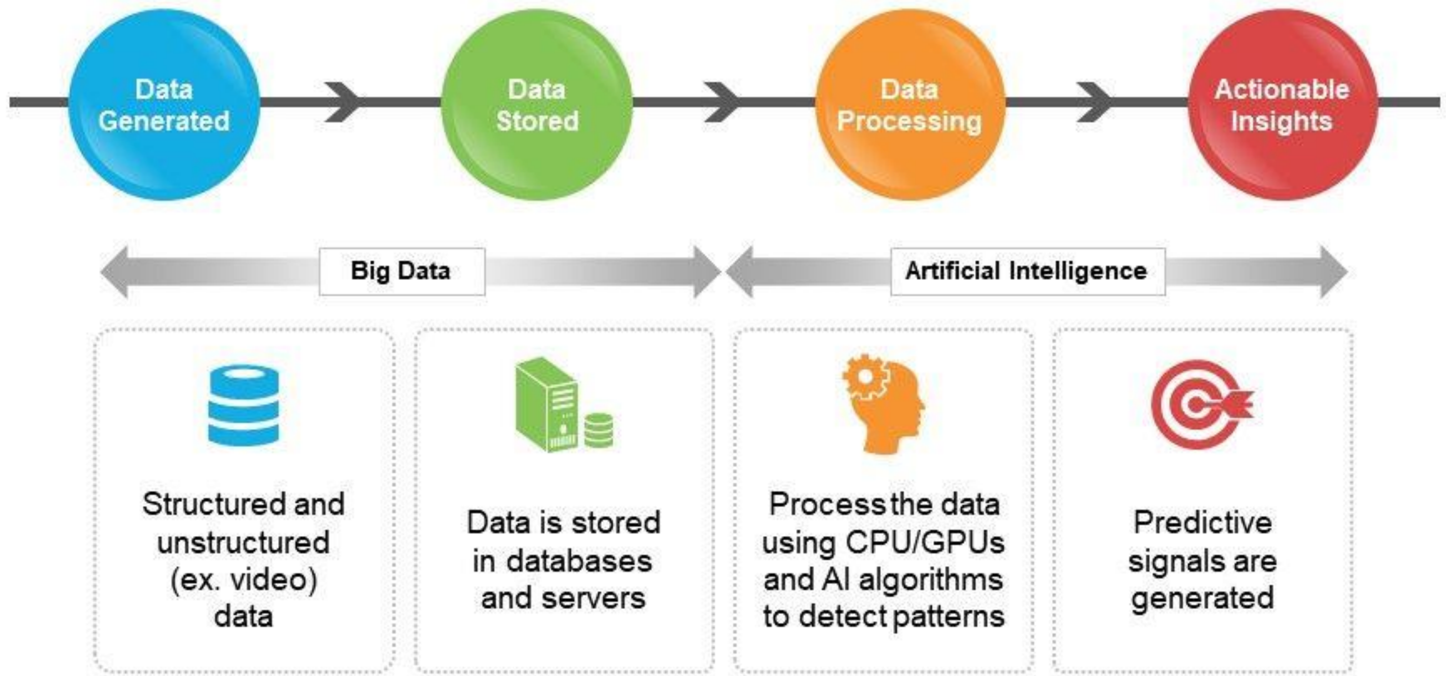
Prescriptive analysis

- How do you make it happen?

Big data and Artificial Intelligence – Predictive Analysis

Artificial Intelligence AI Process Data Generated To Actionable Insights

CYBER SECURITY using BIG DATA



Data Generated → Data Stored → Data Processing → Actionable Insights

Big Data

Artificial Intelligence

Structured and unstructured (ex. video) data

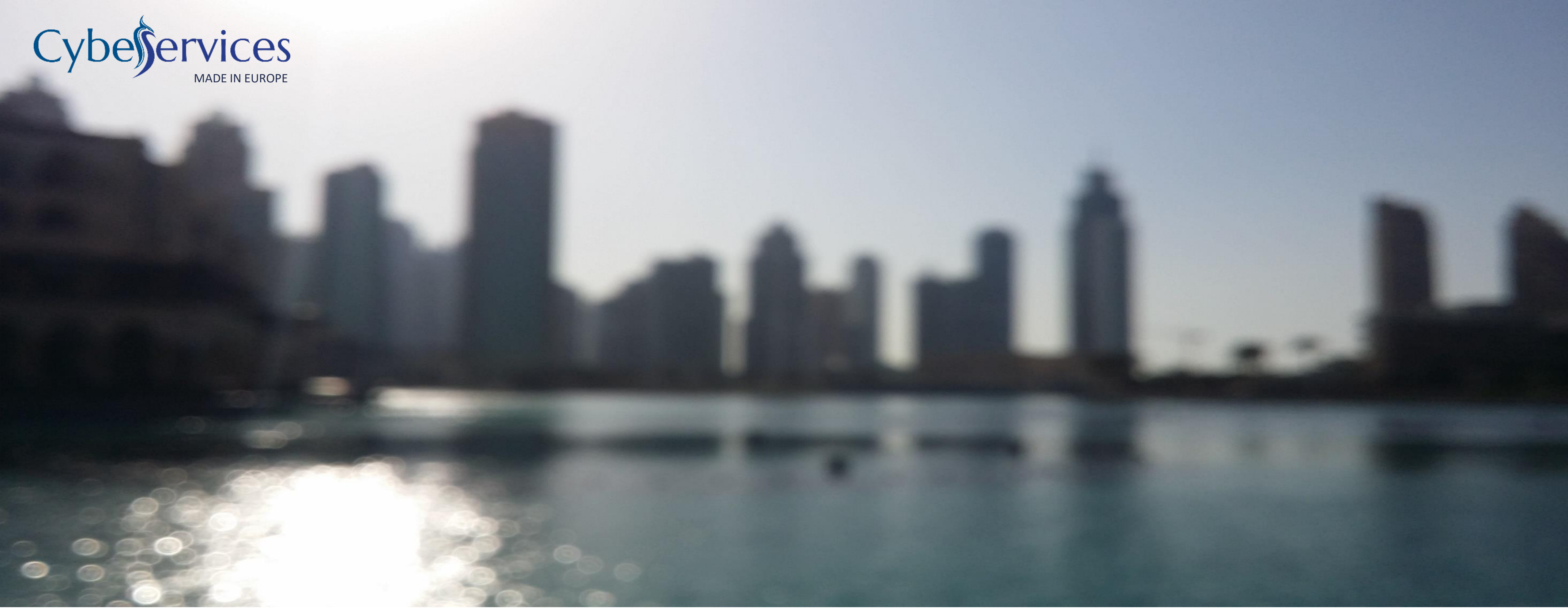
Data is stored in databases and servers

Process the data using CPU/GPUs and AI algorithms to detect patterns

Predictive signals are generated

CYBER SECURITY ON BIG DATA

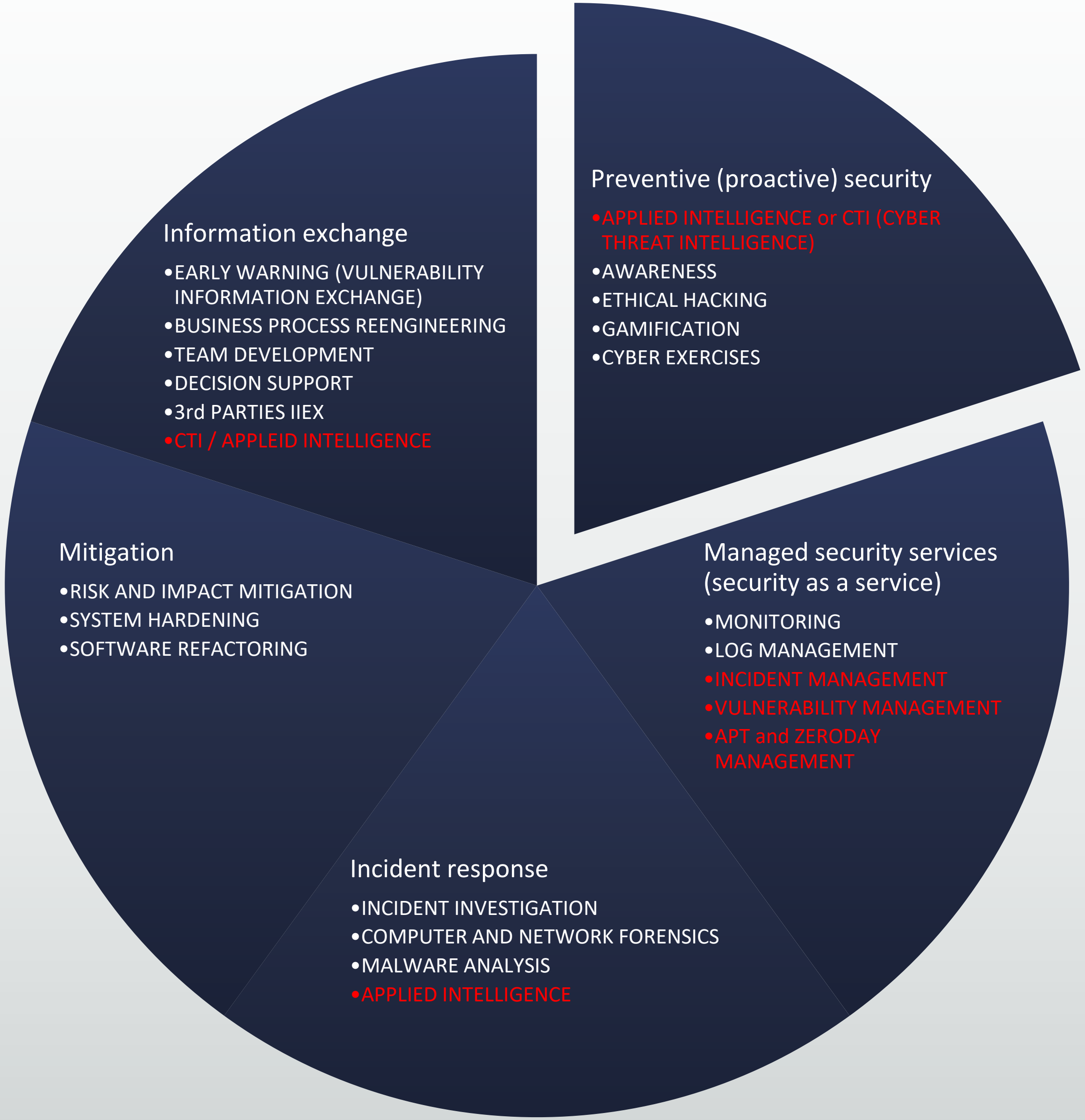
CyberServices
MADE IN EUROPE



How do these all support **CYBERsecurity** of Big Data?

CyberServices
MADE IN EUROPE

Cyber security services in a healthy lifecycle – RED are weaker or missing capabilities



Preventive (proactive) security

- APPLIED INTELLIGENCE or CTI (CYBER THREAT INTELLIGENCE)
- AWARENESS
- ETHICAL HACKING
- GAMIFICATION
- CYBER EXERCISES

Managed security services (security as a service)

- MONITORING
- LOG MANAGEMENT
- INCIDENT MANAGEMENT
- VULNERABILITY MANAGEMENT
- APT and ZERODAY MANAGEMENT

Incident response

- INCIDENT INVESTIGATION
- COMPUTER AND NETWORK FORENSICS
- MALWARE ANALYSIS
- APPLIED INTELLIGENCE

Mitigation

- RISK AND IMPACT MITIGATION
- SYSTEM HARDENING
- SOFTWARE REFACTORING

Information exchange

- EARLY WARNING (VULNERABILITY INFORMATION EXCHANGE)
- BUSINESS PROCESS REENGINEERING
- TEAM DEVELOPMENT
- DECISION SUPPORT
- 3rd PARTIES IIEX
- CTI / APPLEID INTELLIGENCE

Preventive (proactive) security with CTI

APPLIED INTELLIGENCE or CTI (CYBER THREAT INTELLIGENCE)

- Monthly, weekly, daily reports
- AD-HOC reports
- IOC definitions

(SITUATIONAL) AWARENESS

- CTI based real life usecases

ETHICAL HACKING

- Vulnerability information about asset as an internal feed to CTI

GAMIFICATION

- CTI based real scenario development

CYBER EXERCISES

- CTI based real geopolitical and technical scenario development
- Lessons learned information as a feed to CTI

Managed security services with CTI

MONITORING

- Metrics as a feed to CTI

LOG MANAGEMENT

- Events feed to CTI

INCIDENT MANAGEMENT

- CTI related incident handling – AD-HOC reports
- Incident information as a feed to CTI

VULNERABILITY MANAGEMENT

- Vulnerability feed from the CTI
- Asset information as a feed to CTI

APT and ZERODAY MANAGEMENT

- APT related CTI reports
- Zeroday information related CTI reports

Incident response with CTI

INCIDENT INVESTIGATION

- IoC related CTI analyses, AD-HOC reports
- New IoC definitions

COMPUTER AND NETWORK FORENSICS

- IoC related CTI analyses, AD-HOC reports
- New IoC definitions

MALWARE ANALYSIS

- IoC related CTI analyses, AD-HOC reports
- New IoC definitions

Mitigation with CTI

RISK AND IMPACT MITIGATION

- CTI based risk and business impact analyses

SYSTEM HARDENING

- Asset and vulnerability information based CTI advisories

SOFTWARE REFACTORING

- Asset and vulnerability information based CTI advisories

Information exchange with CTI

EARLY WARNING (VULNERABILITY INFORMATION EXCHANGE)

- Asset and sector based CTI reports

BUSINESS PROCESS REENGINEERING

- Sector based CTI reports

TEAM DEVELOPMENT

- CTI related trainings and capability building

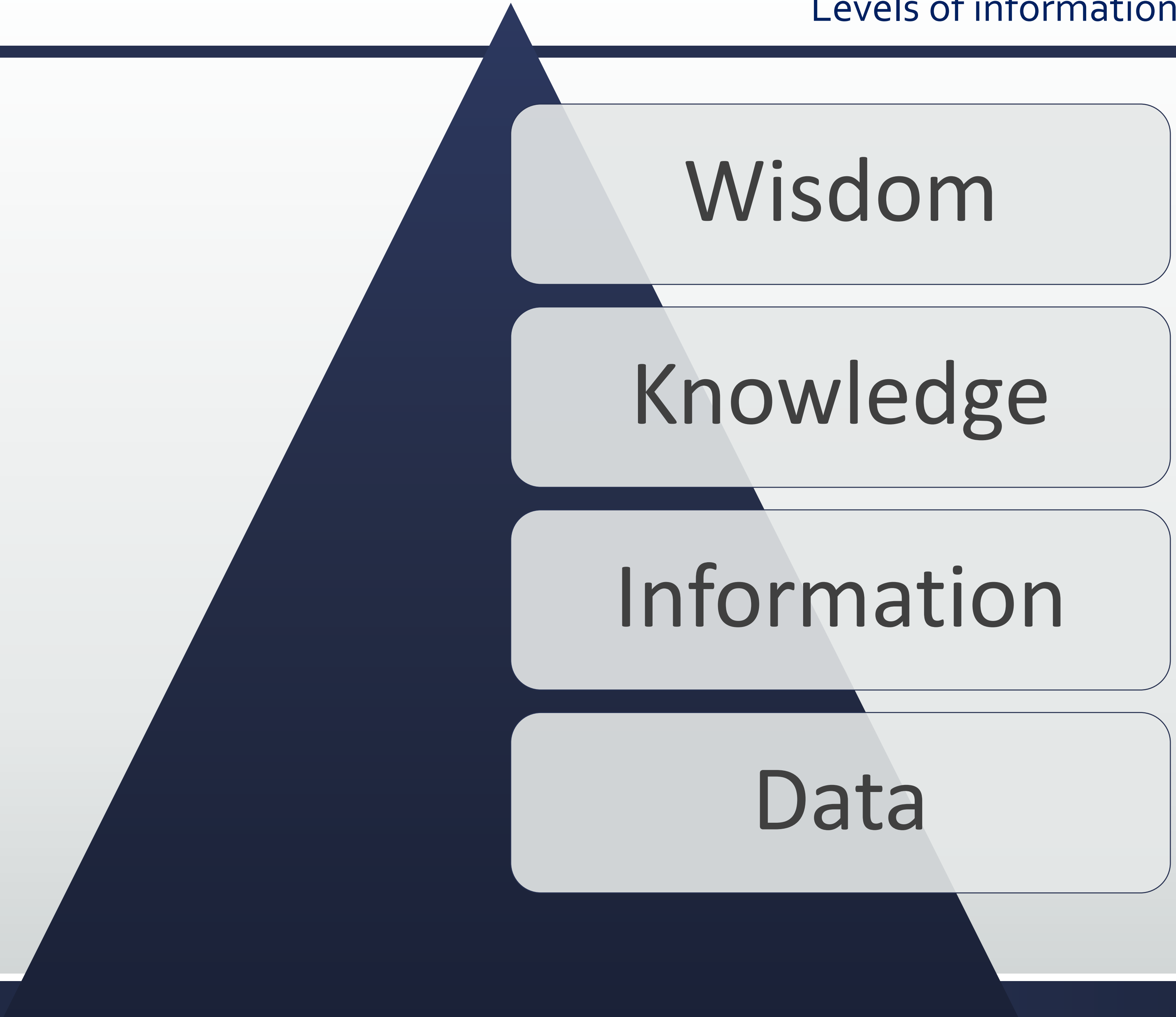
DECISION SUPPORT

- General and sectorial CTI reports

3rd PARTIES IIEX

- CTI based (incident) information exchange

Levels of information – Data evolution



Wisdom

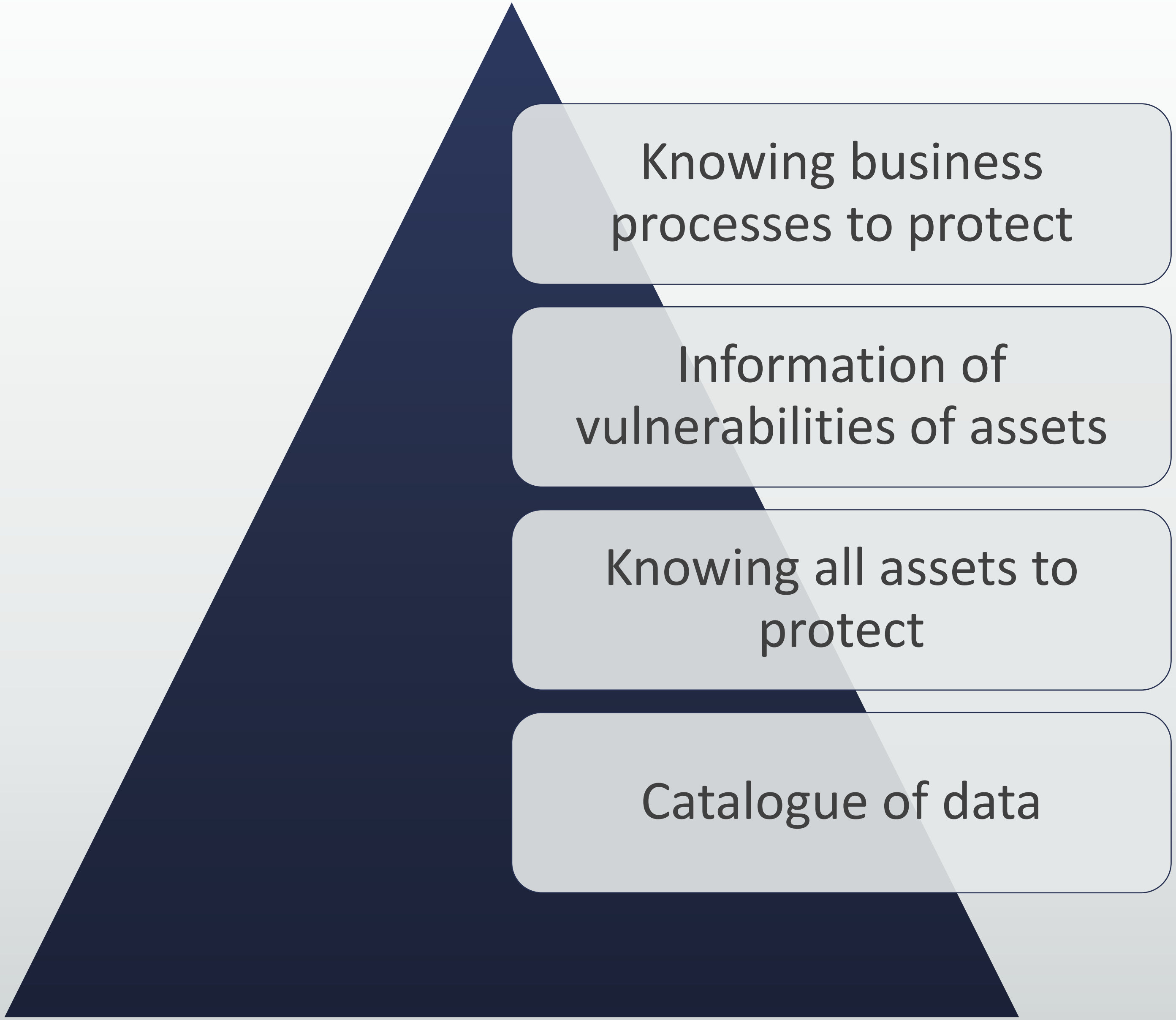
Knowledge

Information

Data

CyberServices MADE IN EUROPE

Missing standpoints



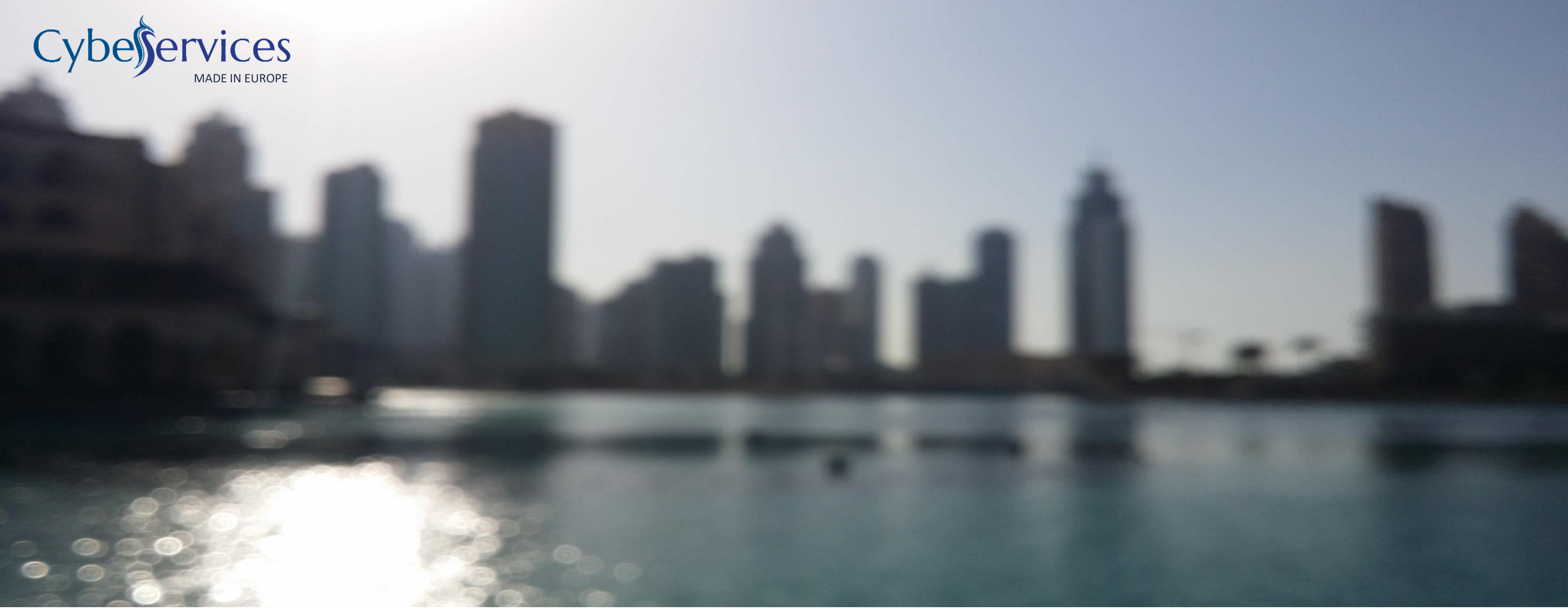
Knowing business processes to protect

Information of vulnerabilities of assets

Knowing all assets to protect

Catalogue of data

CyberServices
MADE IN EUROPE



Thank you for your attention