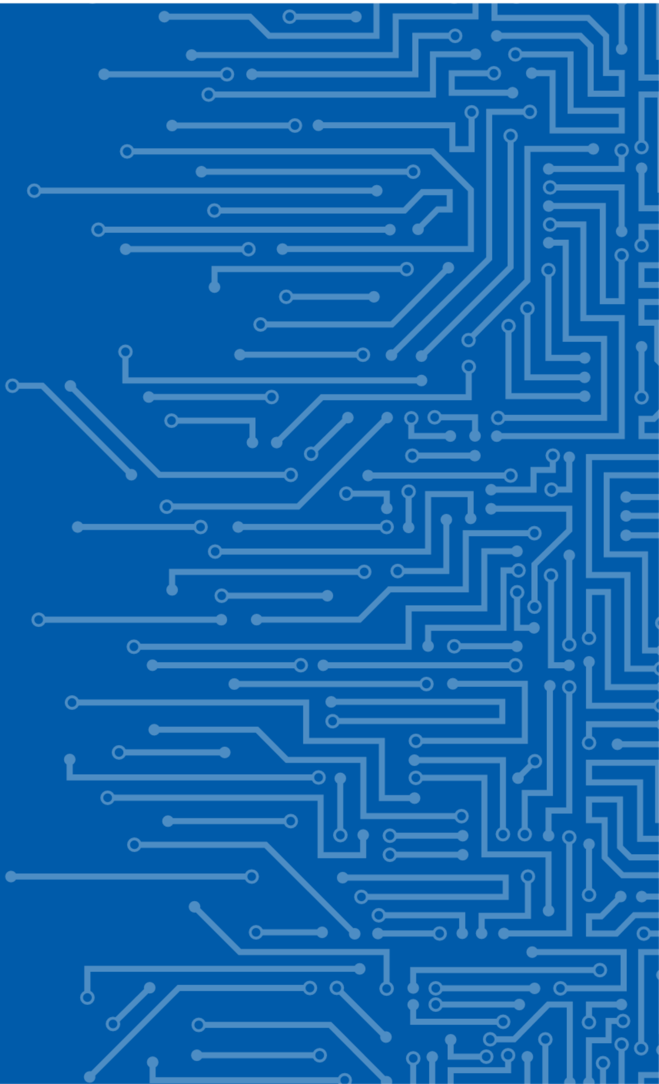
THE EU CYBERSECURITY AGENCY

OPEN-CSAM
INFORMATION AGGREGATOR AND REPORTING TOOL USING AI AND NATURAL LANGUAGE PROCESSING



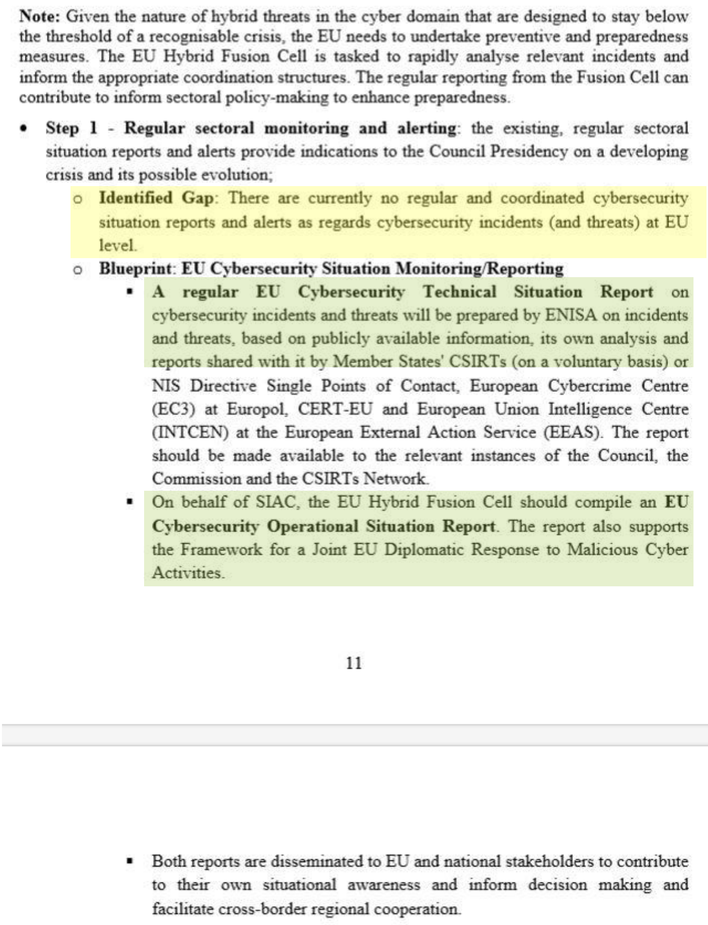
Georgios Chatzichristos
Operational Security Unit - ENISA

6 | 11 | 2018

THE GOAL

Help Decision Makers take better decisions !

THE TRIGGER



Note: Given the nature of hybrid threats in the cyber domain that are designed to stay below the threshold of a recognisable crisis, the EU needs to undertake preventive and preparedness measures. The EU Hybrid Fusion Cell is tasked to rapidly analyse relevant incidents and inform the appropriate coordination structures. The regular reporting from the Fusion Cell can contribute to inform sectoral policy-making to enhance preparedness.

- **Step 1 - Regular sectoral monitoring and alerting**: the existing, regular sectoral situation reports and alerts provide indications to the Council Presidency on a developing crisis and its possible evolution;
  - **Identified Gap**: There are currently no regular and coordinated cybersecurity situation reports and alerts as regards cybersecurity incidents (and threats) at EU level.
  - **Blueprint**: **EU Cybersecurity Situation Monitoring/Reporting**
    - **A regular EU Cybersecurity Technical Situation Report** on cybersecurity incidents and threats will be prepared by ENISA on incidents and threats, based on publicly available information, its own analysis and reports shared with it by Member States' CSIRTs (on a voluntary basis) or NIS Directive Single Points of Contact, European Cybercrime Centre (EC3) at Europol, CERT-EU and European Union Intelligence Centre (INTCEN) at the European External Action Service (EEAS). The report should be made available to the relevant instances of the Council, the Commission and the CSIRTs Network.
    - On behalf of SIAC, the EU Hybrid Fusion Cell should compile an **EU Cybersecurity Operational Situation Report**. The report also supports the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities.

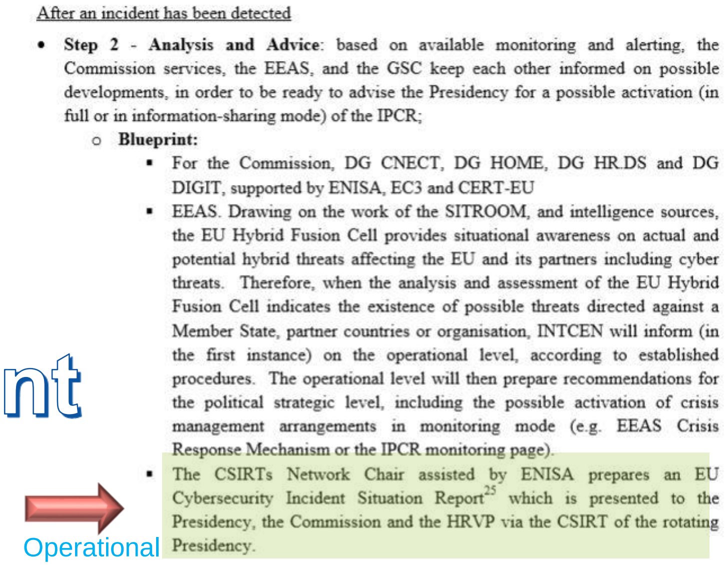
11

- Both reports are disseminated to EU and national stakeholders to contribute to their own situational awareness and inform decision making and facilitate cross-border regional cooperation.

Technical

Operational

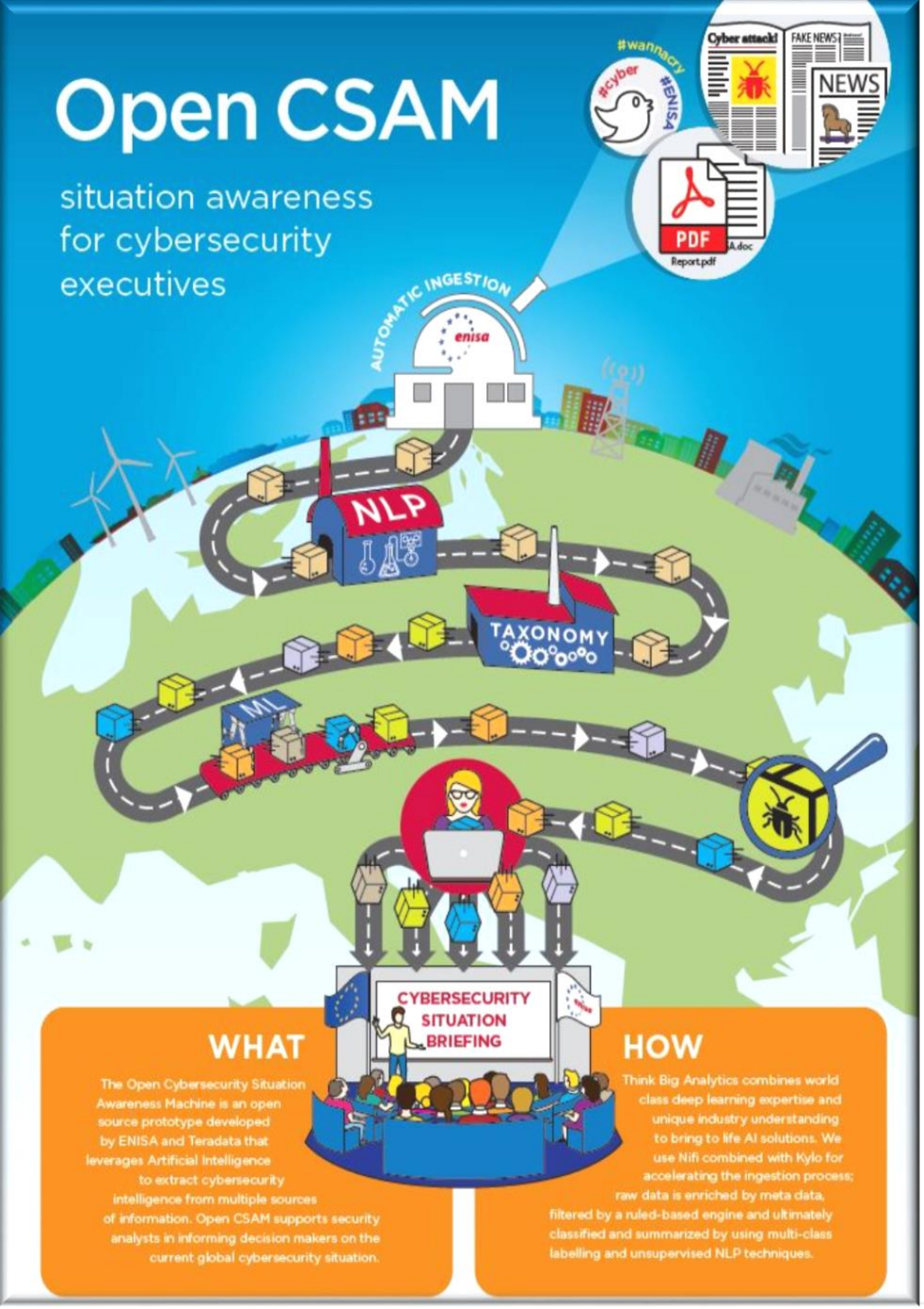
BluePrint



After an incident has been detected

- **Step 2 - Analysis and Advice**: based on available monitoring and alerting, the Commission services, the EEAS, and the GSC keep each other informed on possible developments, in order to be ready to advise the Presidency for a possible activation (in full or in information-sharing mode) of the IPCR;
  - **Blueprint:**
    - For the Commission, DG CNECT, DG HOME, DG HR.DS and DG DIGIT, supported by ENISA, EC3 and CERT-EU
    - EEAS. Drawing on the work of the SITROOM, and intelligence sources, the EU Hybrid Fusion Cell provides situational awareness on actual and potential hybrid threats affecting the EU and its partners including cyber threats. Therefore, when the analysis and assessment of the EU Hybrid Fusion Cell indicates the existence of possible threats directed against a Member State, partner countries or organisation, INTCEN will inform (in the first instance) on the operational level, according to established procedures. The operational level will then prepare recommendations for the political strategic level, including the possible activation of crisis management arrangements in monitoring mode (e.g. EEAS Crisis Response Mechanism or the IPCR monitoring page).
    - The CSIRTs Network Chair assisted by ENISA prepares an EU Cybersecurity Incident Situation Report[25] which is presented to the Presidency, the Commission and the HRVP via the CSIRT of the rotating Presidency.

Operational
Technical



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 ruled-based engine and ultimately classified and summarized by using multi-class labelling and unsupervised NLP techniques.

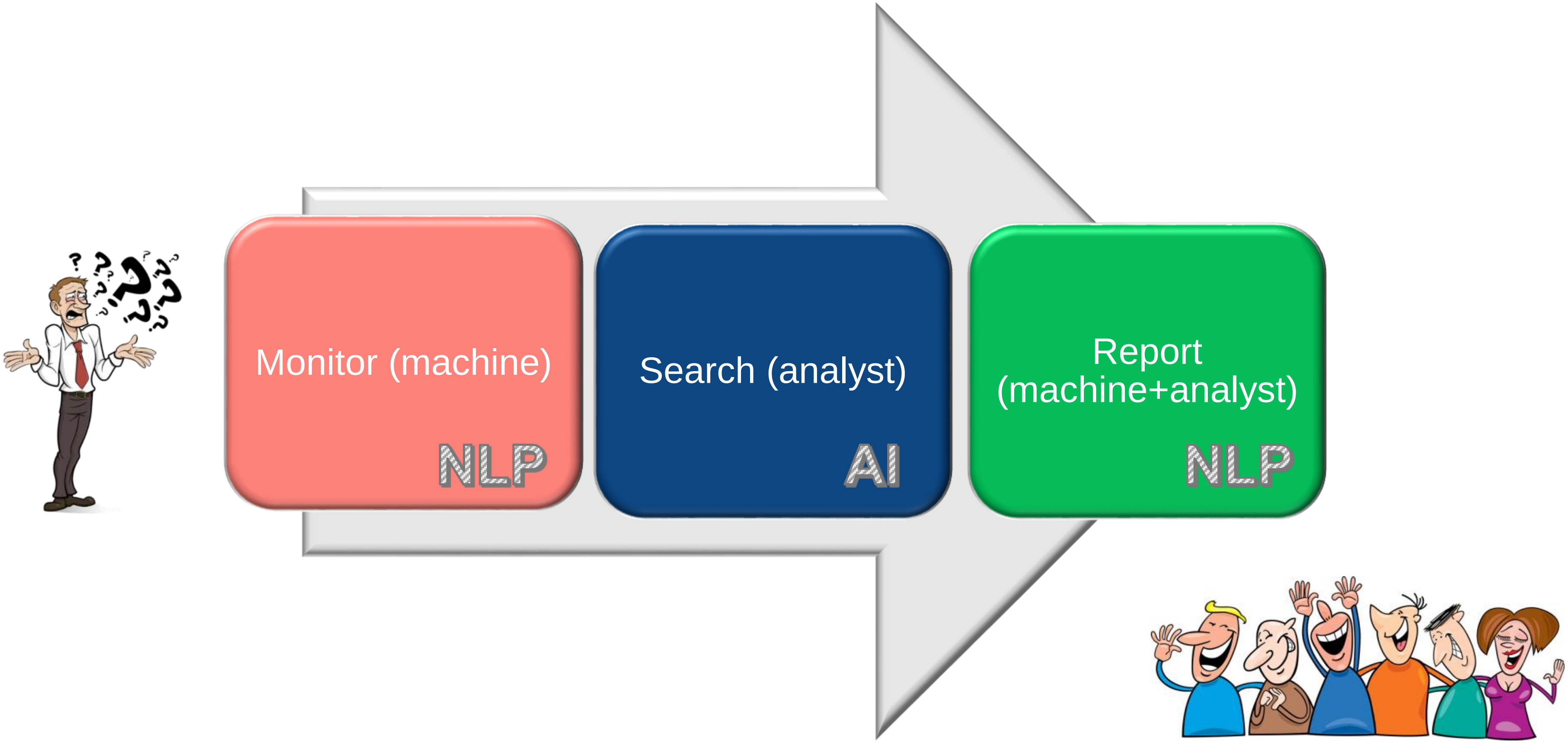
Develop a tool based on latest technologies that will enhance situational awareness and help threat analysts to advise decision makers

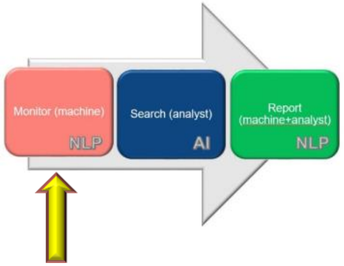
Strategic

Operational

Technical

The process


Monitor (machine)
NLP
Search (analyst)
AI
Report (machine+analyst)
NLP



What is Natural Language Processing?
Field of study focused on making sense of language

Using statistics and computers

Basics tasks of NLP:

Topic identification

Text classification

NLP applications include:

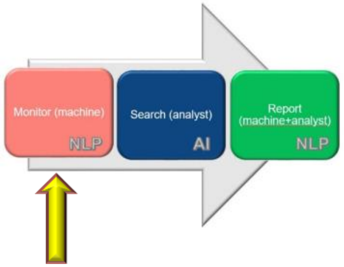
Chatbots

Translation, Fake News detection, text summarization

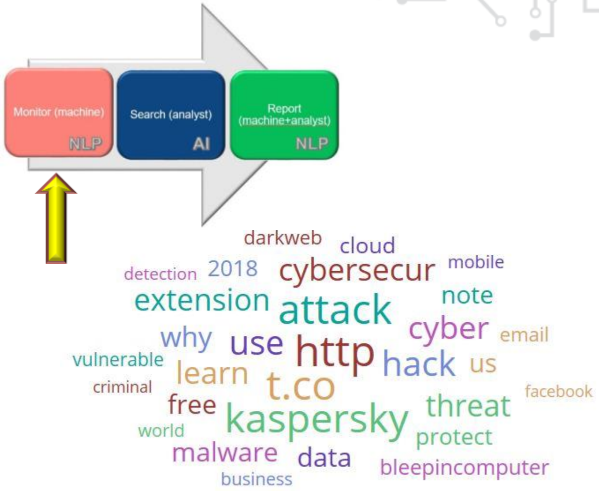
Sentiment analysis -> Social Media, Customer reviews etc.

SPAM

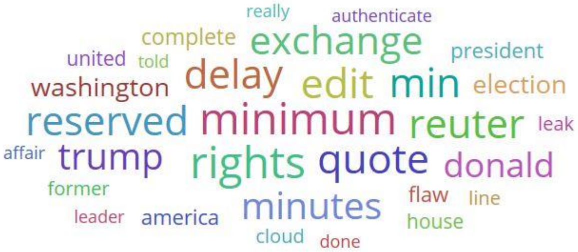
Information aggregation



- News aggregator, monitors 24/7 a set of news sources and tweets
- Uses NLP to isolate trending terms
- Creates clusters of relevant terms using AI
- Searches ENISA’s own publications
- Searches ENISA’s own recommendations



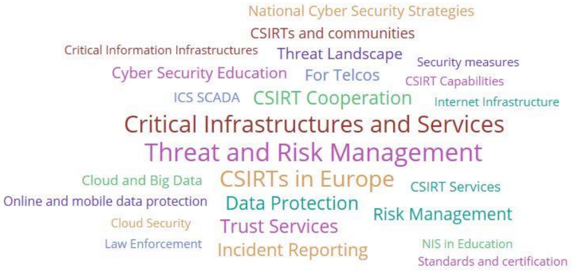
Trending terms in Tweets



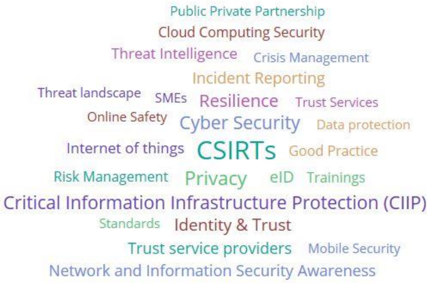
Trending terms in News

Continuous monitoring

Daily/Weekly/Monthly/Yearly Stats

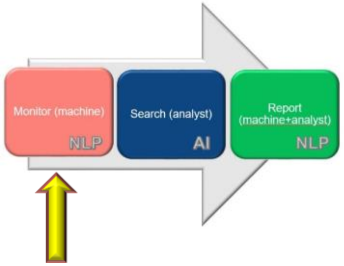


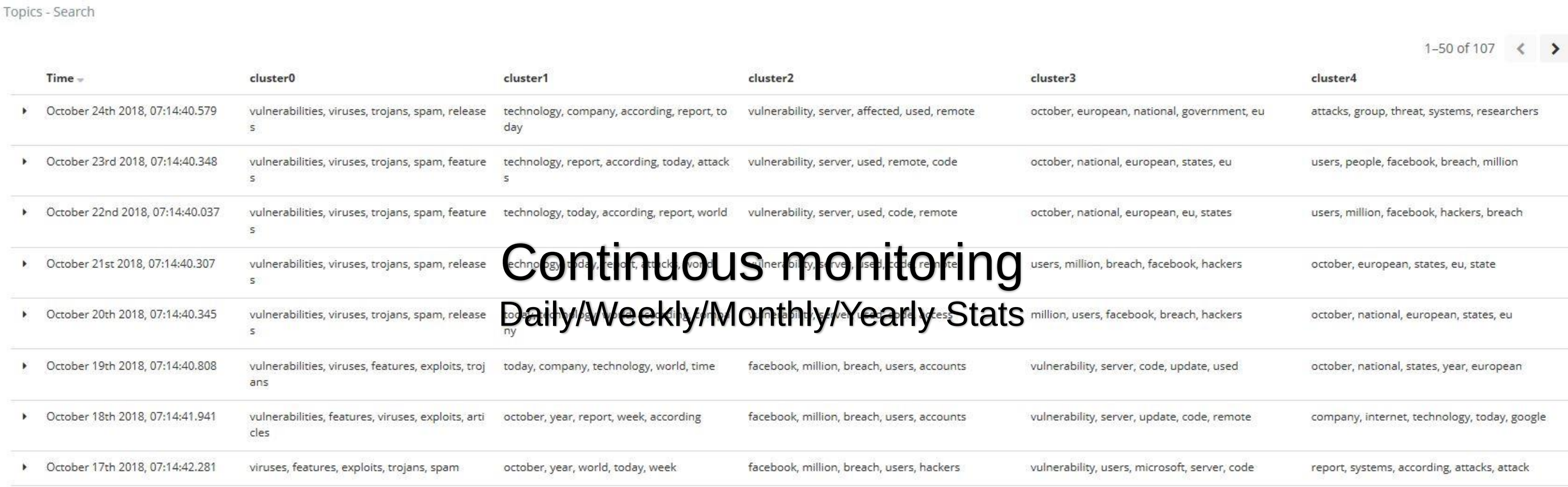
ENISA’s topics



ENISA’s terms

AI





Topics - Search

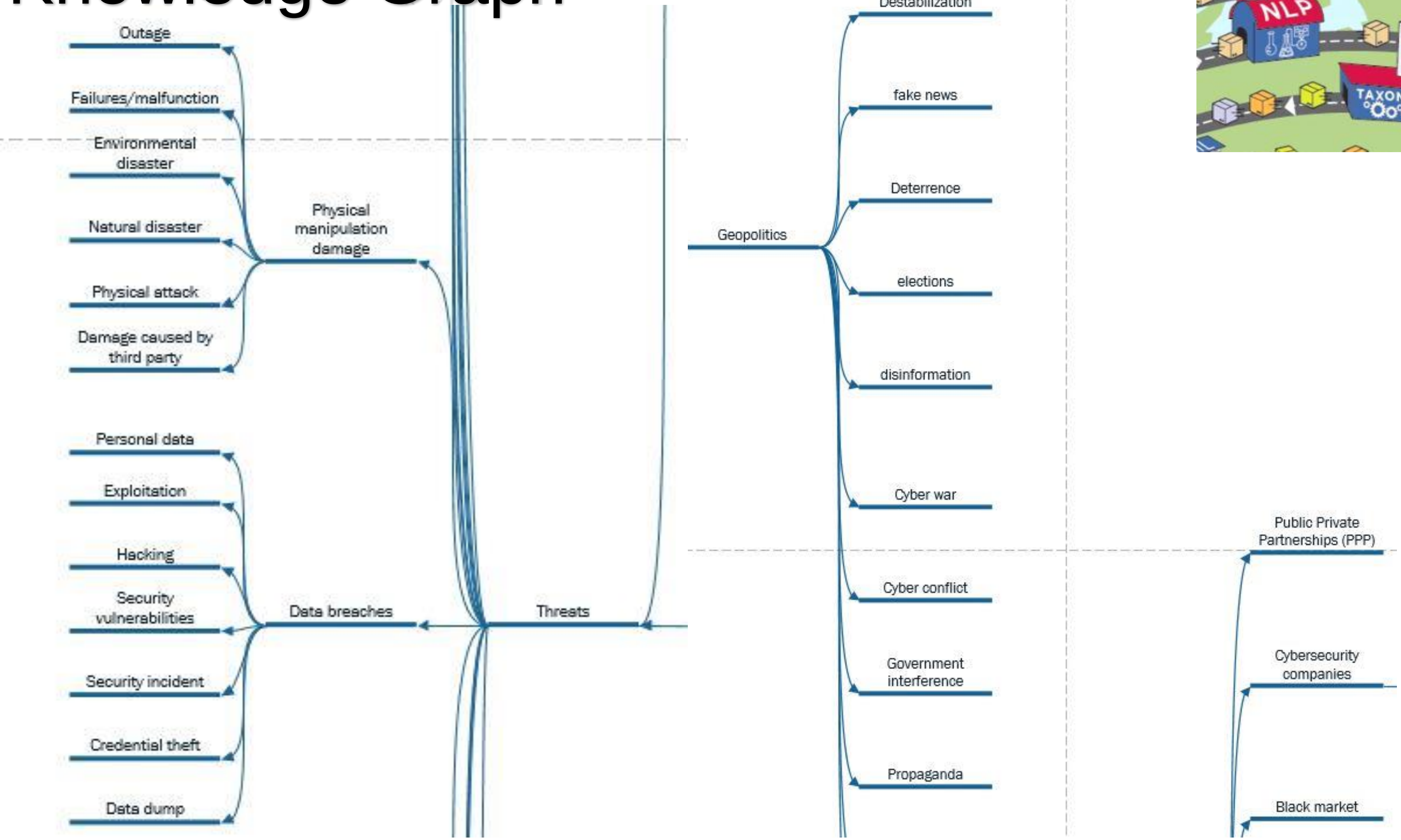
1–50 of 107

	Time	cluster0	cluster1	cluster2	cluster3	cluster4
▸	October 24th 2018, 07:14:40.579	vulnerabilities, viruses, trojans, spam, releases	technology, company, according, report, today	vulnerability, server, affected, used, remote	october, european, national, government, eu	attacks, group, threat, systems, researchers
▸	October 23rd 2018, 07:14:40.348	vulnerabilities, viruses, trojans, spam, features	technology, report, according, today, attacks	vulnerability, server, used, remote, code	october, national, european, states, eu	users, people, facebook, breach, million
▸	October 22nd 2018, 07:14:40.037	vulnerabilities, viruses, trojans, spam, features	technology, today, according, report, world	vulnerability, server, used, code, remote	october, national, european, eu, states	users, million, facebook, hackers, breach
▸	October 21st 2018, 07:14:40.307	vulnerabilities, viruses, trojans, spam, releases	technology, today, report, attacks, world	vulnerability, server, used, code, remote	users, million, breach, facebook, hackers	october, european, states, eu, state
▸	October 20th 2018, 07:14:40.345	vulnerabilities, viruses, trojans, spam, releases	today, technology, world, according, company	vulnerability, server, used, code, access	million, users, facebook, breach, hackers	october, national, european, states, eu
▸	October 19th 2018, 07:14:40.808	vulnerabilities, viruses, features, exploits, trojans	today, company, technology, world, time	facebook, million, breach, users, accounts	vulnerability, server, code, update, used	october, national, states, year, european
▸	October 18th 2018, 07:14:41.941	vulnerabilities, features, viruses, exploits, articles	october, year, report, week, according	facebook, million, breach, users, accounts	vulnerability, server, update, code, remote	company, internet, technology, today, google
▸	October 17th 2018, 07:14:42.281	viruses, features, exploits, trojans, spam	october, year, world, today, week	facebook, million, breach, users, hackers	vulnerability, users, microsoft, server, code	report, systems, according, attacks, attack

Continuous monitoring

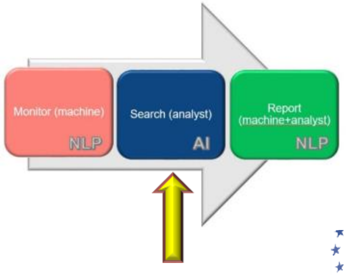
Daily/Weekly/Monthly/Yearly Stats

Knowledge Graph



Hardcoded

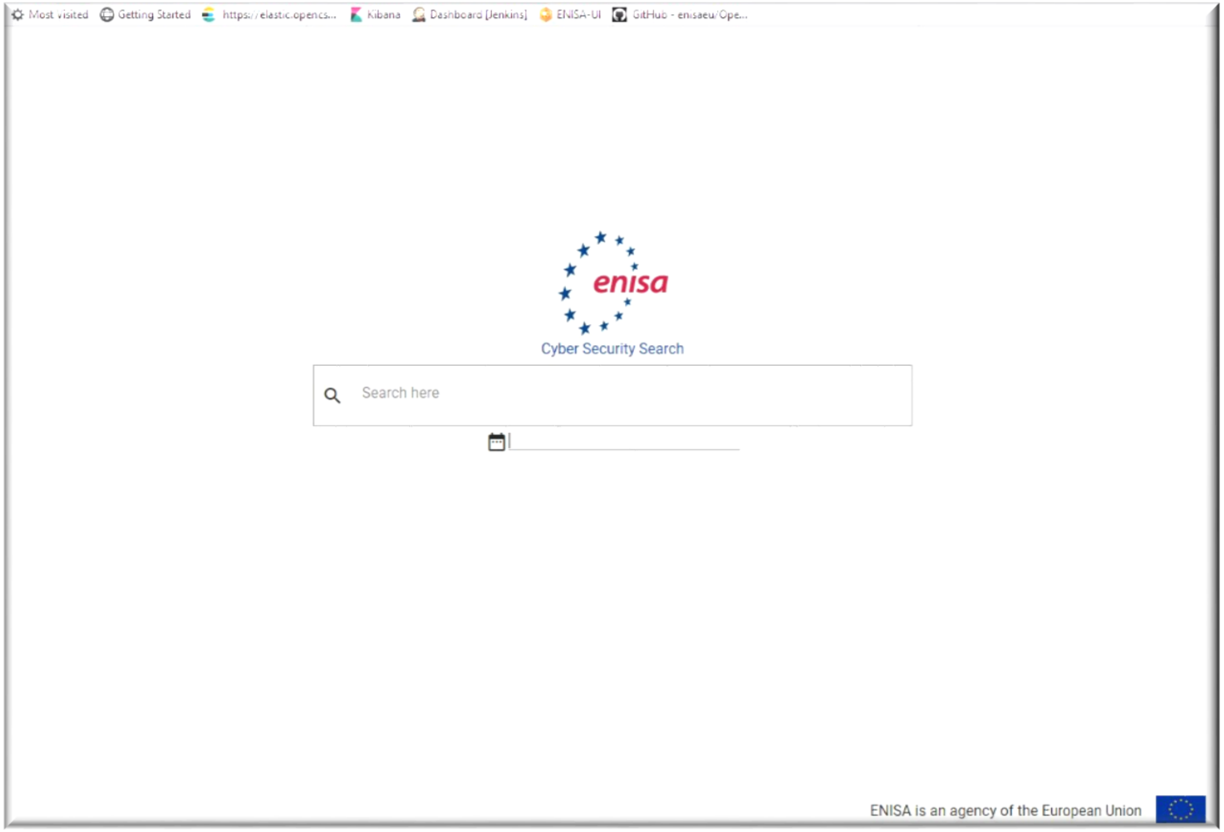
Used to drive AI



Searching

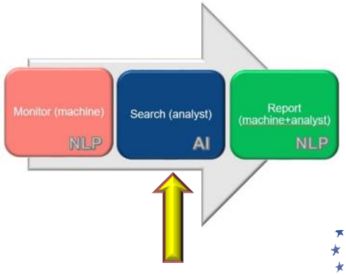
Web Articles and RSS

1. https://www.bleepingcomputer.com/
2. https://arstechnica.com/tag/security/
3. https://threatpost.com/
4. https://www.darkreading.com/attacks-breaches.asp
5. https://techcrunch.com/tag/cybersecurity/
6. https://www.csoonline.com/category/security/
7. https://www.csoonline.com/category/hacking/
8. https://www.csoonline.com/category/malware/
9. https://www.csoonline.com/category/loss-prevention/
10. https://www.csoonline.com/category/social-engineering/
11. https://www.csoonline.com/category/access-control/
12. https://www.securityweek.com/
13. https://securityaffairs.co/wordpress/
14. https://nakedsecurity.sophos.com/
15. https://securelist.com/
16. https://securityintelligence.com/
17. https://www.bankinfosecurity.com/
18. https://www.symantec.com/blogs/
19. https://www.fireeye.com/blog/threat-research.html
20. https://blogs.cisco.com/security
21. https://blog.malwarebytes.com/
22. http://www.itsecurityguru.org/
23. https://www.scmagazine.com/cybercrime/section/6950/
24. http://www.bbc.com/news/topics/cz4pr2gd85qt/cyber-security
25. https://www.independent.co.uk/topic/cyber-security
26. https://www.reuters.com/news/archive/cybersecurity
27. https://www.euractiv.com/sections/cybersecurity/
28. https://www.politico.com/cybersecurity
29. https://www.wired.com/category/security/
30. https://www.secureworks.com/research
31. https://www.tripwire.com/state-of-security/
32. https://blog.trendmicro.com/trendlabs-security-intelligence/
33. https://thehackernews.com/
34. https://news.hitb.org/tags/security?q=tags/security&page=1
35. https://www.infosecurity-magazine.com/news/
36. https://www.ncsc.gov.uk/index/news
37. https://www.welivesecurity.com/

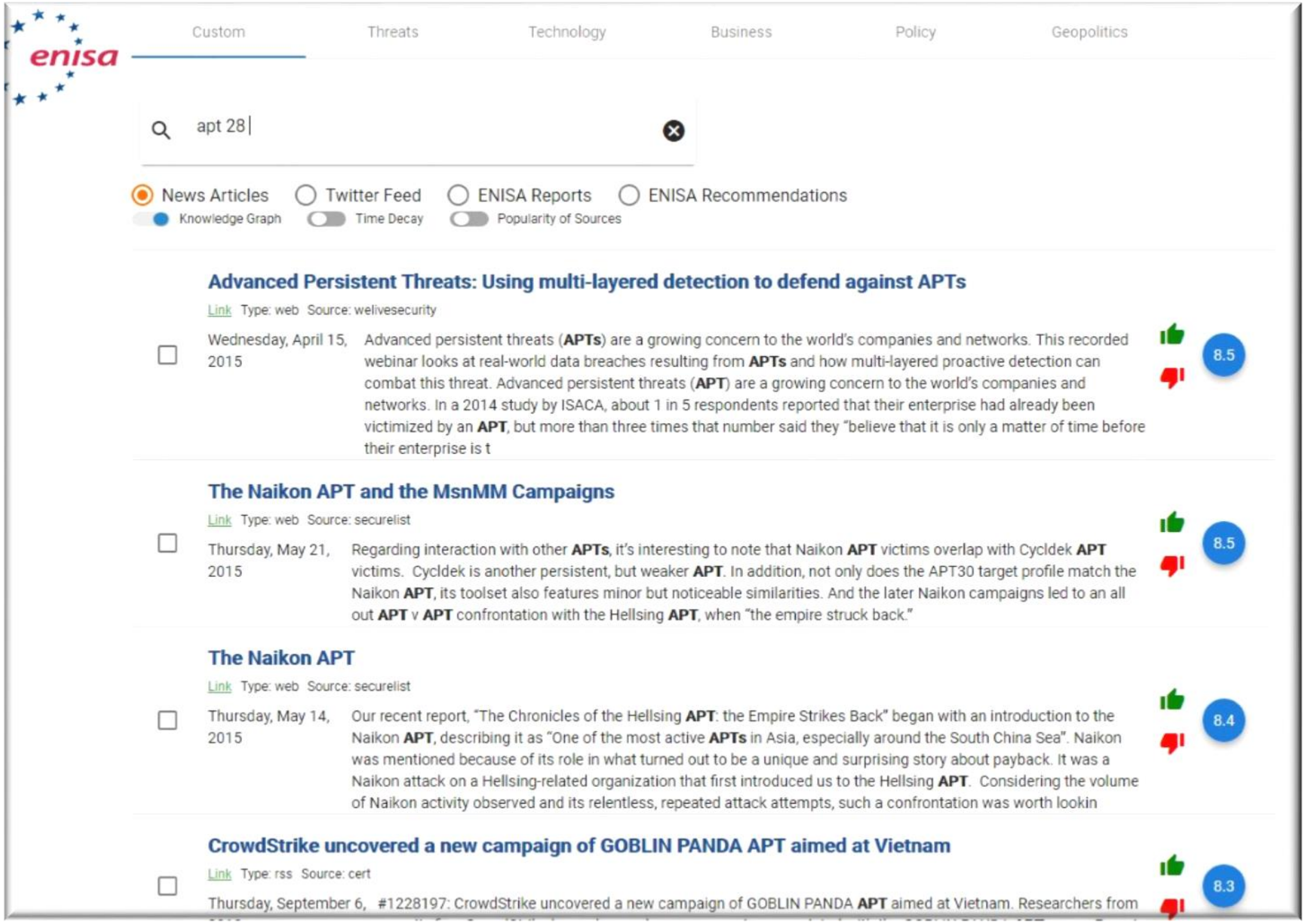


Twitter Profiles

1. DarkReading
2. kaspersky
3. paulsparrows
4. demonslay335
5. haveibeenpwned



Searching



apt 28|

● News Articles ○ Twitter Feed ○ ENISA Reports ○ ENISA Recommendations

Knowledge Graph: on · Time Decay: off · Popularity of Sources: off

□ **Advanced Persistent Threats: Using multi-layered detection to defend against APTs** — 8.5

Link Type: web Source: welivesecurity

Wednesday, April 15, 2015 — Advanced persistent threats (**APTs**) are a growing concern to the world's companies and networks. This recorded webinar looks at real-world data breaches resulting from **APTs** and how multi-layered proactive detection can combat this threat. Advanced persistent threats (**APT**) are a growing concern to the world's companies and networks. In a 2014 study by ISACA, about 1 in 5 respondents reported that their enterprise had already been victimized by an **APT**, but more than three times that number said they "believe that it is only a matter of time before their enterprise is t

□ **The Naikon APT and the MsnMM Campaigns** — 8.5

Link Type: web Source: securelist

Thursday, May 21, 2015 — Regarding interaction with other **APTs**, it's interesting to note that Naikon **APT** victims overlap with Cycldek **APT** victims. Cycldek is another persistent, but weaker **APT**. In addition, not only does the APT30 target profile match the Naikon **APT**, its toolset also features minor but noticeable similarities. And the later Naikon campaigns led to an all out **APT** v **APT** confrontation with the Hellsing **APT**, when "the empire struck back."

□ **The Naikon APT** — 8.4

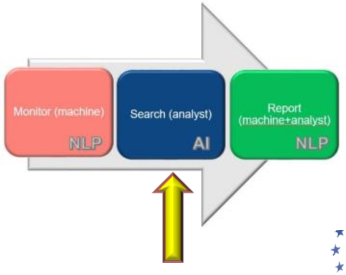
Link Type: web Source: securelist

Thursday, May 14, 2015 — Our recent report, "The Chronicles of the Hellsing **APT**: the Empire Strikes Back" began with an introduction to the Naikon **APT**, describing it as "One of the most active **APTs** in Asia, especially around the South China Sea". Naikon was mentioned because of its role in what turned out to be a unique and surprising story about payback. It was a Naikon attack on a Hellsing-related organization that first introduced us to the Hellsing **APT**. Considering the volume of Naikon activity observed and its relentless, repeated attack attempts, such a confrontation was worth lookin

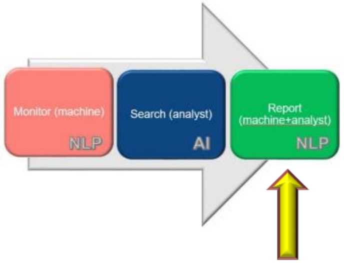
□ **CrowdStrike uncovered a new campaign of GOBLIN PANDA APT aimed at Vietnam** — 8.3

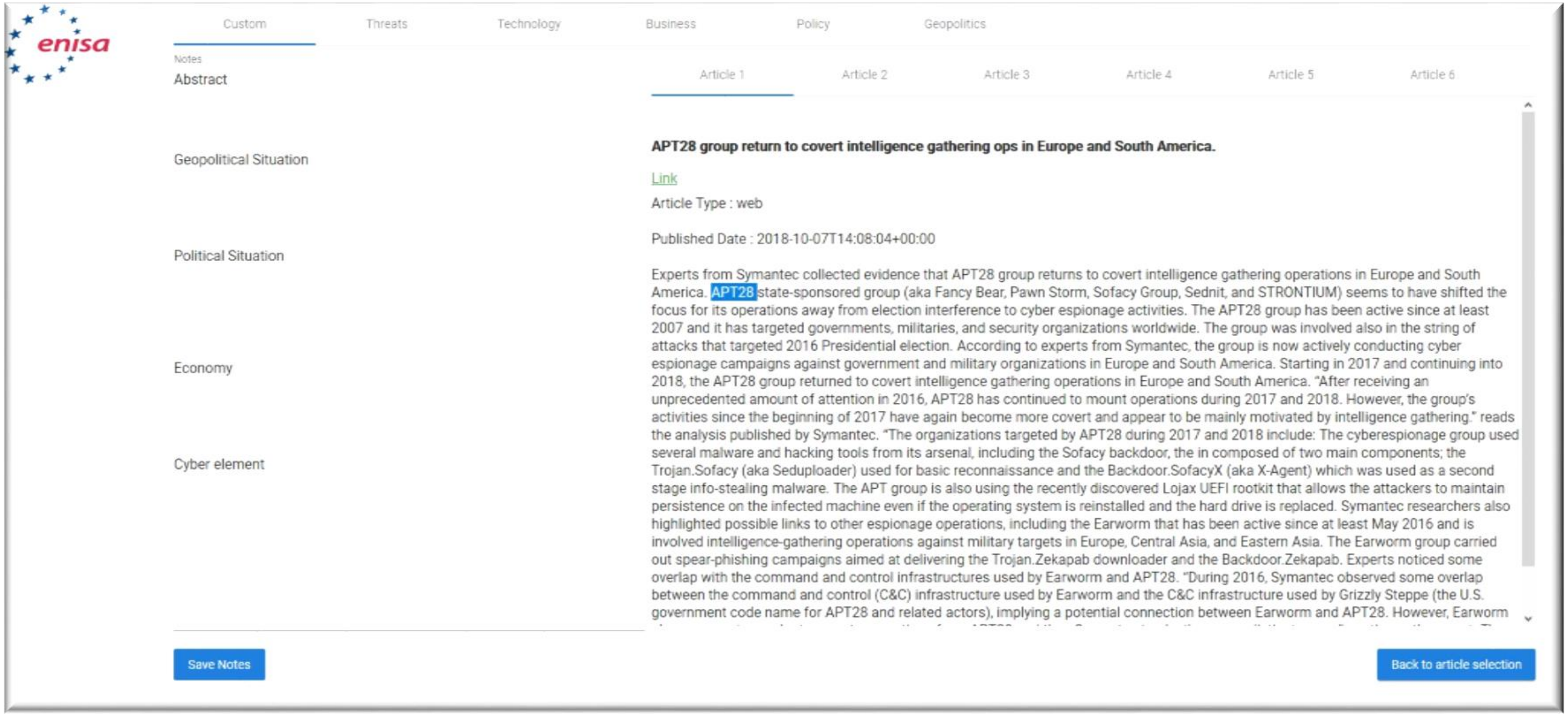
Link Type: rss Source: cert

Thursday, September 6, — #1228197: CrowdStrike uncovered a new campaign of GOBLIN PANDA **APT** aimed at Vietnam. Researchers from



Reporting





Notes

Abstract

Geopolitical Situation

Political Situation

Economy

Cyber element

APT28 group return to covert intelligence gathering ops in Europe and South America.

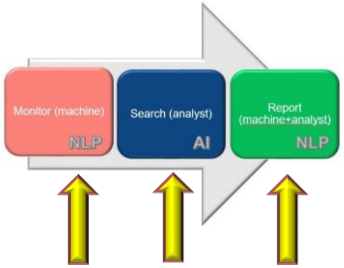
Link

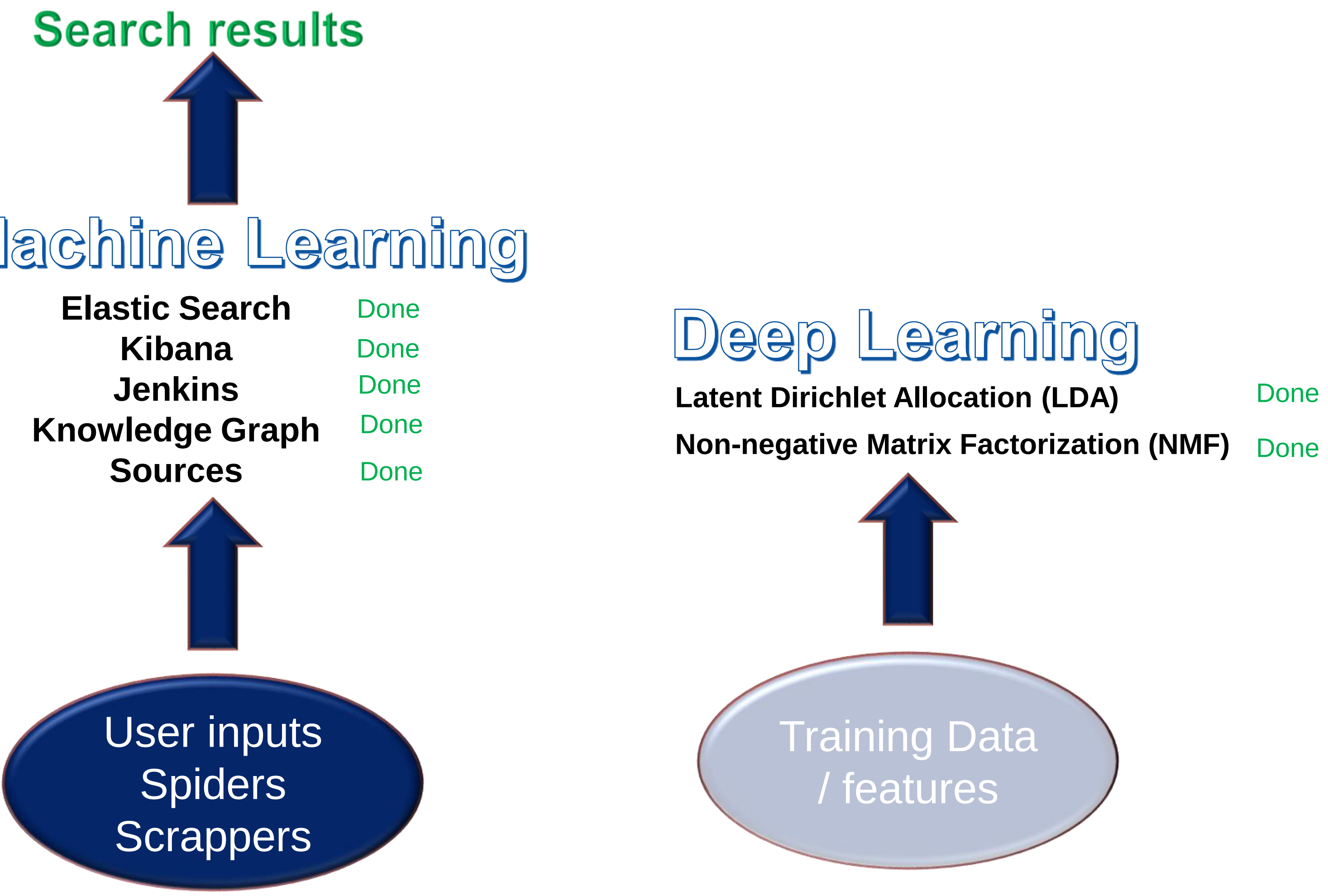
Article Type : web

Published Date : 2018-10-07T14:08:04+00:00

Experts from Symantec collected evidence that APT28 group returns to covert intelligence gathering operations in Europe and South America. APT28 state-sponsored group (aka Fancy Bear, Pawn Storm, Sofacy Group, Sednit, and STRONTIUM) seems to have shifted the focus for its operations away from election interference to cyber espionage activities. The APT28 group has been active since at least 2007 and it has targeted governments, militaries, and security organizations worldwide. The group was involved also in the string of attacks that targeted 2016 Presidential election. According to experts from Symantec, the group is now actively conducting cyber espionage campaigns against government and military organizations in Europe and South America. Starting in 2017 and continuing into 2018, the APT28 group returned to covert intelligence gathering operations in Europe and South America. “After receiving an unprecedented amount of attention in 2016, APT28 has continued to mount operations during 2017 and 2018. However, the group’s activities since the beginning of 2017 have again become more covert and appear to be mainly motivated by intelligence gathering.” reads the analysis published by Symantec. “The organizations targeted by APT28 during 2017 and 2018 include: The cyberespionage group used several malware and hacking tools from its arsenal, including the Sofacy backdoor, the in composed of two main components; the Trojan.Sofacy (aka Seduploader) used for basic reconnaissance and the Backdoor.SofacyX (aka X-Agent) which was used as a second stage info-stealing malware. The APT group is also using the recently discovered Lojax UEFI rootkit that allows the attackers to maintain persistence on the infected machine even if the operating system is reinstalled and the hard drive is replaced. Symantec researchers also highlighted possible links to other espionage operations, including the Earworm that has been active since at least May 2016 and is involved intelligence-gathering operations against military targets in Europe, Central Asia, and Eastern Asia. The Earworm group carried out spear-phishing campaigns aimed at delivering the Trojan.Zekapab downloader and the Backdoor.Zekapab. Experts noticed some overlap with the command and control infrastructures used by Earworm and APT28. “During 2016, Symantec observed some overlap between the command and control (C&C) infrastructure used by Earworm and the C&C infrastructure used by Grizzly Steppe (the U.S. government code name for APT28 and related actors), implying a potential connection between Earworm and APT28. However, Earworm

1^{st} Prototype (2018)





Search results

Machine Learning

Elastic Search Done

Kibana Done

Jenkins Done

Knowledge Graph Done

Sources Done

User inputs
Spiders
Scrappers

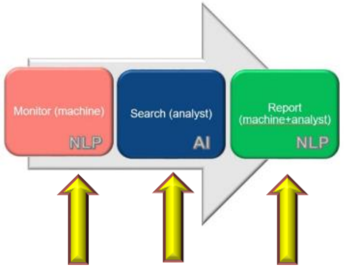
Deep Learning

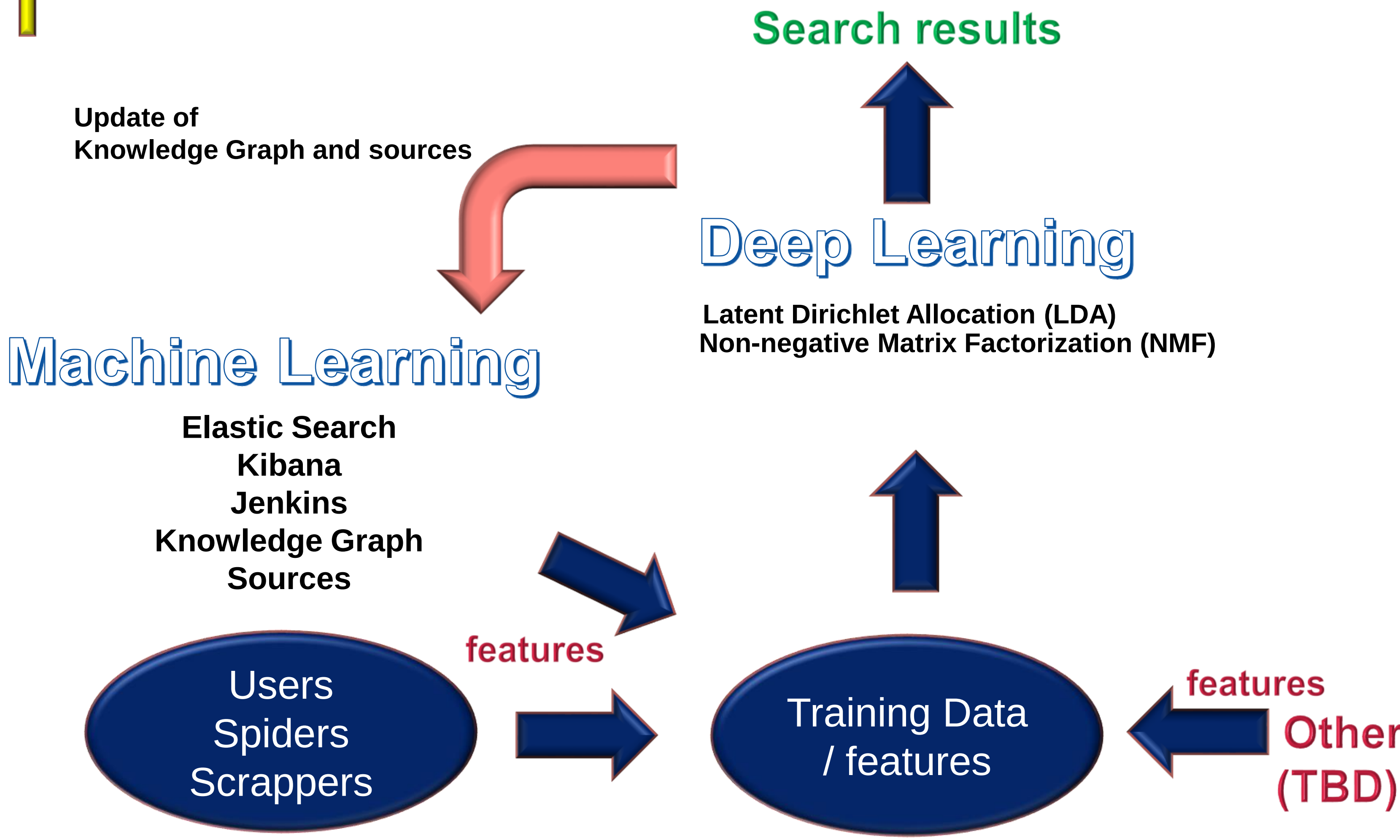
Latent Dirichlet Allocation (LDA) Done

Non-negative Matrix Factorization (NMF) Done

Training Data
/ features

2nd Prototype (2019)





Search results

Update of
Knowledge Graph and sources

Deep Learning

Latent Dirichlet Allocation (LDA)
Non-negative Matrix Factorization (NMF)

Machine Learning

Elastic Search
Kibana
Jenkins
Knowledge Graph
Sources

features

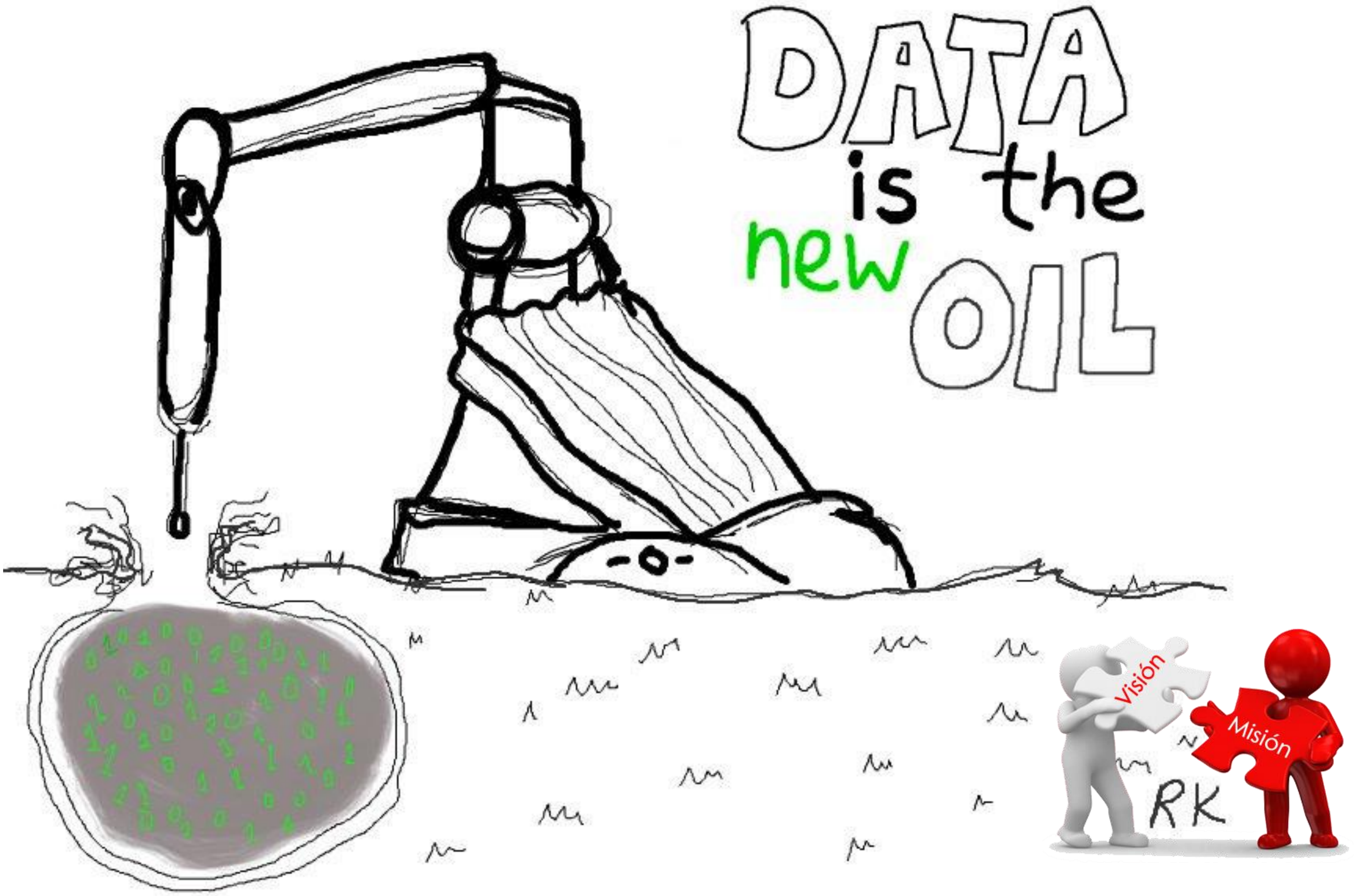
Users
Spiders
Scrappers

Training Data
/ features

features

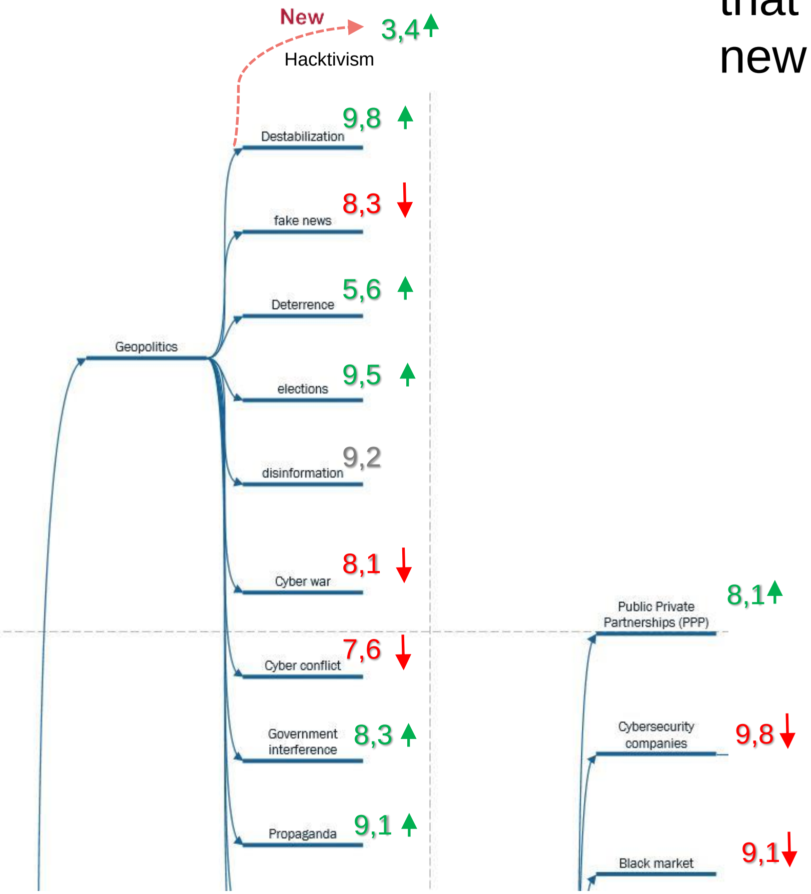
Other
(TBD)

WAY FORWARD

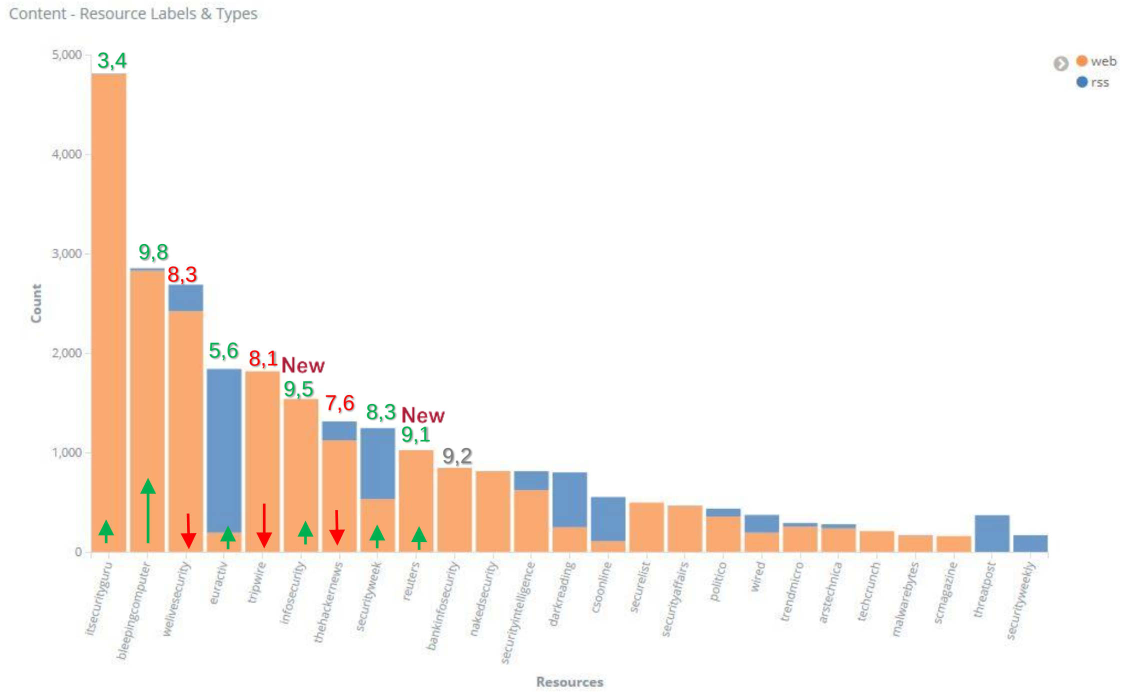


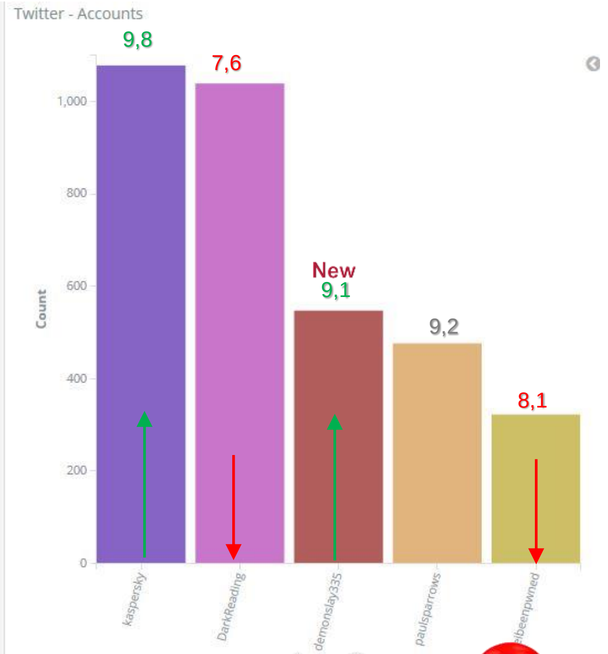
DATA
is the
new
OIL
Visión
Misión
RK

Develop a dynamic knowledge graph fed by threat analysts and AI that will keep itself up to date by adding new terms and delete obsolete ones



Develop a dynamic pool of sources fed by threat analysts and AI





Originality
Authenticity
Popularity
Quality

Also…new types of sources like DarkWeb, Pastebin and sentiment analysis !

The Vision

Make enisa an open source info hub with good training data for AI available for all

Threat analysts ↔

CSIRTs ↔

Cyber Security Professionals ↔

Open CSAM
situation awareness for cybersecurity executives
NLP
TAXONOMY
CYBERSECURITY SITUATION BRIEFING
WHAT
HOW

Training data for AI →

Academia
Essential Services providers
Researchers
Cyber Security professionals
.
.
.
.

Use services
Contribute to QoS

European Commission
European Council
enisa
EUINTCEN INTELLIGENCEANALYSISCENTRE
CSIRTs NETWORK
EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL
computer emergency response team CERT-EU
EUROPEAN DEFENCE AGENCY

EPILOGUE

Beta testers welcomed. Let us know if you are interested !

georgios.chatzichristos@enisa.europa.eu

https://github.com/enisaeu/OpenCSAM

THANK YOU FOR YOUR ATTENTION

Vasilissis Sofias Str 1, Maroussi 151 24,
Attiki, Greece

☎ +30 28 14 40 9711

✉ info@enisa.europa.eu

🌐 www.enisa.europa.eu