

ADVANCED OSINT ANALYSIS FOR NIS AUTHORITIES, CSIRT TEAMS AND ORGANISATIONS

IKT Sicherheitskonferenz des AbwA

Florian Skopik and **Benjamin Akhras**
Center for Digital Safety and Security
AIT Austrian Institute of Technology



Linz, October 3rd, 2023



WHAT IS CYBER SECURITY OSINT?

- Open-source intelligence (OSINT) is the collection and analysis of data gathered from open sources to produce actionable intelligence.
- Technical Cyber Threat Intelligence (CTI) to configure detection systems:
 - Indicators to put into SIEMs
 - Domains to block in name-servers or proxies
 - Execution patterns to block in EDRs
- But also “softer CTI”:
 - News about threat actors
 - New (features of) security products
 - News about breaches, incidents, campaigns
 - News about vulnerabilities, patches, mitigations, counter-measures, exploitation, post-exploitation, ...
 - Policy news: political/diplomatic initiatives, new EU policy documents, GDPR-related lawsuits
 - Updates on security standards (ISO, BSI, ANSI, CIS, OWASP, ...)
 - Mergers, acquisitions, failures, ... or other company news

Baseline today at CERT.at:
approx 250 sources, up to
500 articles per day, more
after longer weekends or
large-scale events

WHAT IS OSINT GOOD FOR?

- Gather public information on potential security threats, vulnerabilities, trends, attacker TTPs, new risks etc. to maintain situational awareness and take early counter actions.
- Input for products
 - Advisories
 - Summaries (daily, weekly)
 - Situational picture reports, white papers, fact-sheets
- Awareness / Preparedness
 - Consulting / Answering calls for help
 - Media inquiries
 - “Boss/CEO/Politician asking questions”
 - Trigger for proactive activities
- Challenge: Number of OSINT sources is high and the number of news items massive
 - Grasp quickly what’s relevant and omit the rest
 - Filter repetitive content
 - The workflow is actually pretty similar to a journalists work



CEF PROJECT AWAKE



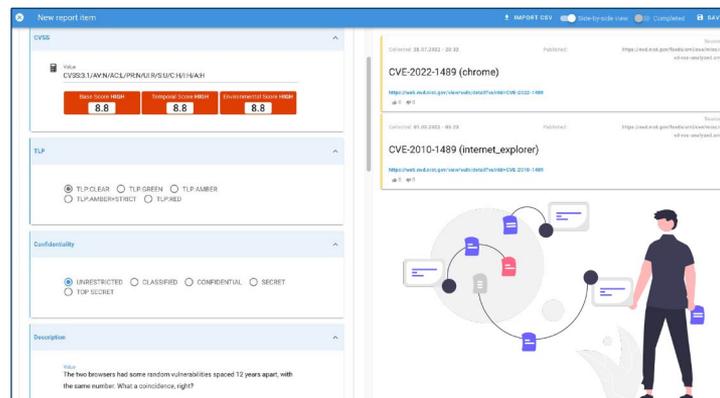
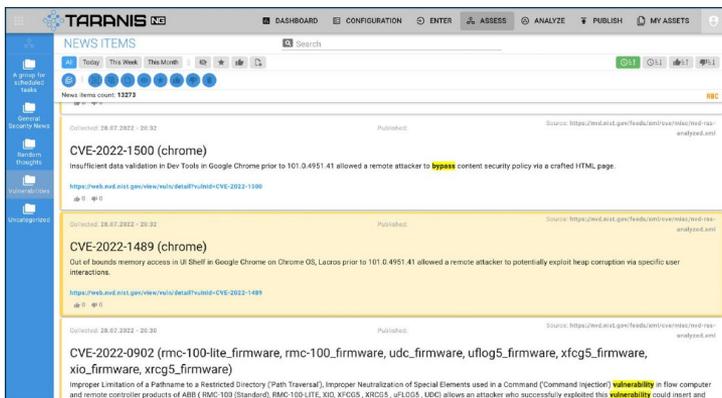
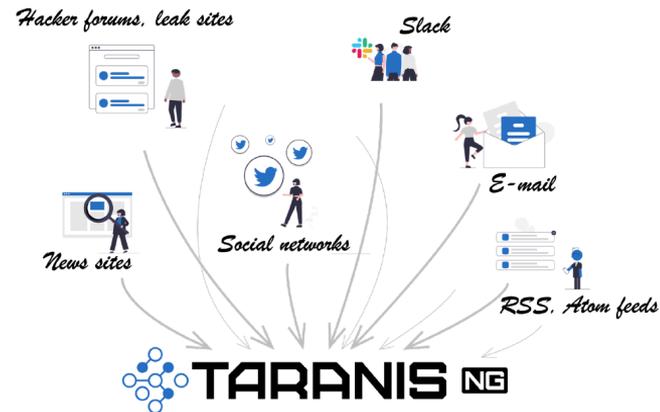
Co-financed by the Connecting Europe
Facility of the European Union



- CEF funded project:
 - AIT (coordinator), CERT.at, Ministry of the Interior (NIS-CA), Federal Chancellery
- Main Goal
 - Sharing Situational Awareness between the NIS actors in Austria (CSIRT, NIS-CA(s), LEA, MFA)
 - By collecting, aggregating, filtering, translating and sharing situational information
- Focus on
 - Unstructured data
 - Freeform text
 - For human consumption
 - Focus is **not** on technical or operational data, but on high-level, strategic information



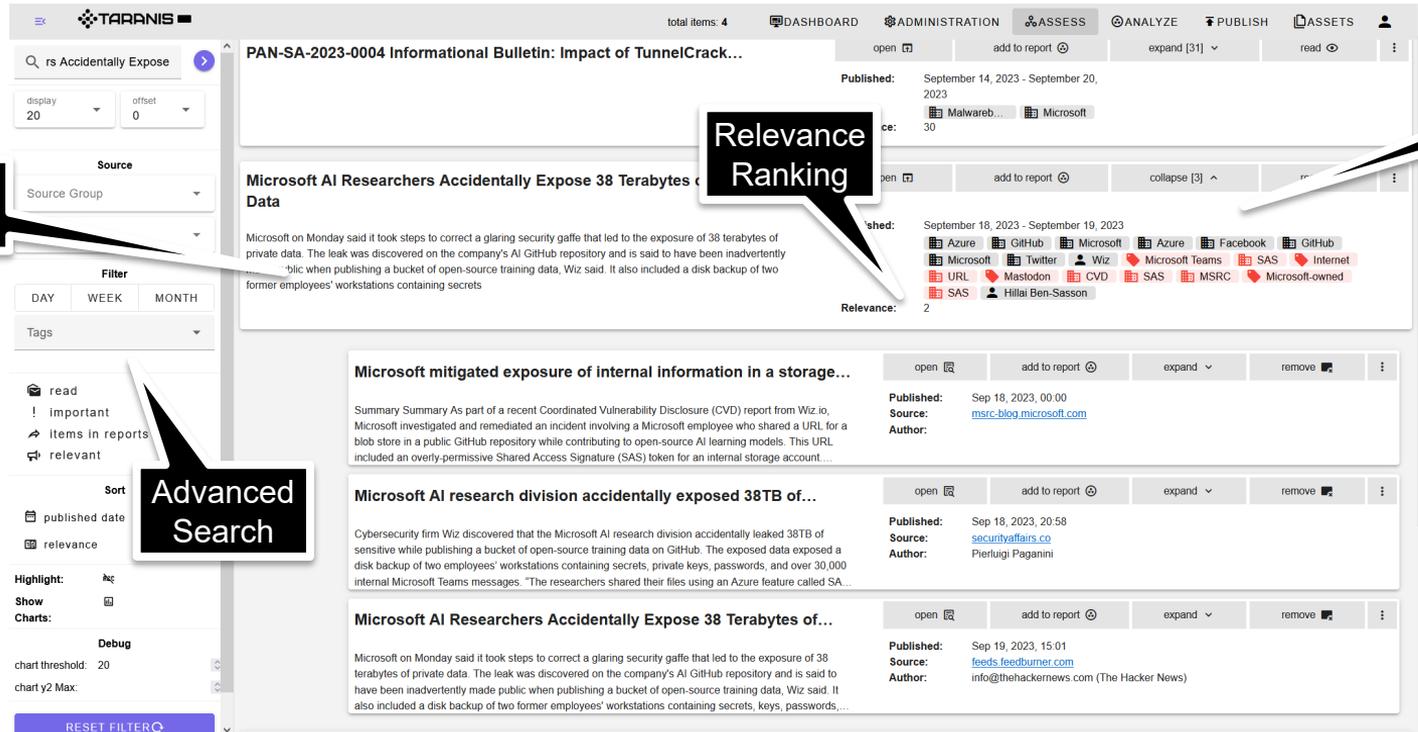
- Ingest raw unstructured data from various sources
- Use human knowledge to identify relevant information
- Compile reports and distribute advisories and reports to the community
- → A great tool and an awesome basis for further extensions using modern NLP and machine learning ...



APPLYING THE POWER OF NLP

- 
- 1 User Story 1: What was going on in the last 24 hours? („Hot Topics Clustering“)
 - 2 User Story 2: What do we know about entity X? (e.g., a vulnerability, malware, company, product)
 - 3 User Story 3: I've read an interesting article. What related news items do exist?
 - 4 User Story 4: Which news items are recommended (collaboratively and AI-assisted)?
 - 5 User Story 5: I'd like to build a sharing set for my partners. How to sum up my findings?

NOVEL FEATURES AND DEVELOPMENTS



The screenshot shows the TARANIS interface with a search query 'rs Accidentally Expose'. The main content area displays a list of search results. The top result is titled 'Microsoft AI Researchers Accidentally Expose 38 Terabytes of Data'. Below it are two more results with similar titles. The interface includes a left sidebar with filters and a top navigation bar with tabs like DASHBOARD, ADMINISTRATION, ASSESS, ANALYZE, PUBLISH, and ASSETS.

Summary Creation

Relevance Ranking

NER

Advanced Search

Story Clustering

FEATURES (1/5): NAMED ENTITY RECOGNITION

- Named-entity recognition (NER) seeks to locate and classify named entities mentioned in unstructured text into pre-defined categories such as person names, organizations, locations, etc.
- Mix of pre-defined lists (e.g., countries), custom regex (e.g., CVEs), and trained language model on German/English standard text
- Custom extensions to recognize IT products, vendors, APT groups etc.
- *Future Extension:*
 - Additional use of domain-specific word lists

open | add to report | collapse [4] | read | ⋮

Published: September 17, 2023 - September 20, 2023

Tags: Liechtenstein, Schweiz, Österreich, DoppelPaymer, Ukraine, Deutschland, Vaduz, Franz Ruf, fedpol, Nicoletta della V..., Jules Hoch, Sabine Monauni, Ruf, LKA, Süddeutschland, Igor Garshin, Europol, FBI, Parker, Garshin

Relevance: 3

open | add to report | collapse [2] | read | ⋮

Published: September 15, 2023 ⚠

Tags: Volt Typhoon, PDF, Microsoft, China, Russia, Taiwan, Ukraine, FortiOS, FortiProxy, FortiWeb, Fortinet, CVE-2023-29183, CVE-2023-34984

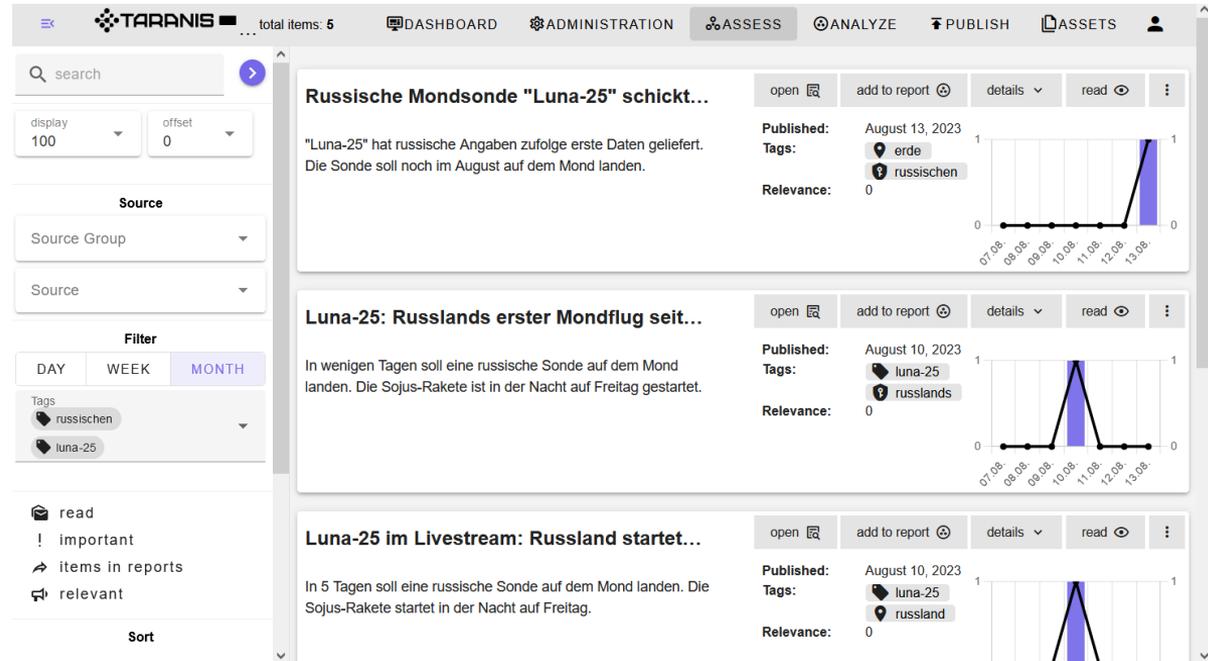
Relevance: 1

DoD: China's ICS Cyber Onslaught Aimed at Gaining Kinetic Warfare Advantage

Escalating incursions into military base infrastructure, telecom networks, utilities, and more signal that Beijing is laying the groundwork for mass disruption.

FEATURES (2/5): ADVANCED SEARCH & FILTERING

- Tags from NER can be used to filter and cluster items belonging to the same topic
- Additional free-text search
- Further filter and sort parameters (read/unread, relevance score etc.)
- *Future extension:*
 - Collaborative search and filtering
 - Sharing of filters



The screenshot shows the TARPANIS dashboard with a search bar and various filters. The search results are displayed in a list view, showing three items related to the Russian moon probe 'Luna-25'. Each item includes a title, a brief description, publication date, tags, and a relevance chart.

Search Results:

- Item 1:** "Russische Mondsonde "Luna-25" schickt..."
 Published: August 13, 2023
 Tags: erde, russischen
 Relevance: 0
- Item 2:** "Luna-25: Russlands erster Mondflug seit..."
 Published: August 10, 2023
 Tags: luna-25, russlands
 Relevance: 0
- Item 3:** "Luna-25 im Livestream: Russland startet..."
 Published: August 10, 2023
 Tags: luna-25, russland
 Relevance: 0

The relevance charts show a peak in relevance for the second and third items on August 10, 2023, and for the first item on August 13, 2023.

FEATURES (3/5): RELEVANCE RANKING

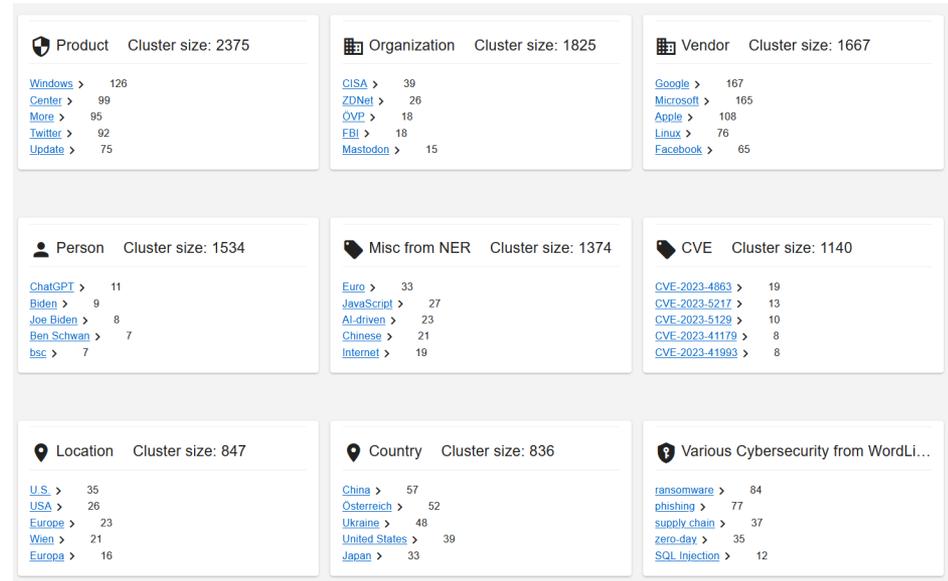
- Relevance Ranking helps to identify “interesting items” based on general importance and personal preferences
 - Upvotes and downvotes from collaborators
 - Shared articles
 - Related news items
- *Future Extensions:*
 - Feedback Loop: Learn properties of often up-/downvotes items.
 - What properties do “good” articles have in common?
 - Which sources deliver such items?

Search <input type="text"/>					NEW ITEM	IMPORT	EXPORT	COLLECT SOURCES
<input type="checkbox"/>	tag	state	name	FEED_URL	Actions			
<input type="checkbox"/>		ok	eset_WeLiveSecurity	https://feeds.feedburner.com/eset/blog?format=xml				
<input type="checkbox"/>		ok	TheHackerNews	http://feeds.feedburner.com/TheHackersNews				
<input type="checkbox"/>		ok	CERT.at (en) - Blog	http://cert.at/cert-at.en.blog.rss_2.0.xml				
<input type="checkbox"/>		ok	NOYBeu	https://noyb.eu/feed				
<input type="checkbox"/>		ok	MISP	https://www.misp-project.org/feed.xml				
<input type="checkbox"/>		error	GrahamCluley	https://www.grahamcluley.com/feed/				
<input type="checkbox"/>		ok	dalepeterson	http://unsolicitedresponse.libsyn.com/rss				
<input type="checkbox"/>		error	Exploit_DB	https://www.exploit-db.com/rss.xml				
<input type="checkbox"/>		ok	NVISO	https://blog.nviso.eu/rss				
<input type="checkbox"/>		ok	CZ.NIC	http://en.blog.nic.cz/feed/				

Items per page: 1-10 of 161 << >>

FEATURES (4/5): SUMMARY & REPORT CREATION

- Summaries help to condense lengthy texts to their essential parts for quick decisions on their relevance
 - Summary of lengthy news items to quickly grasp its content
 - Summary of stories based on its collection of articles
- *Future Extensions*
 - Summary of Sharing Sets for reports
 - AI-assisted Pre-filling of report fields
 - Tuning of summaries regarding appropriate length, wording and content



The screenshot displays a grid of nine cluster cards, each representing a different category of data. Each card includes a title, a cluster size, and a list of sub-items with their respective counts.

Cluster Name	Cluster Size	Sub-items
Product	2375	Windows (126), Center (99), More (85), Twitter (92), Update (75)
Organization	1825	CISA (39), ZDNet (26), ÖVP (18), FBI (18), Mastodon (15)
Vendor	1667	Google (167), Microsoft (165), Apple (108), Linux (76), Facebook (65)
Person	1534	ChatGPT (11), Biden (9), Joe Biden (8), Ben Schwan (7), bsc (7)
Misc from NER	1374	Euro (33), JavaScript (27), AI-driven (23), Chinese (21), Internet (19)
CVE	1140	CVE-2023-4863 (19), CVE-2023-5217 (13), CVE-2023-5129 (10), CVE-2023-41179 (8), CVE-2023-41993 (8)
Location	847	U.S. (35), USA (26), Europe (23), Wien (21), Europa (16)
Country	836	China (57), Österreich (52), Ukraine (48), United States (39), Japan (33)
Various Cybersecurity from WordLI...	-	ransomware (84), phishing (77), supply chain (37), zero-day (35), SQL Injection (12)

FEATURES (5/5): TOPIC & STORY CLUSTERING

- News Items are usually delivered not just by one, but multiple sources at approximately the same time with mostly similar content
- Cluster items and create “meta item” that summarizes important content
 - Decrease human effort needed to ingest all news items!
 - Visualize development of a story over time
- Show development of “top topics” over time

06/10/2023

Signal Messenger Introduces PQXDH Quantum-Resistant Encryption

Encrypted messaging app Signal has announced an update to the Signal Protocol to add support for quantum resistance by upgrading the Extended Triple Diffie-Hellman (X3DH) specification to Post-Quantum Extended Diffie-Hellman (PQXDH). "With this upgrade, we are adding a layer of protection against the threat of a quantum computer being built in the future that is powerful enough to break current

Published: September 14, 2023 - September 20, 2023

Tags: Azure, Google, IBM, Infrastructure, Intel, Microsoft, X3DH, RSA, transmission, supply chain, NIST, PQC, Internet, Windows NT, SSL, TLS1.3, Cryptocurrencies, Microsoft Active..., SHA-2, SaaS, DHS

Relevance: 3

Getting ready for a post-quantum world

Quantum computers are changing the cryptography rules Under Data Encryption, the CISA Zero Trust Maturity Model v2.0 cites the criticality of "cryptographic agility" on the third (out of four) level of maturity. Cryptographic agility is the ability to change the underlying cryptographic algorithms in applications and...

Published: Sep 14, 2023, 10:00
Source: [cybersecurity.ait.com](#)
Author:

Signal adds quantum-resistant encryption to its...

Signal adds quantum-resistant encryption to its E2EE messaging protocol Bill Toulas - September 20, 2023 - 09:29 AM - 0 Signal has announced that it upgraded its end-to-end communication protocol to use quantum-resistant encryption keys to protect users from future attacks. Quantum computers that us...

Published: Sep 20, 2023, 09:29
Source: [bleepingcomputer.com](#)
Author: Bill Toulas

The Signal Protocol used by 1+ billion people is...

The Signal Foundation, maker of the Signal Protocol that encrypts messages sent by more than a billion people, has rolled out an update designed to prepare for a very real prospect that's never far from the thoughts of just about every security engineer on the planet: the catastrophic fall of cryptographic protocols that secur...

Published: Sep 20, 2023, 13:59
Source: [feeds.arstechnica.com](#)
Author: Dan Goodin

Signal Messenger Introduces PQXDH Quantum-...

Encrypted messaging app Signal has announced an update to the Signal Protocol to add support for quantum resistance by upgrading the Extended Triple Diffie-Hellman (X3DH) specification to Post-Quantum Extended Diffie-Hellman (PQXDH). "With this upgrade, we are adding a layer of protection against the...

Published: Sep 20, 2023, 14:59
Source: [feeds.feedburner.com](#)
Author: info@thehackernews.com (The Hacker News)

LIVE DEMO

DEMO

CONCLUSION AND OUTLOOK

- AWAKE: several NLP extensions that improve taranis-ng to increase the efficiency of OSINT analysts by clustering, categorizing and filtering items
- Continuous development secured!
 - EDF and DEP projects until 2027
 - Collaboration with CERT.sk -> upstream of changes!
 - Opportunity to contribute: <https://taranis.ai/>
- Planned extensions:
 - Allow the collaboration across multiple instances, e.g. CERT, ministries (future extension)
 - Matching of news items to predefined asset lists (CPEs) to determine risks
 - Improvement of NLP magic
- Future application cases
 - Different from SOC cases
 - Coordination of NIS-relevant knowledge to specific topics between CERT and BM*



THANK YOU!

Please contact:

Florian Skopik

florian.skopik@ait.ac.at



October, 3rd 2023