EUROPEAN UNION AGENCY
FOR CYBERSECURITY

PUTTING AI IN THE EU CYBER CRISIS COLLABORATION

CDR (ret) Georgios Chatzichristos
Operational Security Unit - ENISA

03 | 10 | 2019

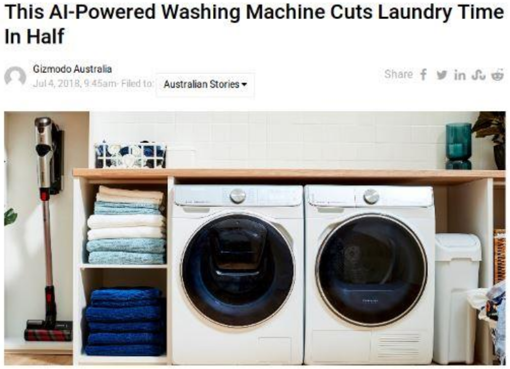
Buzz?

Is it new?

What is it?

Applications?

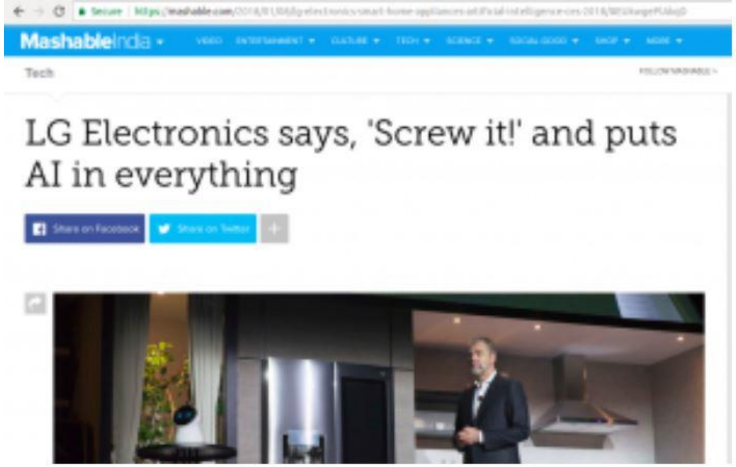
Buzz word



This AI-Powered Washing Machine Cuts Laundry Time In Half

Gizmodo Australia

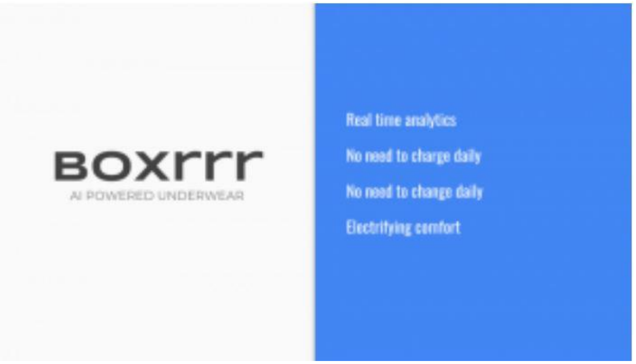
Jul 4, 2018, 9:45am · Filed to: Australian Stories ▾



Tech

LG Electronics says, 'Screw it!' and puts AI in everything

?



BOXrrr

AI POWERED UNDERWEAR

Real time analytics

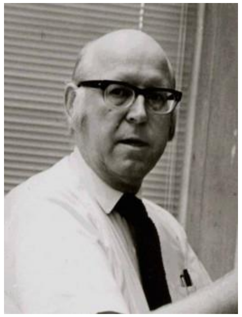
No need to charge daily

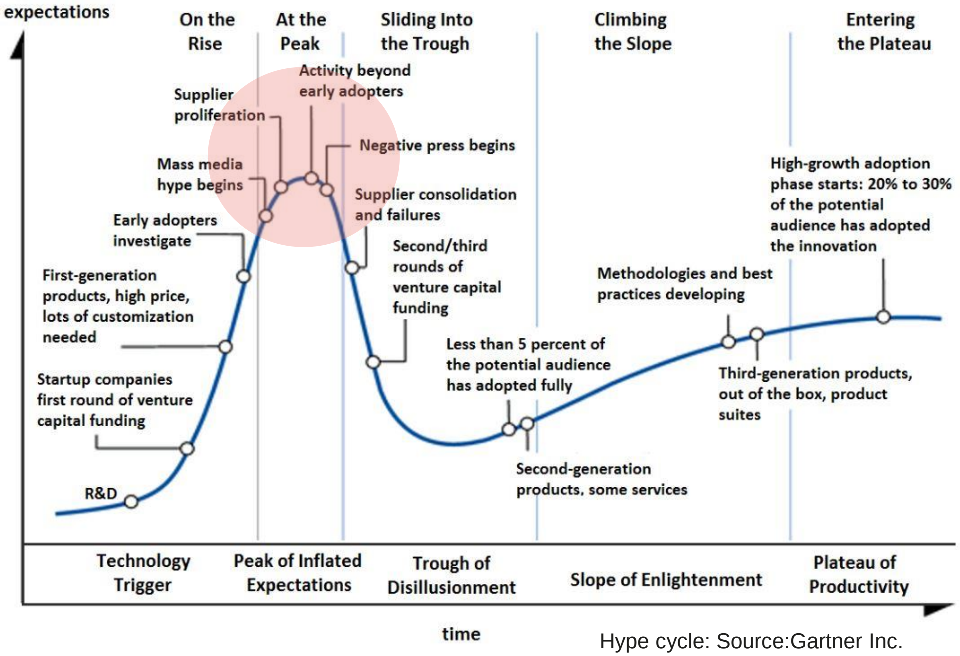
No need to change daily

Electrifying comfort

Is it new?

The invention of digital computers in the 40s led to discussions
on the building of an electronic brain




expectations
On the Rise
At the Peak
Sliding Into the Trough
Climbing the Slope
Entering the Plateau
Activity beyond early adopters
Supplier proliferation
Negative press begins
Mass media hype begins
Supplier consolidation and failures
High-growth adoption phase starts: 20% to 30% of the potential audience has adopted the innovation
Early adopters investigate
Second/third rounds of venture capital funding
First-generation products, high price, lots of customization needed
Methodologies and best practices developing
Less than 5 percent of the potential audience has adopted fully
Startup companies first round of venture capital funding
Third-generation products, out of the box, product suites
R&D
Second-generation products, some services
Technology Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
time

Hype cycle: Source:Gartner Inc.

- The Dartmouth workshop on AI - 1956
- The golden years 1956-1974
- The 1st AI winter 1974-1980 **No money**
- The 2nd AI winter 1987-1993 **No money**
- The 3rd AI winter 2002-2007 **No data**
- The big boom 2008-present **Big data – Cyber - IoT** → **Lots of data !**

TYPES OF AI

Supervised

Goal is to approximate a desired function so that we can predict the output

Classification
Recognition

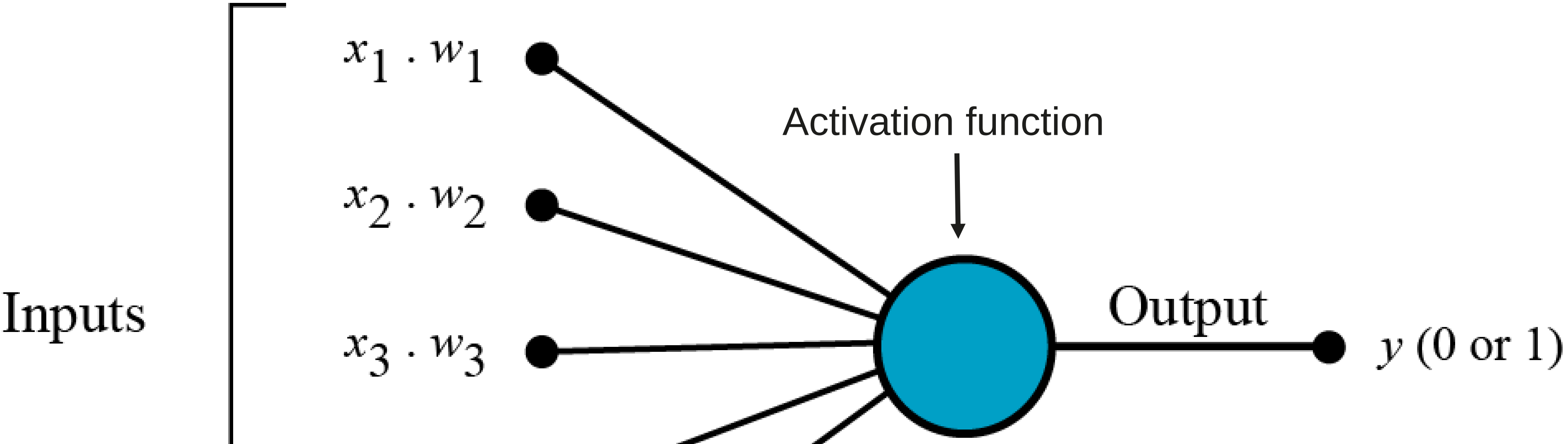
Unsupervised

Goal is to model patterns in given inputs in order to learn about the data

Clustering
Anomaly detection

What is it?

… basically a classifier



Inputs

$x_1 \cdot w_1$

$x_2 \cdot w_2$

$x_3 \cdot w_3$

$x_4 \cdot w_4$

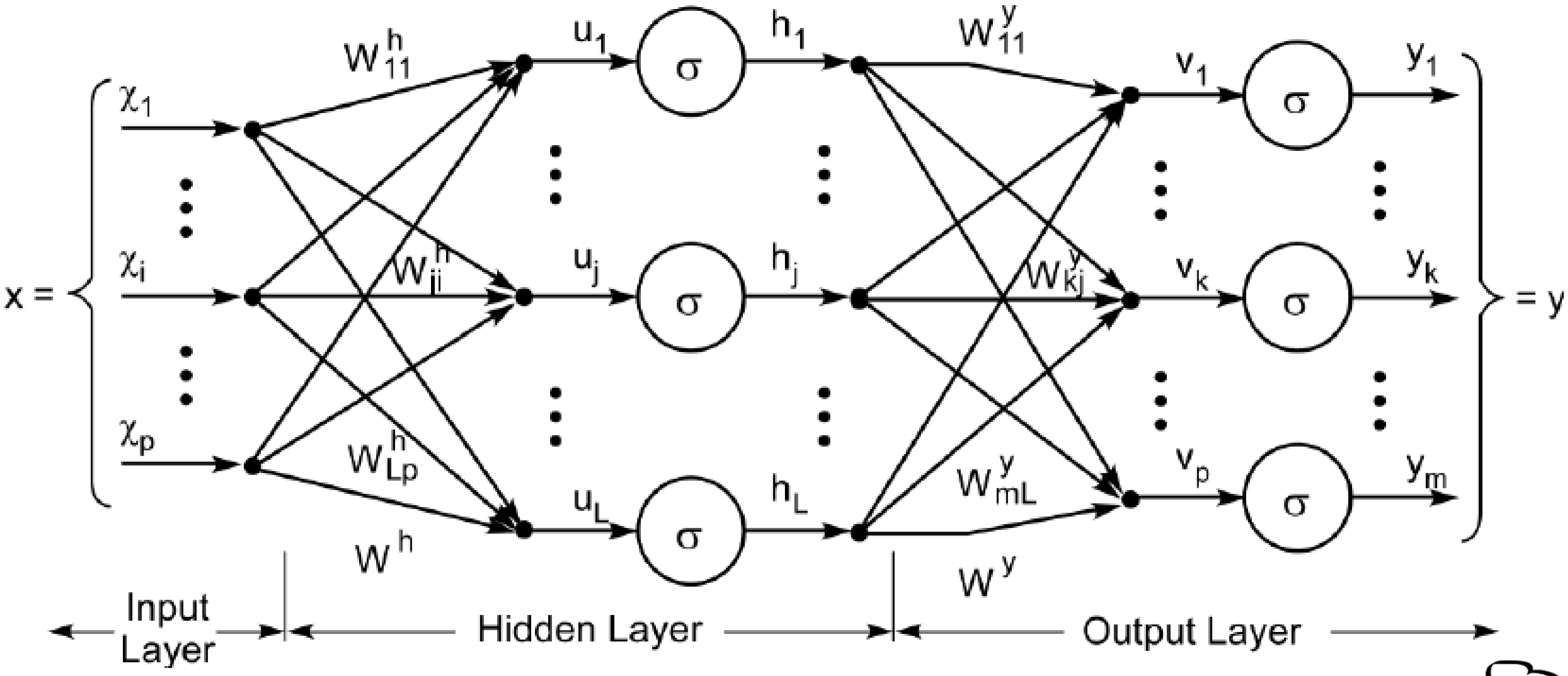
$x_5 \cdot w_5$

Activation function

Output

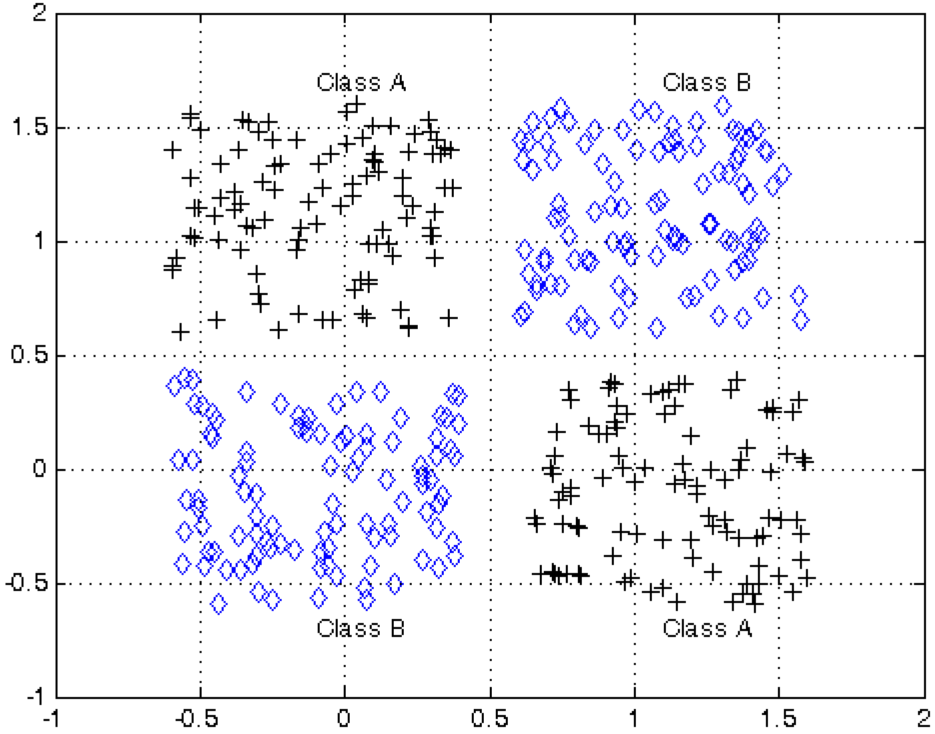
y (0 or 1)

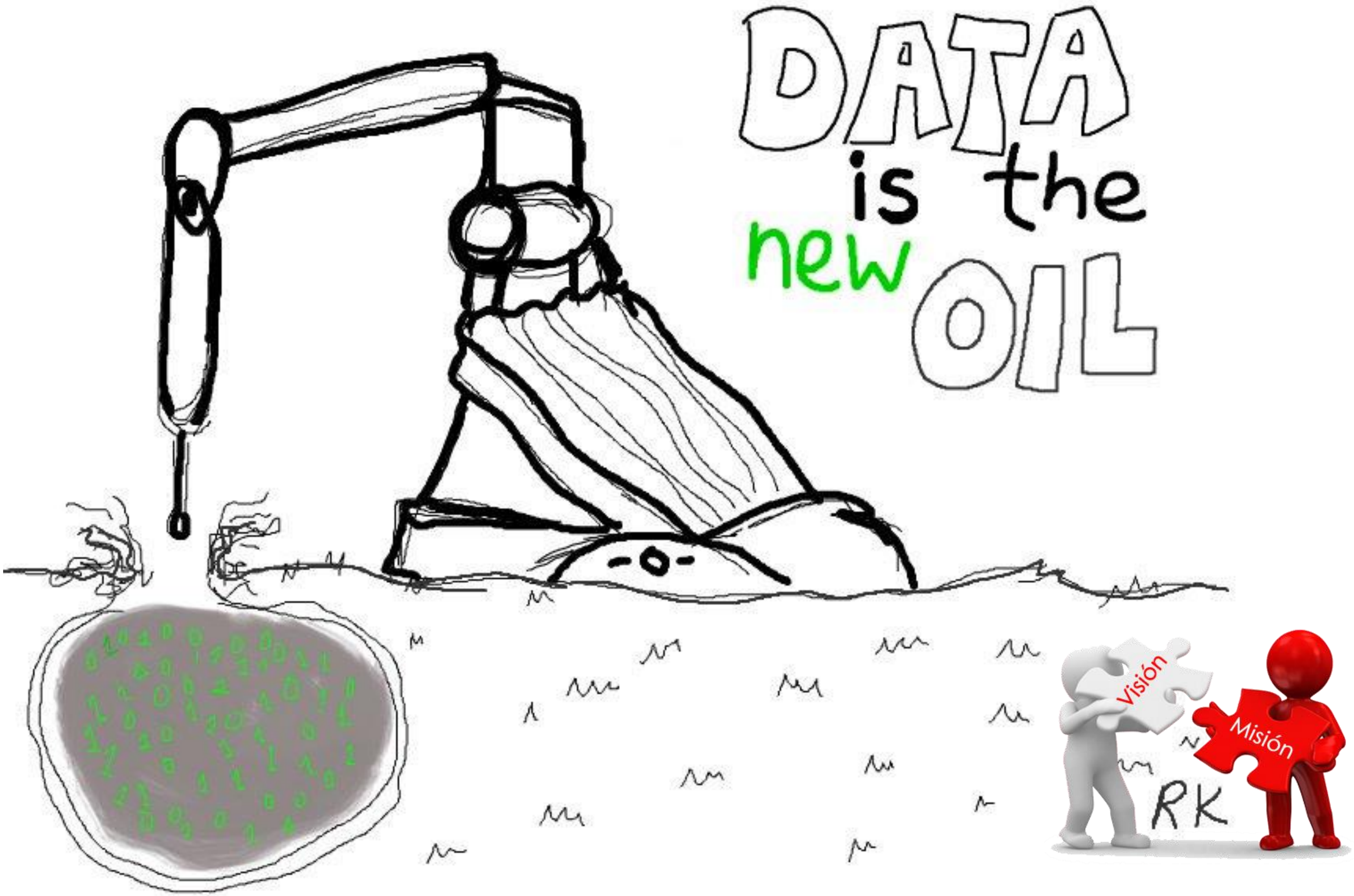
Ladies and gentlemen the Perceptron !



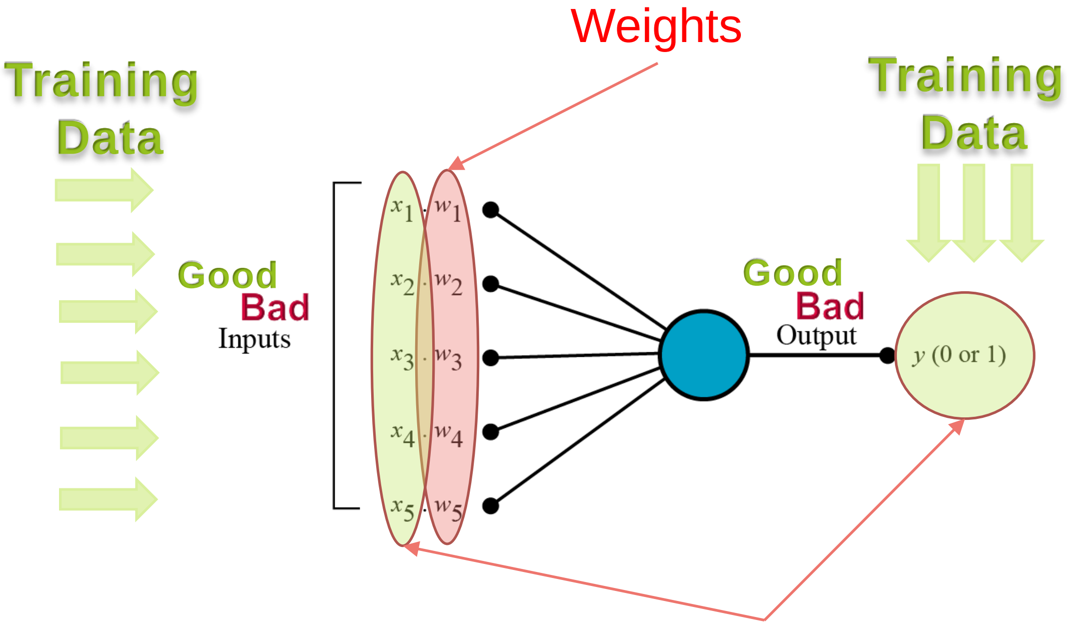
Ooops this can become quite complex…

attempting to cluster data and decide…




DATA is the new OIL
Visión
Misión
RK

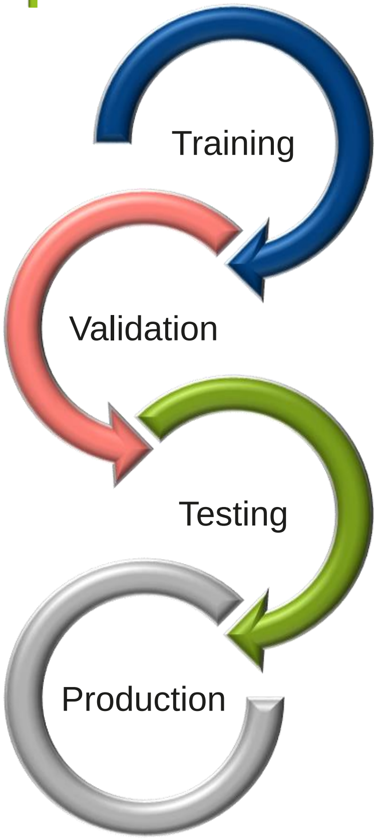
Supervised learning



Training data

Problem 1: Ensuring quality and quantity of training data is hard

Supervised/Unsupervised learning



Which data are considered correct/right/ethical?

Are human/moral values/freedom respected?

How much training data do we need?

Is supervised or unsupervised learning better?

How training data are produced?

How training is validated/certified?

What happens if the situation changes?

Problem 2: Ethics and trustworthiness

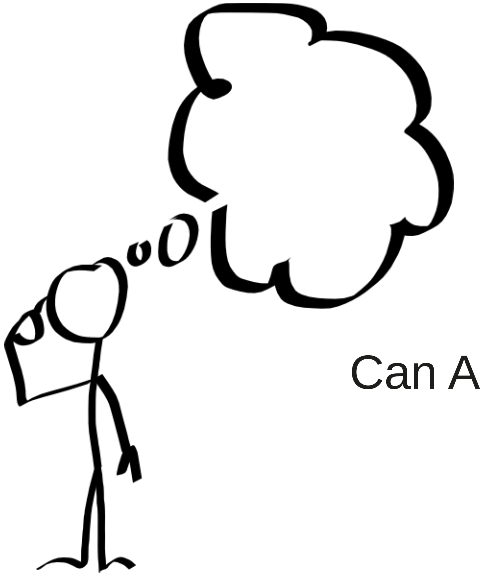
Where it applies?

AI applies to complex situations where we want to **classify** information that cannot be easily (linearly) classified

The explosion of **big data** made processing with traditional methods not practical

AI can be used to identify **complex patterns**

In cyber security AI can be used across all levels of **governance** (Political/Operational/Technical)



Can AI add value to the EU cyber crisis management?

AI & the Blueprint

EUROPEAN COMMISSION

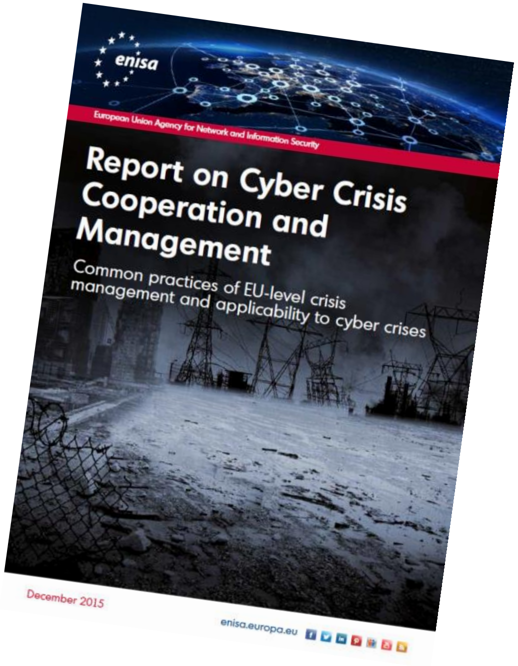
Brussels, 13.9.2017
C(2017) 6100 final

COMMISSION RECOMMENDATION

of 13.9.2017

on Coordinated Response to Large Scale Cybersecurity Incidents and Crises

EN EN



enisa

European Union Agency for Network and Information Security

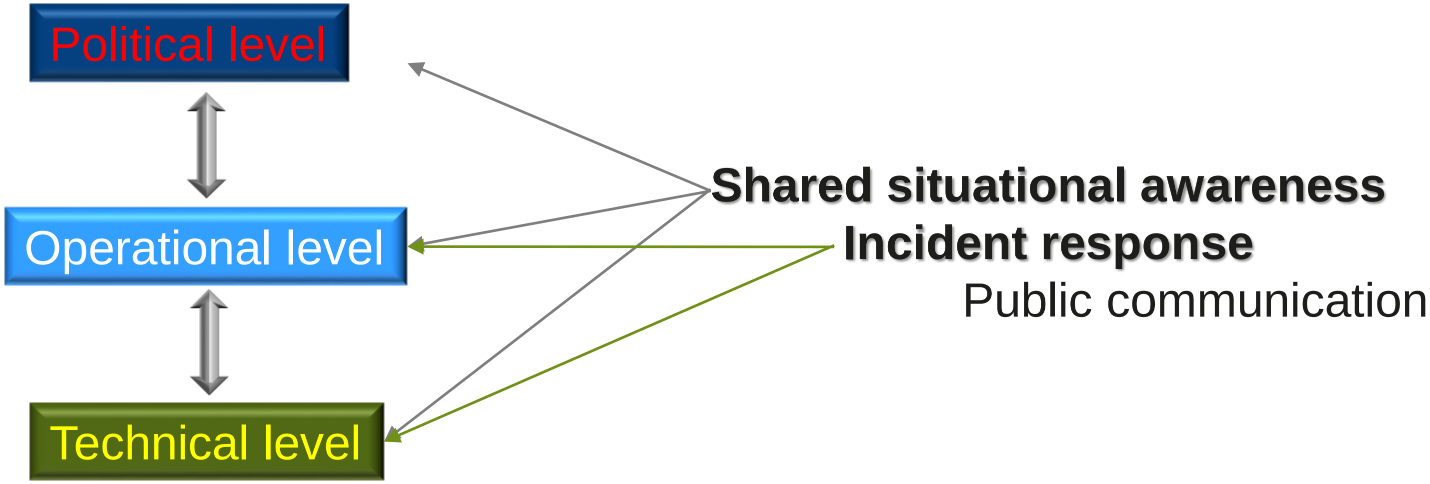
Report on Cyber Crisis Cooperation and Management

Common practices of EU-level crisis management and applicability to cyber crises

December 2015

enisa.europa.eu

Shared situational awareness
Incident response
Public communication



Political level

Operational level

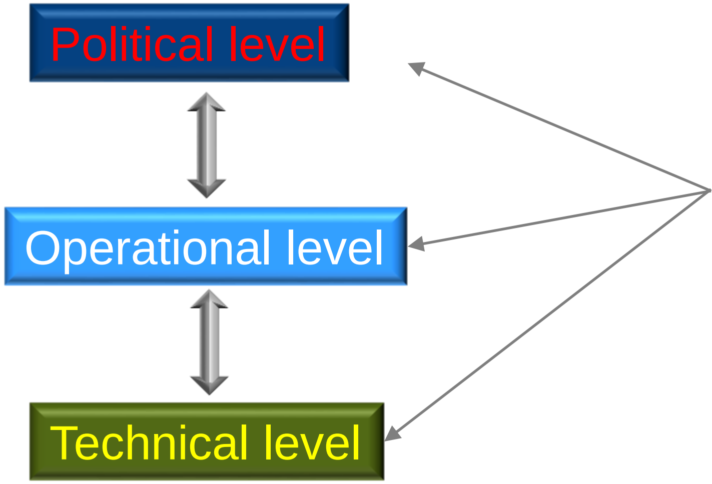
Technical level

Shared situational awareness

Incident response

Public communication

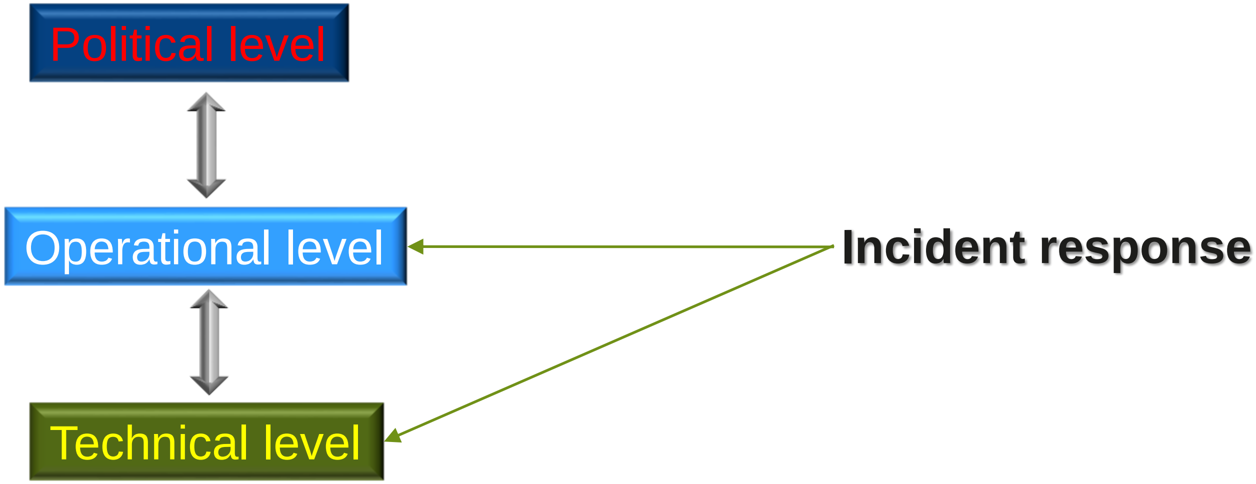
AI & the Blueprint



Shared situational awareness

News aggregation
NLP
Multi lingual analysis
Sentiment analysis
Fake news
Deep fake

AI & the Blueprint



Political level

Operational level

Technical level

Incident response

Threat pattern identification
Information fusion
Autonomous cyber response

European Commission

EU STRATEGY ON ARTIFICIAL INTELLIGENCE

published in April 2018

enisa

Open CSAM
situation awareness for cybersecurity executives
AUTOMATIC INGESTION
Cyber attack!
NEWS
PDF
NLP
TAXONOMY
ML
CYBERSECURITY SITUATION BRIEFING

WHAT

The Open Cybersecurity Situation Awareness Machine is an open source prototype developed by ENISA and Teradata that leverages Artificial Intelligence to extract cybersecurity intelligence from multiple sources of information. Open CSAM supports security analysts in informing decision makers on the current global cybersecurity situation.

HOW

Think Big Analytics combines world class deep learning expertise and unique industry understanding to bring to life AI solutions. We use NiFi combined with Kylo for accelerating the ingestion process. raw data is enriched by meta data, filtered by a rules-based engine and ultimately classified and summarized by using multi-class labeling and unsupervised NLP techniques.

ARTIFICIAL INTELLIGENCE

An opportunity for the EU cyber crisis blueprint

3-4 June | Athens, Greece

enisa THE EU CYBERSECURITY AGENCY

Shared situational awareness
Incident response
Public communication

EU STRATEGY ON ARTIFICIAL INTELLIGENCE

published in April 2018

Respect for human autonomy

Prevention of harm

Fairness

Explicability

High-Level Expert Group on Artificial Intelligence (AI HLEG) in June 2018

- Ethics Guidelines for Artificial Intelligence
- Policy & Investment Recommendations

Key impacts & enablers

Ensuring competitiveness and trustworthiness

AI & the Blueprint

Blueprint’s pillars for SA and IR

Threat analysts ↔

CSIRTs ↔

Cyber Security Professionals ↔

↙↗

Use services
Contribute to QoS

European Council

enisa EUINTCEN CSIRTs NETWORK EC3 EUROPOL CERT-EU EUROPEAN DEFENCE AGENCY

Open CSAM
situation awareness for cybersecurity executives
AUTOMATIC INGESTION
NEWS
PDF
NLP
TAXONOMY
CYBERSECURITY SITUATION BRIEFING
WHAT
HOW

Open Cyber Security Awareness Machine

Training data for AI →

Academia

Essential Services providers

Researchers

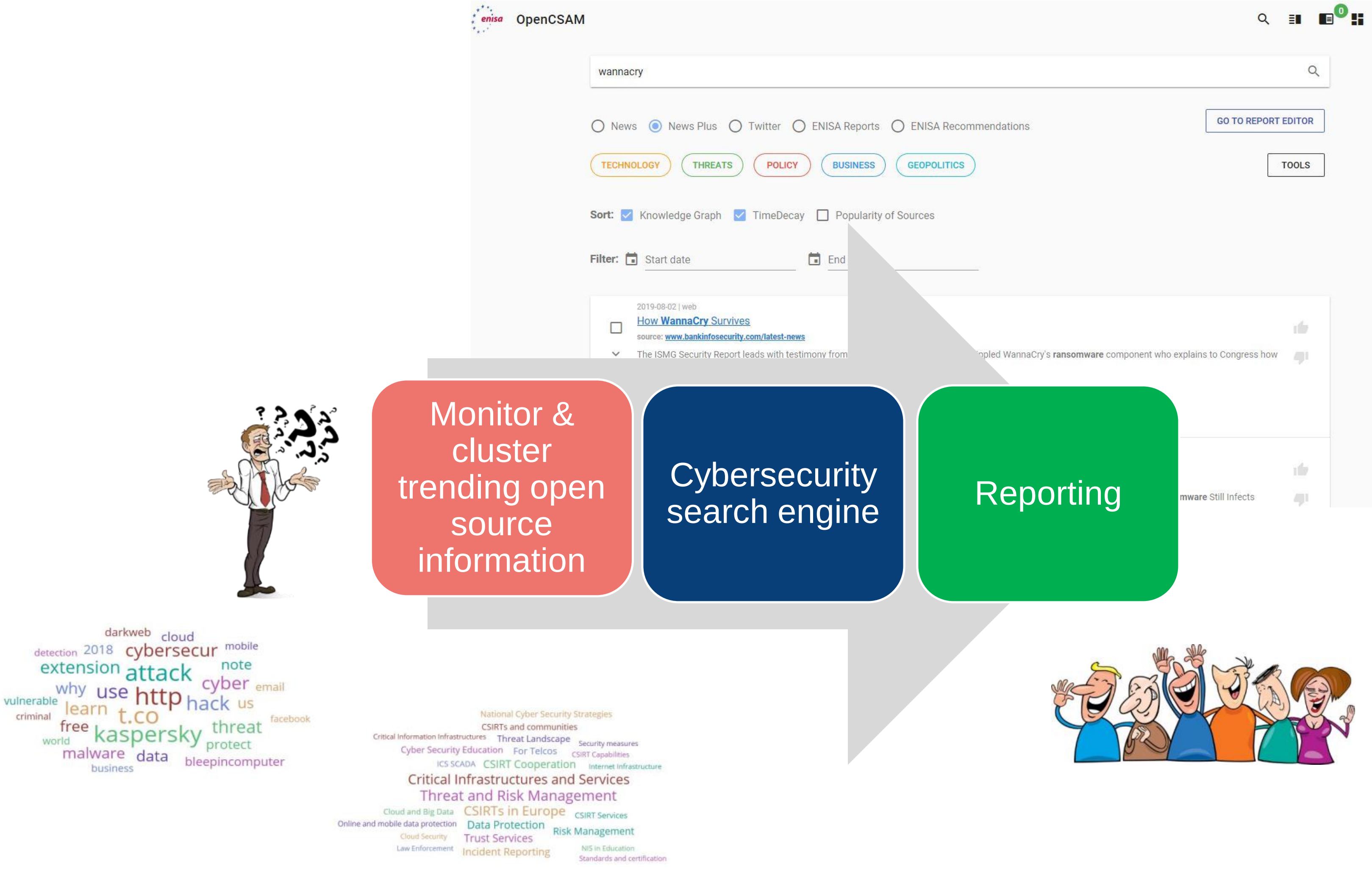
Cyber Security professionals

.

.

.

.



OpenCSAM

wannacry

○ News ● News Plus ○ Twitter ○ ENISA Reports ○ ENISA Recommendations

GO TO REPORT EDITOR

TECHNOLOGY · THREATS · POLICY · BUSINESS · GEOPOLITICS

TOOLS

Sort: ☑ Knowledge Graph ☑ TimeDecay □ Popularity of Sources

Filter: Start date End

□ 2019-08-02 | web
How **WannaCry** Survives
source: www.bankinfosecurity.com/latest-news
The ISMG Security Report leads with testimony from ...pled WannaCry's **ransomware** component who explains to Congress how

...**mware** Still Infects

Monitor & cluster trending open source information

Cybersecurity search engine

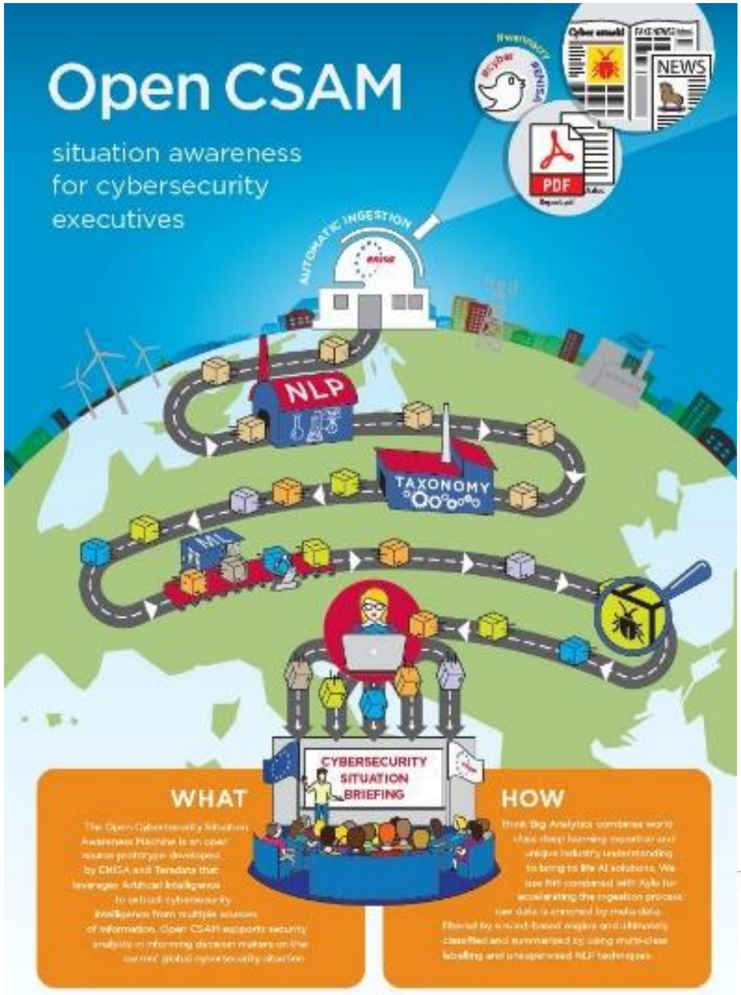
Reporting

How we are using AI

Knowledge Representation

Knowledge Graph

- Tree based flexible taxonomy
- Automatic suggestion of new terms from crawlers
- Use of KG in searching and classification



Open CSAM

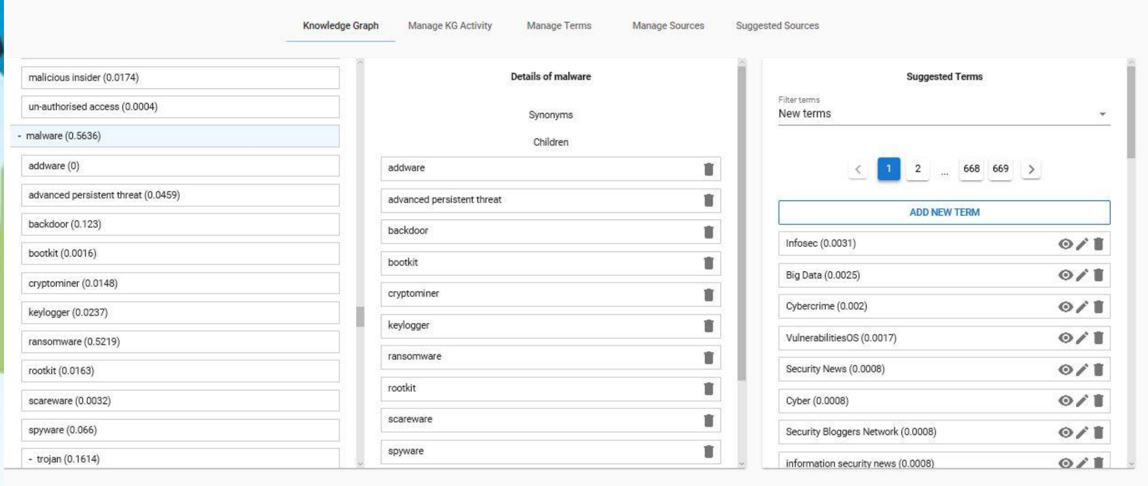
situation awareness
for cybersecurity
executives

WHAT

The Open Cybersecurity Situation Awareness Machine is an open source prototype developed by ENISA and Teradata that leverages Artificial Intelligence to extract cybersecurity intelligence from multiple sources of information. Open CSAM supports security analysts in informing decision makers on the current global cybersecurity situation

HOW

Think Big Analytics combines world class deep learning expertise and unique industry understanding to bring to life AI solutions. We use NiFi combined with Kylo for accelerating the ingestion process: raw data is enriched by meta data, filtered by a rule-based engine and ultimately classified and summarized by using multi-class labelling and unsupervised NLP techniques.



malicious insider (0.0174)
un-authorised access (0.0004)
- malware (0.5636)
addware (0)
advanced persistent threat (0.0459)
backdoor (0.123)
bootkit (0.0016)
cryptominer (0.0148)
keylogger (0.0237)
ransomware (0.5219)
rootkit (0.0163)
scareware (0.0032)
spyware (0.066)
- trojan (0.1614)

Details of malware

Synonyms

Children

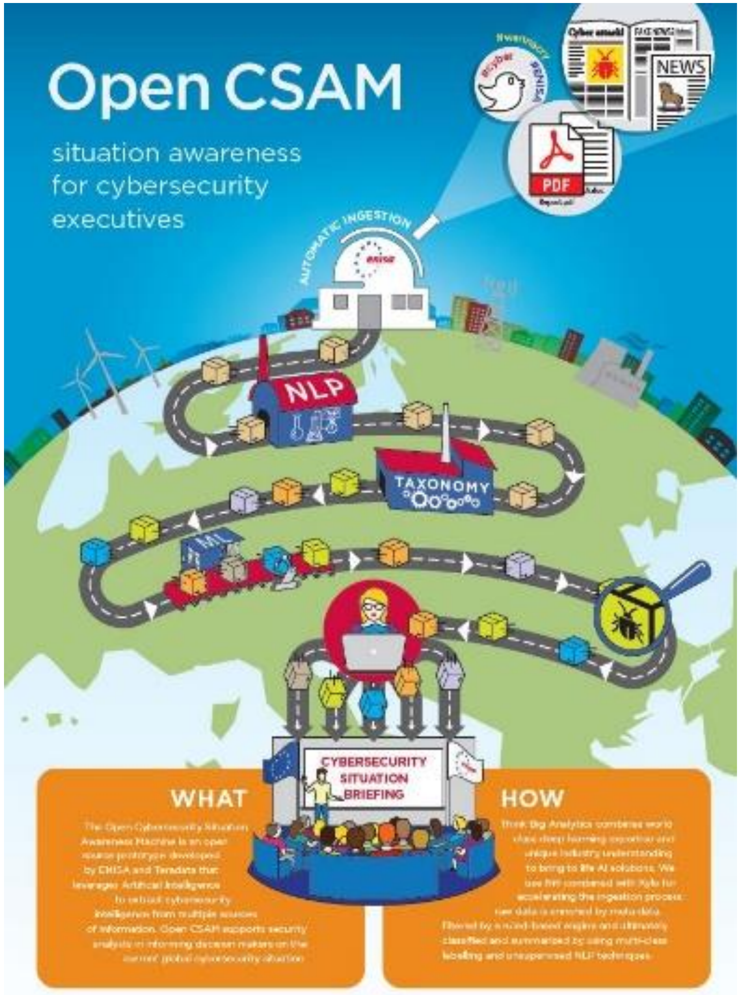
addware
advanced persistent threat
backdoor
bootkit
cryptominer
keylogger
ransomware
rootkit
scareware
spyware

Suggested Terms

Filter terms: New terms

Infosec (0.0031)
Big Data (0.0025)
Cybercrime (0.002)
VulnerabilitiesOS (0.0017)
Security News (0.0008)
Cyber (0.0008)
Security Bloggers Network (0.0008)
information security news (0.0008)

How we are using AI



WHAT

The Open Cybersecurity Situation Awareness Machine is an open source prototype developed by ENISA and Teradata that leverages Artificial Intelligence to extract cybersecurity intelligence from multiple sources of information. Open CSAM supports security analysts in informing decision makers on the current global cybersecurity situation.

HOW

Think Big Analytics combines world class deep learning expertise and unique industry understanding to bring to life AI solutions. We use NiFi combined with Kylo for accelerating the ingestion process: raw data is enriched by meta data, filtered by a rule-based engine and ultimately classified and summarized by using multi-class labelling and unsupervised NLP techniques.

NLP

Dynamic crawling

- Understand the language of the text
- Understand where in the text is the relevant document
- Identification of different types of relevant content (Entity recognition)

Summarization

- Text de noising
- Word clustering
- Calculation of importance

Classification

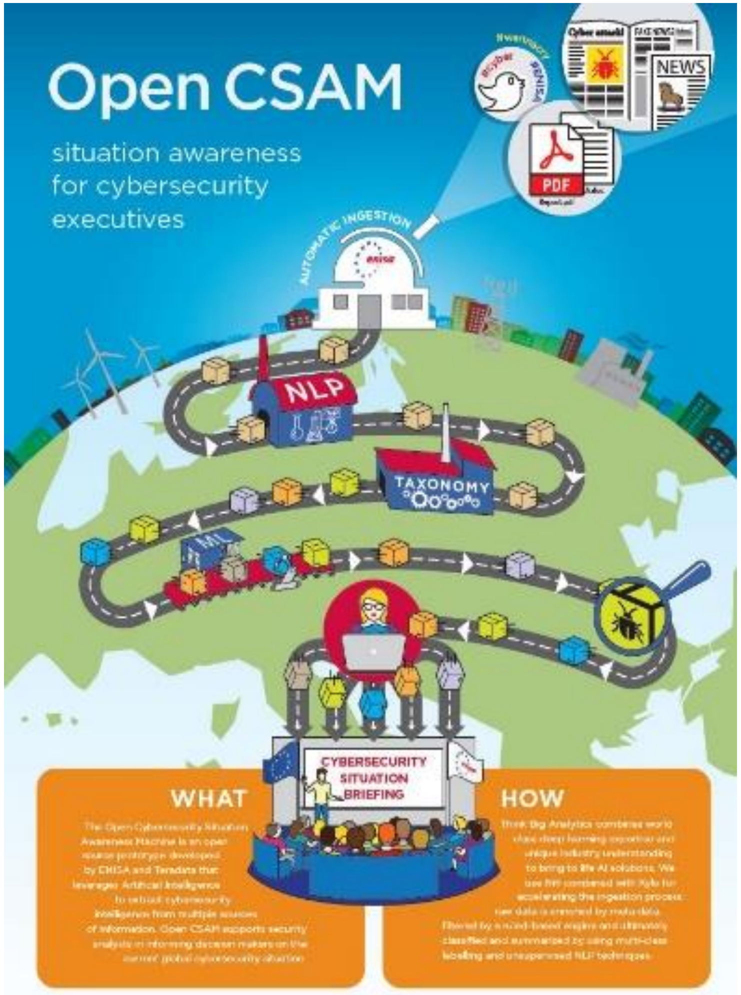
- Generation of training matrices for ML

Suggestion of new sources

- Comparison of random articles of a new source with articles in the sources repository via text tokenization and calculation of its relevance and importance

How we are using AI

Machine Learning



Open CSAM

situation awareness
for cybersecurity
executives

WHAT

The Open Cybersecurity Situation Awareness Machine is an open source prototype developed by ENISA and Teradata that leverages Artificial Intelligence to extract cybersecurity intelligence from multiple sources of information. Open CSAM supports security analysts in informing decision makers on the current global cybersecurity situation.

HOW

Think Big Analytics combines world class deep learning expertise and unique industry understanding to bring to life AI solutions. We use NiFi combined with Kylo for accelerating the ingestion process: raw data is enriched by meta-data, filtered by a rule-based engine and ultimately classified and summarized by using multi-class labelling and unsupervised NLP techniques.

Dynamic crawling

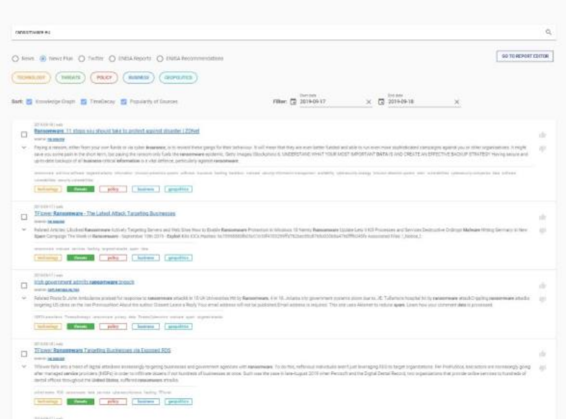
- Content deduplication

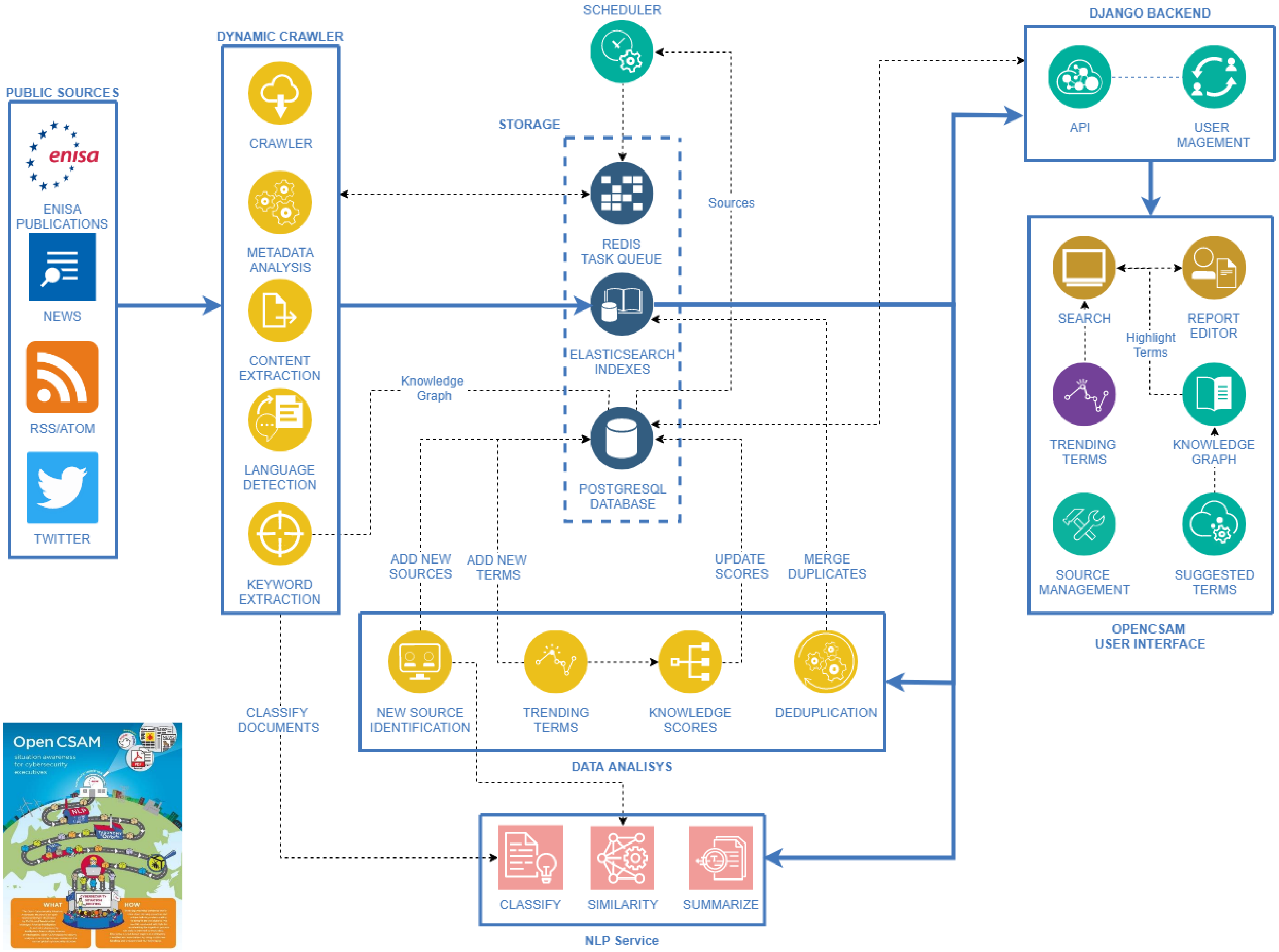
Classification of content

- 4 categories (Technology, Threats, Policy, Business, Geopolitics) via CNN

Summarization

- Vectorization of sentences for better clustering via cosine similarities



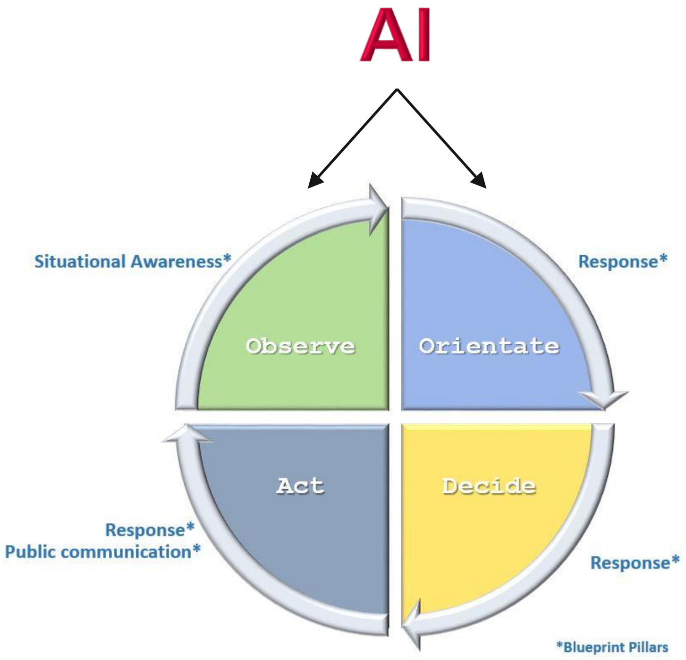

PUBLIC SOURCES
enisa
ENISA PUBLICATIONS
NEWS
RSS/ATOM
TWITTER
DYNAMIC CRAWLER
CRAWLER
METADATA ANALYSIS
CONTENT EXTRACTION
LANGUAGE DETECTION
KEYWORD EXTRACTION
SCHEDULER
STORAGE
REDIS TASK QUEUE
ELASTICSEARCH INDEXES
POSTGRESQL DATABASE
Sources
Knowledge Graph
ADD NEW SOURCES
ADD NEW TERMS
UPDATE SCORES
MERGE DUPLICATES
CLASSIFY DOCUMENTS
NEW SOURCE IDENTIFICATION
TRENDING TERMS
KNOWLEDGE SCORES
DEDUPLICATION
DATA ANALISYS
CLASSIFY
SIMILARITY
SUMMARIZE
NLP Service
DJANGO BACKEND
API
USER MAGEMENT
SEARCH
REPORT EDITOR
Highlight Terms
TRENDING TERMS
KNOWLEDGE GRAPH
SOURCE MANAGEMENT
SUGGESTED TERMS
OPENCSAM USER INTERFACE
Open CSAM
situation awareness for cybersecurity executives
NLP
TAXONOMY
WHAT
HOW

ARTIFICIAL INTELLIGENCE
An opportunity for the EU cyber crisis blueprint
3-4 June | Athens, Greece
enisa
THE EU CYBERSECURITY AGENCY

- The future of the Blueprint
- How can Artificial Intelligence help the blueprint
- Improving OpenCSAM
- Cyber autonomous response, threat detection and security automation

EU Internal report with recommendations approved recently

A vision for the **Blue**print



THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

☎ +30 28 14 40 9711

✉ info@enisa.europa.eu

🌐 www.enisa.europa.eu