

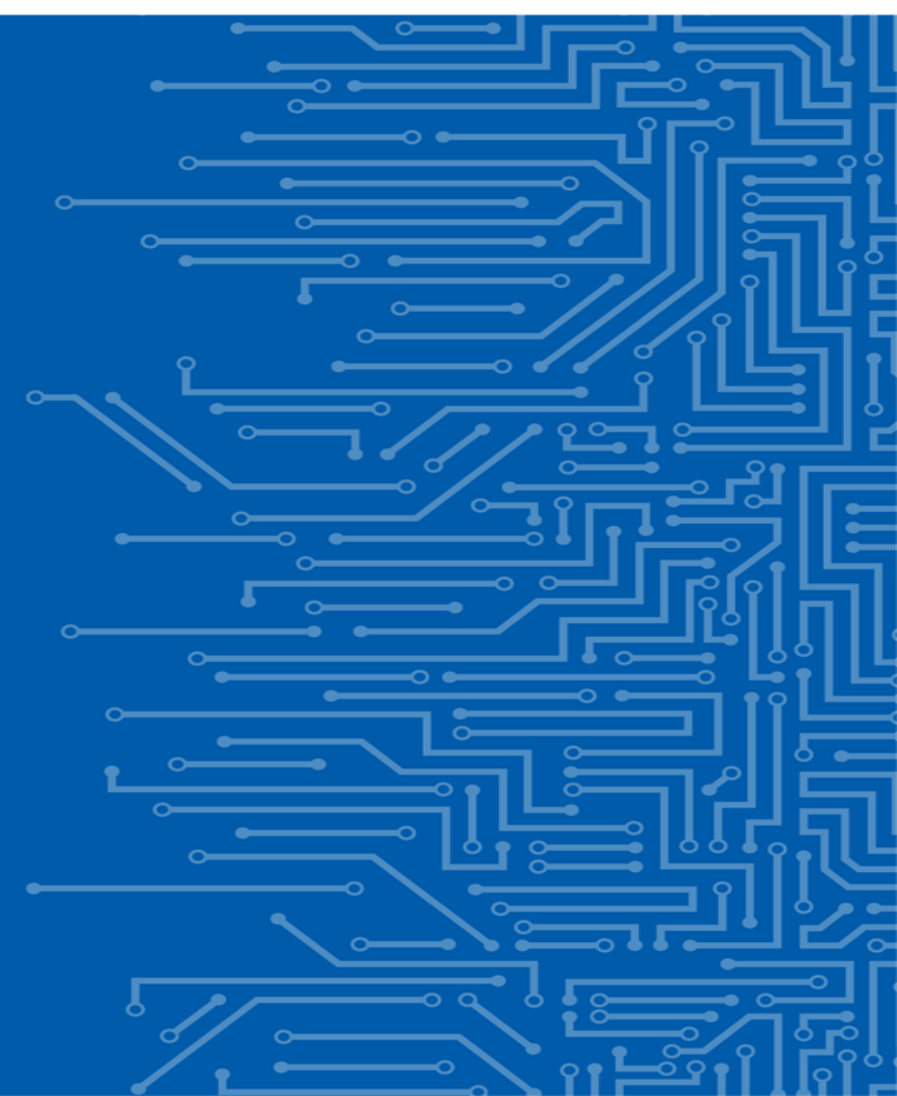


THE EU CYBERSECURITY AGENCY

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

Georgios Chatzichristos
Operational Security Unit - ENISA

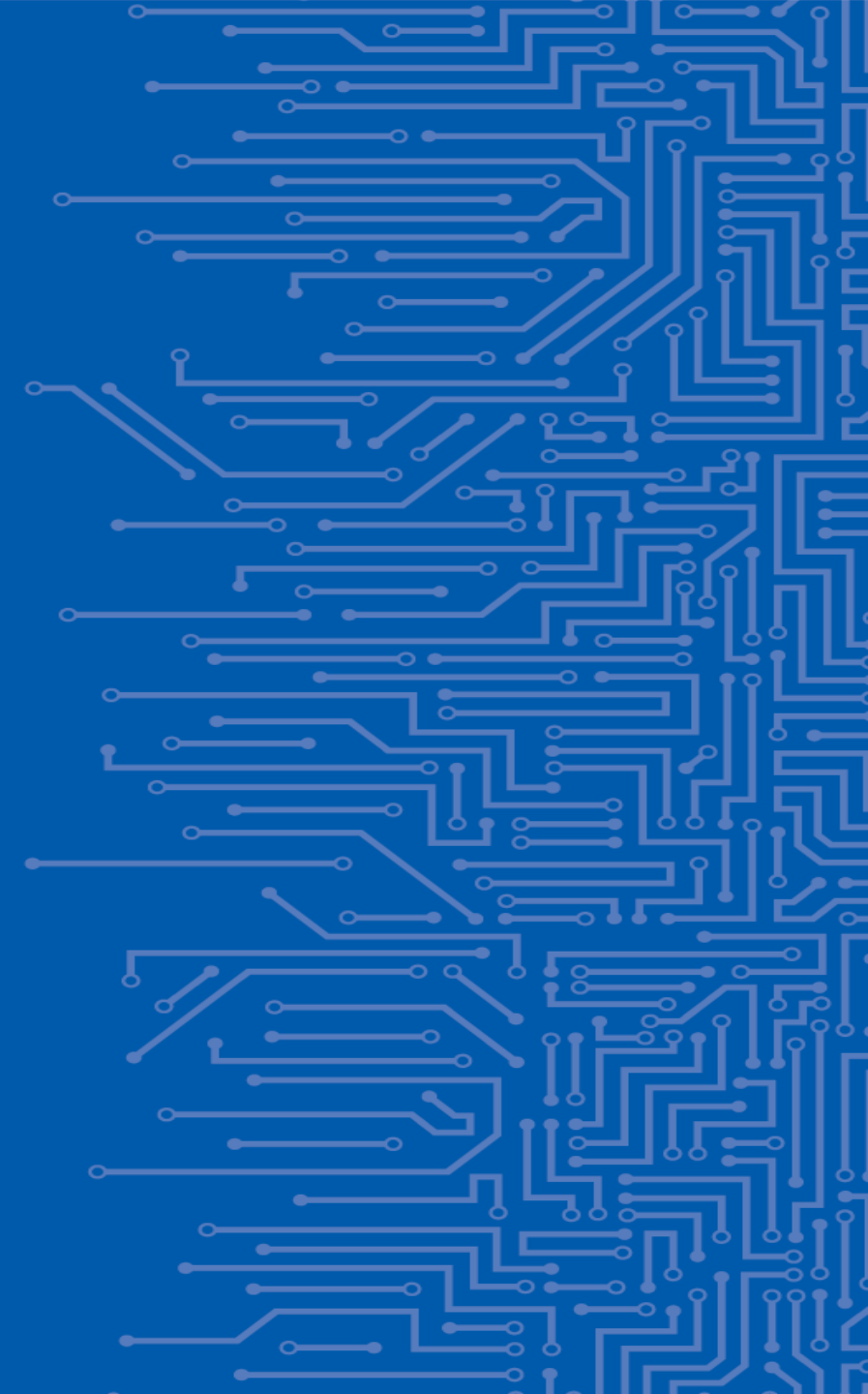
| | 04 06 2019



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.

Technical



Blue

Operational



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 Report²⁵ which is presented to the Presidency, the Commission and the HRVP via the CSIRT of the rotating Presidency.

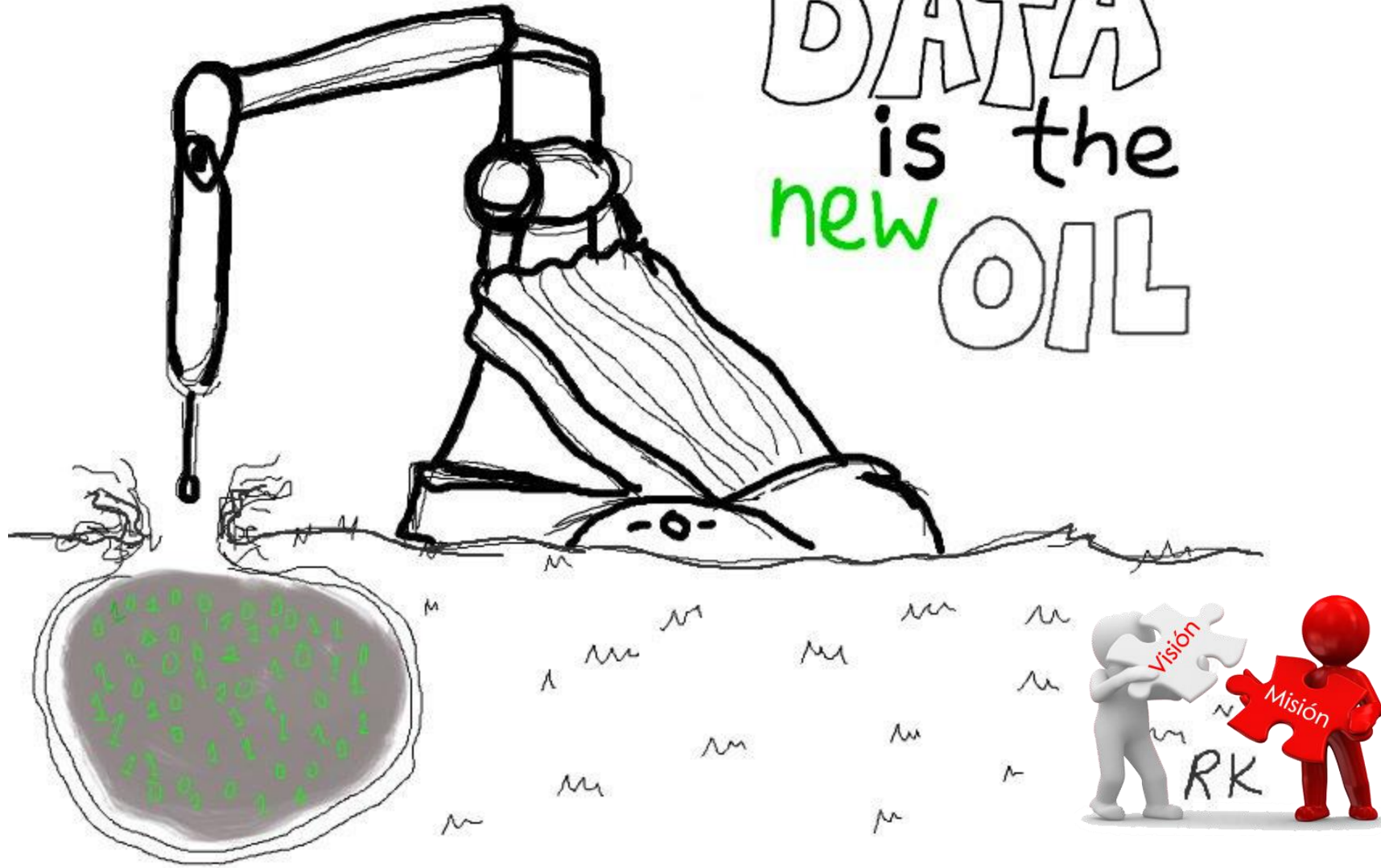


Operational
Technical

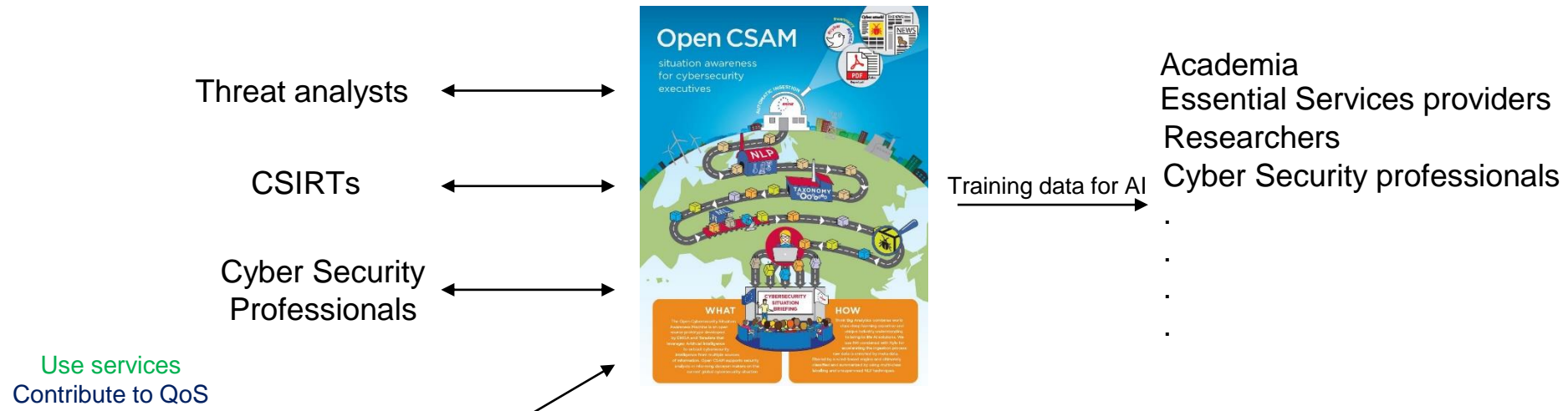
11

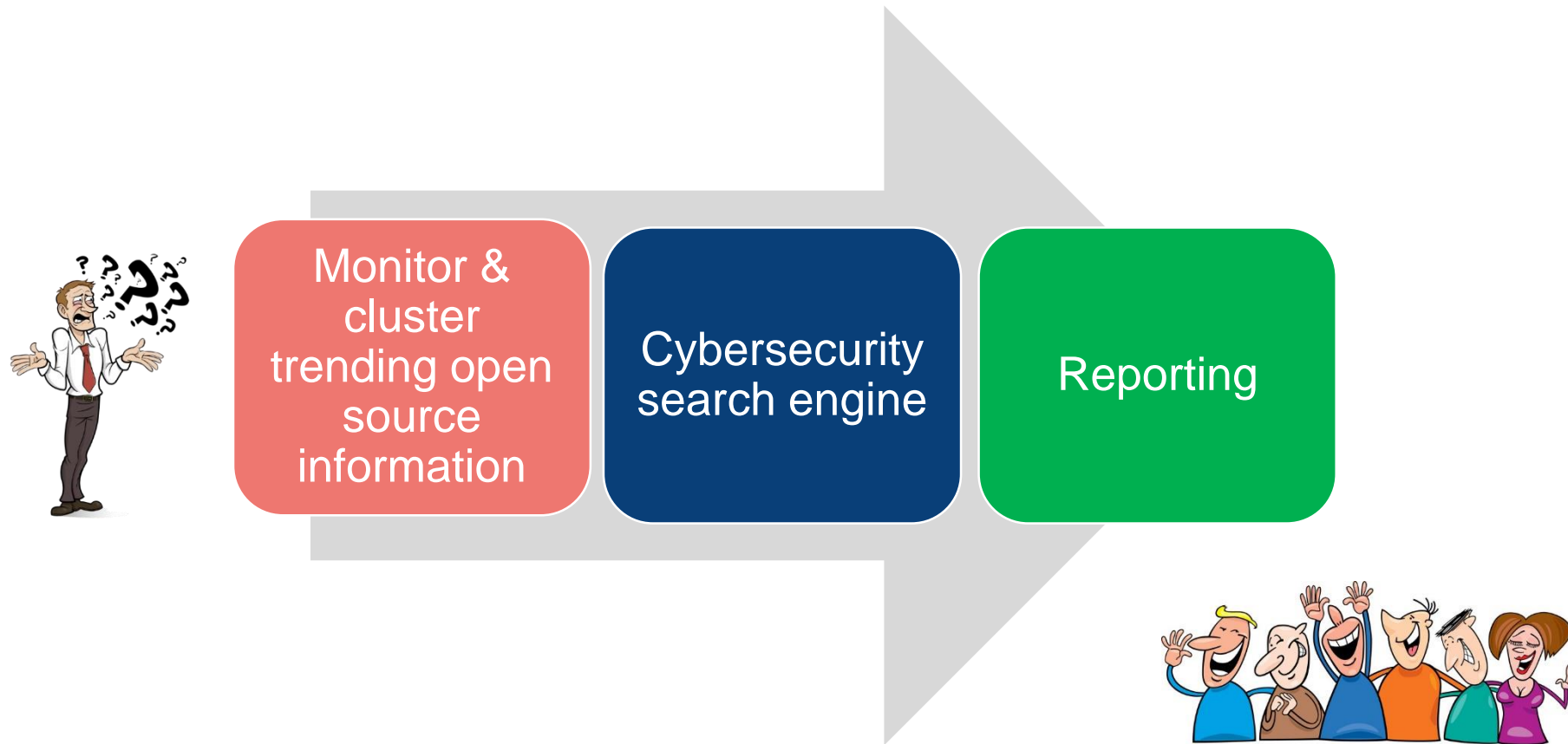
- Both reports are disseminated to EU and national stakeholders to contribute to their own situational awareness and inform decision making and facilitate cross-border regional cooperation.

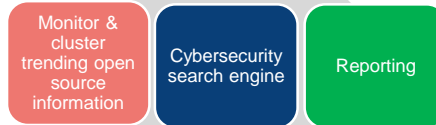
DATA
is the
new
OIL



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







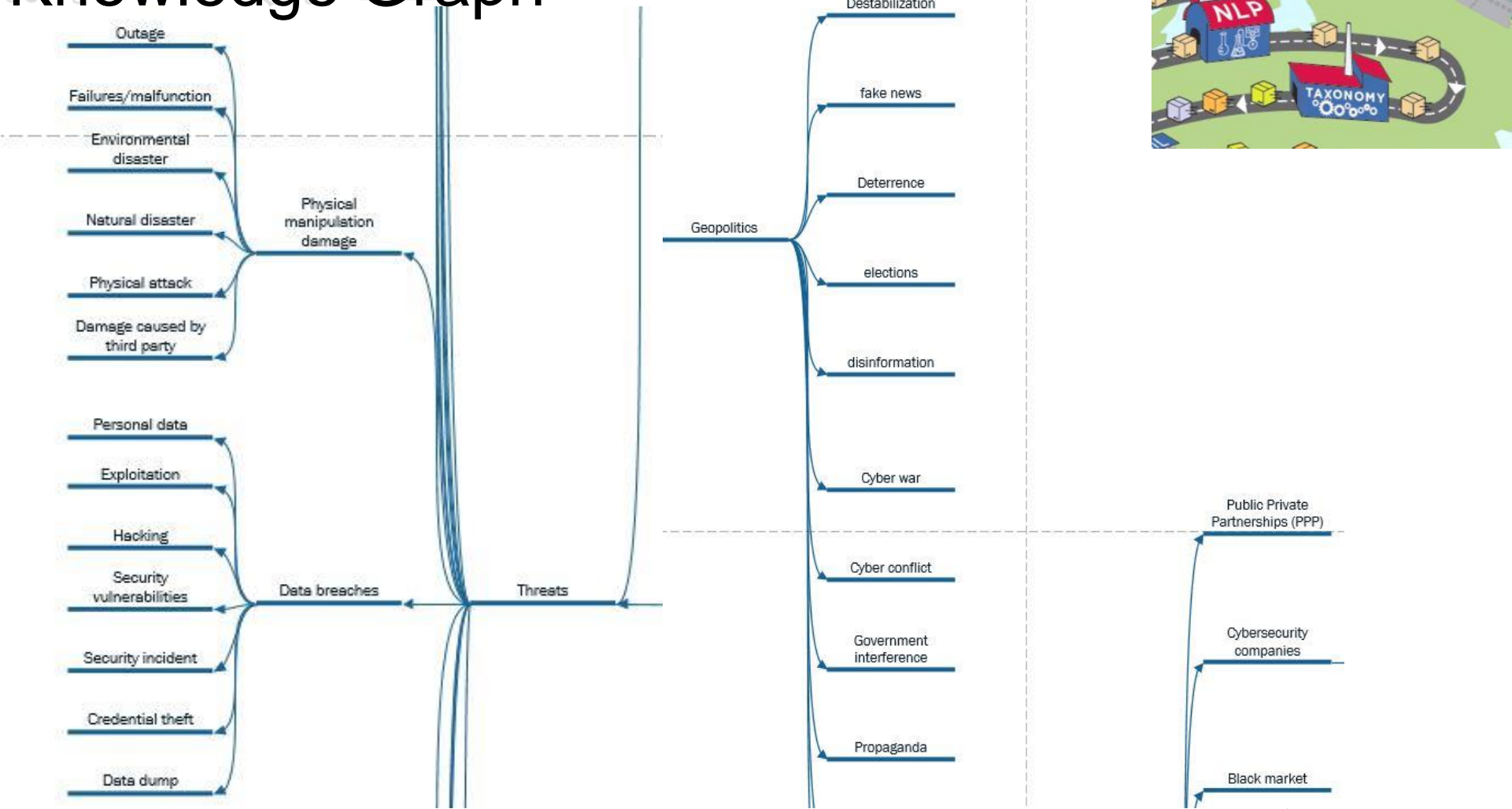
Topics - Search

1-50 of 107 < >

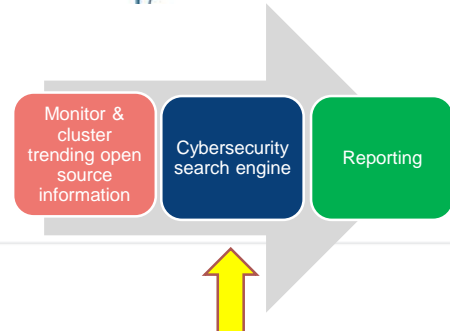
Time	cluster0	cluster1	cluster2	cluster3	cluster4
▶ October 24th 2018, 07:14:40.579	vulnerabilities, viruses, trojans, spam, releases	technology, company, according, report, today	vulnerability, server, affected, used, remote	october, european, national, government, eu	attacks, group, threat, systems, 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, according, report, world	vulnerability, server, used, code, remote	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	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



Web Articles and RSS

- <https://www.bleepingcomputer.com/>
- <https://arstechnica.com/tag/security/>
- <https://threatpost.com/>
- <https://www.darkreading.com/attacks-breaches.asp>
- <https://techcrunch.com/tag/cybersecurity/>
- <https://www.csoonline.com/category/security/>
- <https://www.csoonline.com/category/hacking/>
- <https://www.csoonline.com/category/malware/>
- <https://www.csoonline.com/category/loss-prevention/>
- <https://www.csoonline.com/category/social-engineering/>
- <https://www.csoonline.com/category/access-control/>
- <https://www.securityweek.com/>
- <https://securityaffairs.co/wordpress/>
- <https://nakedsecurity.sophos.com/>
- <https://securelist.com/>
- <https://securityintelligence.com/>
- <https://www.bankinfosecurity.com/>
- <https://www.symantec.com/blogs/>
- <https://www.fireeye.com/blog/threat-research.html>
- <https://blogs.cisco.com/security>
- <https://blog.malwarebytes.com/>
- <http://www.itsecurityguru.org/>
- <https://www.scmagazine.com/cybercrime/section/6950/>
- <http://www.bbc.com/news/topics/cz4pr2gd85qt/cyber-security>
- <https://www.independent.co.uk/topic/cyber-security>
- <https://www.reuters.com/news/archive/cybersecurity>
- <https://www.euractiv.com/sections/cybersecurity/>
- <https://www.politico.com/cybersecurity>
- <https://www.wired.com/category/security/>
- <https://www.secureworks.com/research>
- <https://www.tripwire.com/state-of-security/>
- <https://blog.trendmicro.com/trendlabs-security-intelligence/>
- <https://thehackernews.com/>
- <https://news.hitb.org/tags/security?q=tags/security&page=1>
- <https://www.infosecurity-magazine.com/news/>
- <https://www.ncsc.gov.uk/index/news>
- <https://www.welivesecurity.com/>

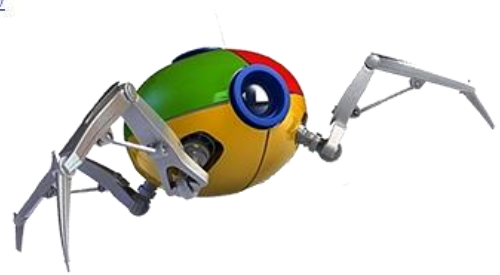


Cyber Security Search

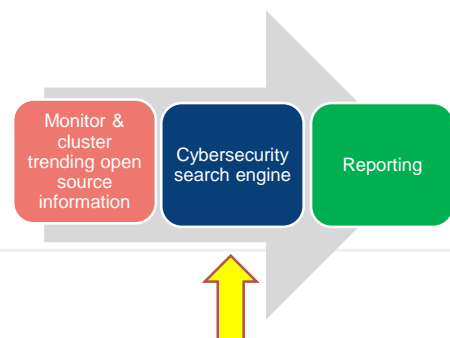
Search here


Twitter Profiles

- [DarkReading](#)
- [kaspersky](#)
- [paulsparrows](#)
- [demonslay335](#)
- [havebeenpwned](#)



ENISA is an agency of the European Union 





Custom Threats Technology Business Policy Geopolitics

apt 28

News Articles
 Twitter Feed
 ENISA Reports
 ENISA Recommendations

Knowledge Graph
 Time Decay
 Popularity of Sources

Advanced Persistent Threats: Using multi-layered detection to defend against APTs

[Link](#) Type: web Source: welivesecurity

Wednesday, April 15, 2015

 8.5

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

[Link](#) Type: web Source: securelist

Thursday, May 21, 2015

 8.5

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

[Link](#) Type: web Source: securelist

Thursday, May 14, 2015

 8.4

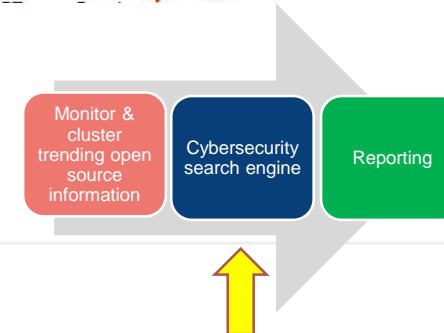
Our recent report, "The Chronicles of the Hellsing APT: the Empire Strikes Back" began with an introduction to the Naikon APT, describing it as "One of the most active APTs in Asia, especially around the South China Sea". Naikon was mentioned because of its role in what turned out to be a unique and 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

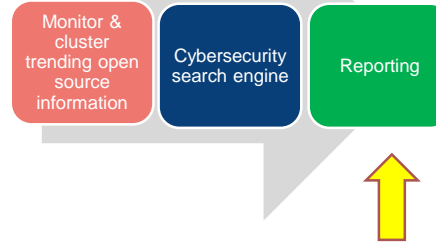
CrowdStrike uncovered a new campaign of GOBLIN PANDA APT aimed at Vietnam

[Link](#) Type: rss Source: cert

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

 8.3





Custom Threats Technology Business Policy Geopolitics

Notes

Abstract Article 1 Article 2 Article 3 Article 4 Article 5 Article 6

Geopolitical Situation

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

Political Situation

Economy

Cyber element

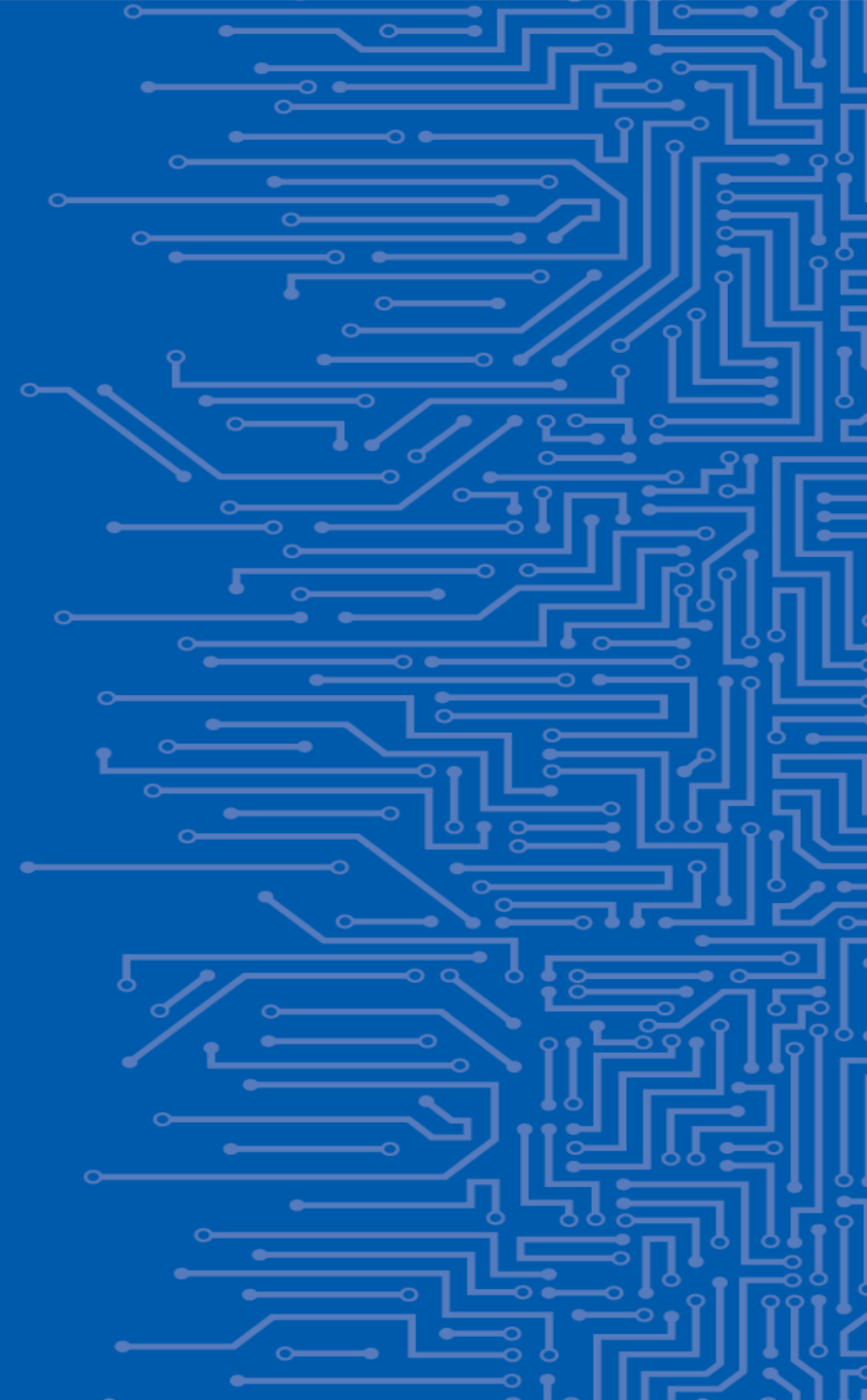
Experts from Symantec collected evidence that APT28 group returns to covert intelligence gathering operations in Europe and South America. [APT28](#) state-sponsored group (aka Fancy Bear, Pawn Storm, Sofacy Group, Sednit, and STRONTIUM) seems to have shifted the focus for its operations away from election 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

Save Notes Back to article selection



OPENCSAM CURRENT STATUS OF DEVELOPMENT

EAU DE WEB

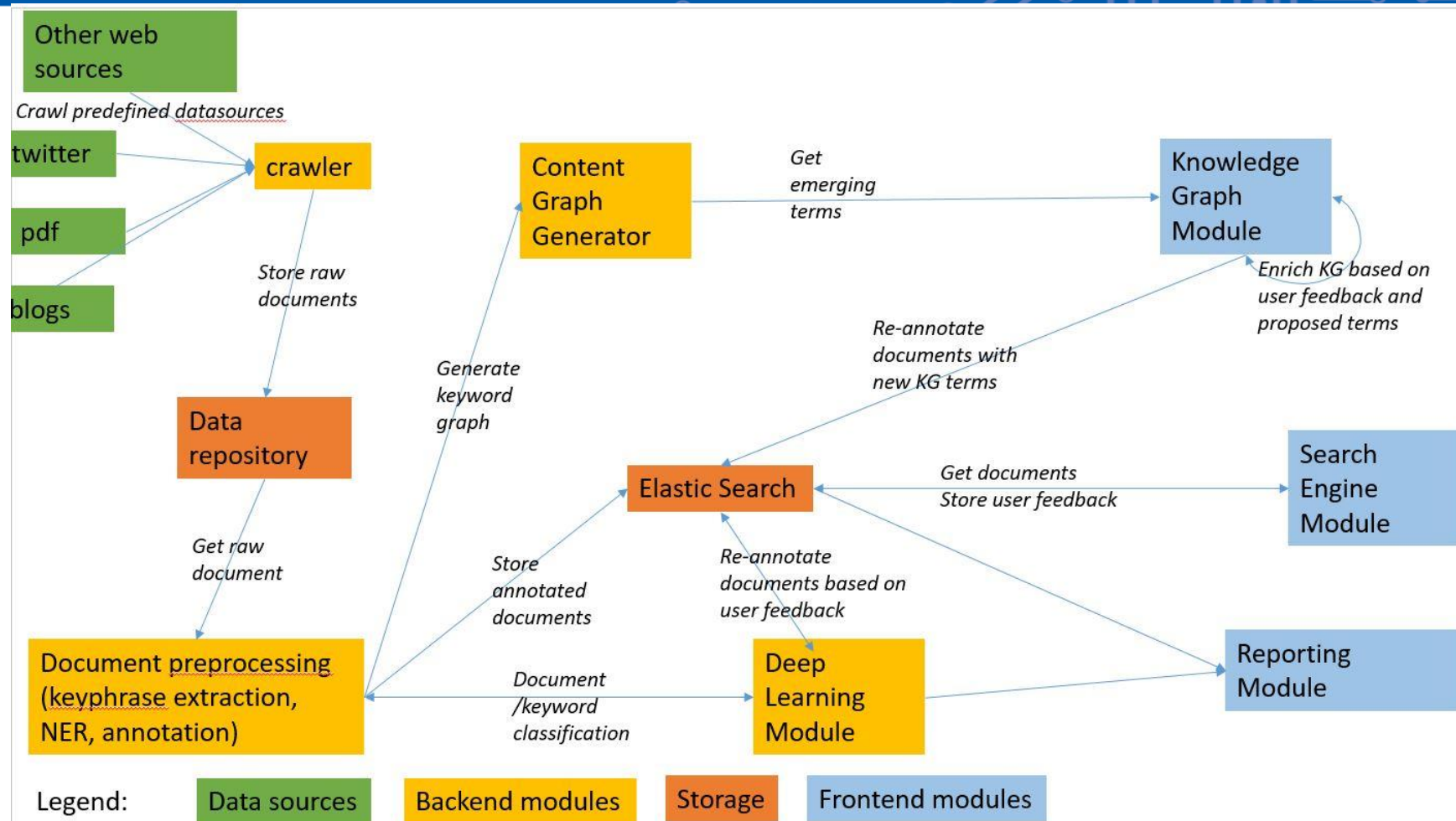


OPENCSAM STATUS

3 main directions:

- Scalable backend using Django REST API
- Friendly UX for all user types
- Proof-of-concept implementations for:
 - **Knowledge Graph enrichment** (w/ Twitter hashtags and PageRank)
 - **News clusterization** (w/ Universal Sentence Encoder)
 - **Text summarization** (w/ Universal Sentence Encoder)
 - **Classify web content for KG terms** (w/ Tensorflow and corpus-derived FastText SkipGram word embeddings)
 - **Classify web corpus** (w/ USE & seed corpus)

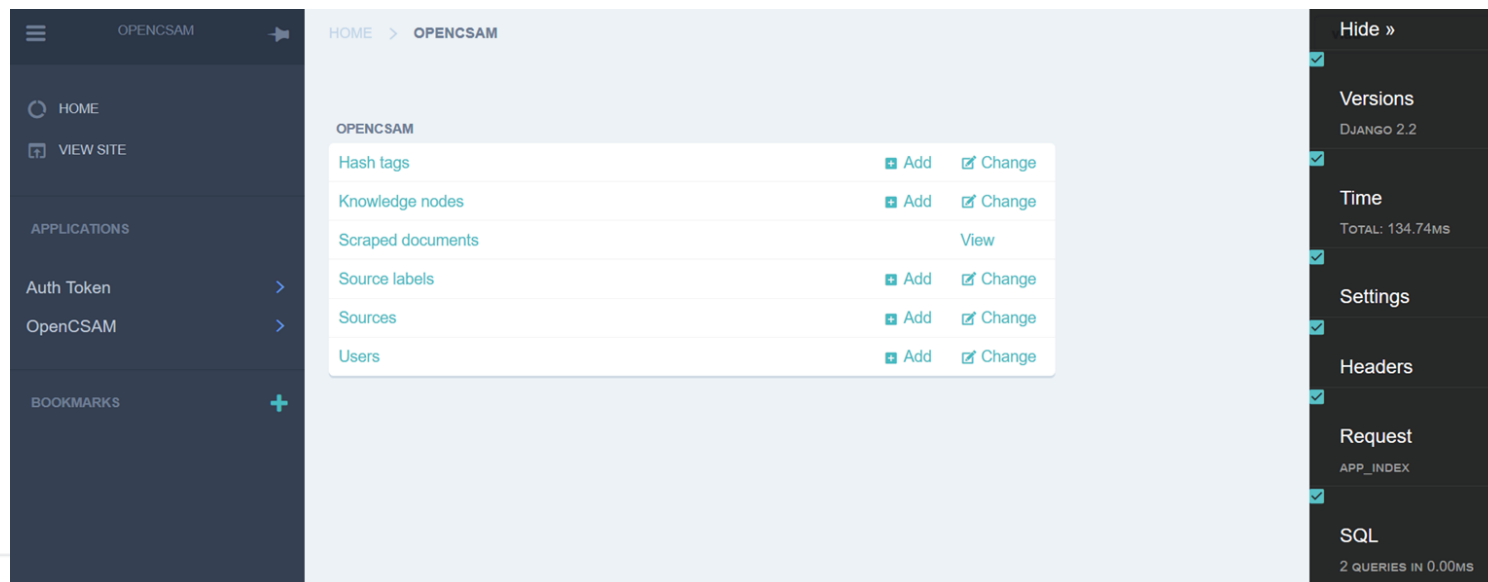
OPENCNSAM ARCHITECTURE



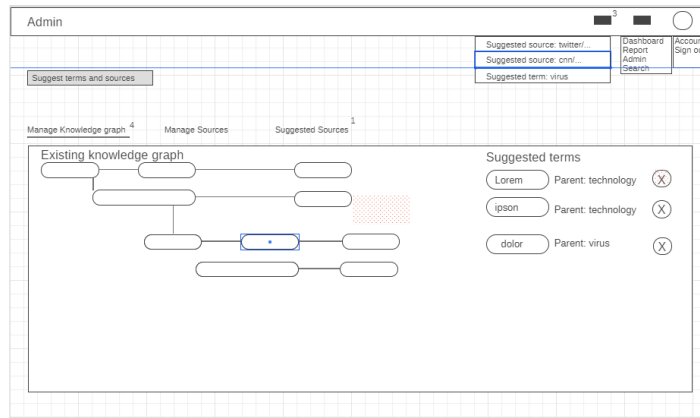
OPENCSAM - BACKEND

Django REST API based backend
Celery for queue management and scrapers

Postgresql database
ElasticSearch for document management
Docker for easy deployment



OPENCNSAM - UI DEVELOPMENT



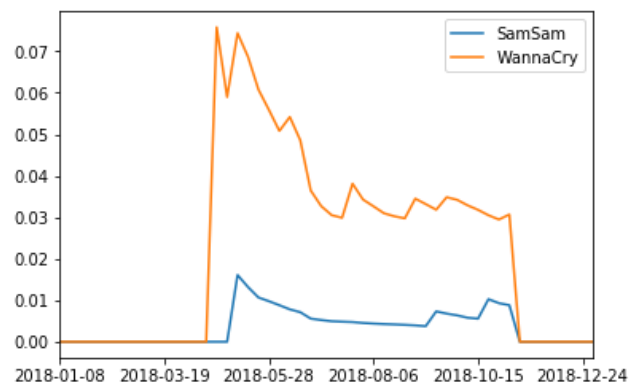
- Developed wireframes for main modules:

- Knowledge graph
- Reporting/summarisation
- Trending terms
- Search
- Source administration



OPENCSAM - UI DEVELOPMENT

Dynamic KG editor prototype Term evolution over time



EXPAND ALL COLLAPSE ALL

- + Assets
- + Business
- + Emerging technology
- + General terms
- + Geopolitics
- Policy
- Ban
- Cybersecurity doctrine
- Cybersecurity strategy
- + Directives

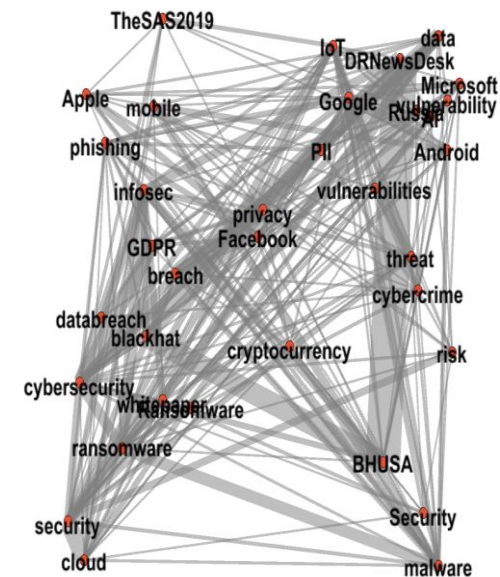
Children

- Ban
- Cybersecurity doctrine
- Cybersecurity strategy
- Directives
- EIDAS
- Regulation
- Synonyms

- security
- cybersecurity
- malware
- IoT
- Ransomware
- ransomware
- infosec
- phishing
- BHUSA
- cloud
- privacy

OPENCSAM KG SUGGESTED TERMS

- Extract emerging terms (hashtag co-occurrence)
- Generate co-occurrence graph
- Score concepts with PageRank
- Detect variations in rank over time
- Suggest terms with the highest positive variation
- The super-user adds the terms to the KG



OPENCSAM – KEYPHRASES

- Build a set of corpus-wide common keyphrases
 - bigrams and trigrams, scored using Normalized Pointwise Mutual Information (NPMI)
 - 1,2,3,4 elements PositionRank-ed keyphrases
- Cluster the keyphrases using word embeddings
- Build co-occurrence graph, use traverse distances as feature in text classification task
- Propose for Knowledge Graph, based on quality

OPENCSAM – CLUSTER NEWS

High quality sentence encodings from Universal Sentence Encoder

- Seed topics with “topic words”
- Encode topic words and news titles to vectors
- Set seed-word vectors as cluster centers
- Group titles around cluster centers

Future:

- replace USE with BERT, finetune for our corpus
- Explore VLAWE (Vector of Locally-Aggregated Word Embeddings)

OPENCSAM – SUMMARISATION

- Extractive summarization (best ranked phrases)
- Users can select phrases to be kept/removed
- Included text comes from multiple articles
- Algorithm uses **Universal Sentence Encoder** sentence embeddings

JOIN THE OPENC SAM COMMUNITY

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

