

&&



{codemotion} CONFERENCE
MADRID 2025

LLM-Driven Attack Flow
Generation from
Security Publications





Juan Manuel Cristóbal

Senior Engineer

Senior Software Engineer con más de una década de experiencia diseñando y desplegando soluciones backend escalables para entornos de misión crítica.

Me apasiona la arquitectura en la nube, la automatización de procesos mediante prácticas DevOps y la adopción de metodologías ágiles para asegurar la calidad y el rendimiento en cada proyecto. A lo largo de mi trayectoria, he liderado implementaciones de principio a fin, garantizando que las soluciones cumplan altos estándares de seguridad y disponibilidad.

Disfruto compartiendo conocimientos sobre TDD, Python y la integración de tecnologías emergentes, con el objetivo de impulsar la innovación y el crecimiento continuo en cada equipo con el que colaboro.



Fran Gomez

Security Research

Fran Gómez (@ffranz) is a cybersecurity researcher, builder, and speaker passionate about Threat Intelligence, OSINT/OSTI, IPv6, and Hacking. Founder of @MrLooquer, the creator of @e_Sinfonier, and currently leads Security Research at @devo_inc.

Previously involved with @OwaspMadrid and @TelefonicaTech, I've been sharing security insights since 2008 and has spoken at major conferences such as RootedCON, Black Hat, Spark Summit, CCNCERT, Codemotion Amsterdam, and NIAS (@nciagency).

How
Do
You
Defend
Against
What
You
Don't
Understand?



Cybersecurity Knowledge

{E} CONFERENCE
MADRID 2025

Understand
attack vectors

Knowing how
breaches occur helps
you detect early signs

01

Reduce false
positives

Knowledge allows
better tuning of
detection systems.

02

Speed up
response

Recognizing
indicators of
compromise quickly
limits damage.

03

Design secure
systems

Developers with
security knowledge
build code that
resists exploitation.

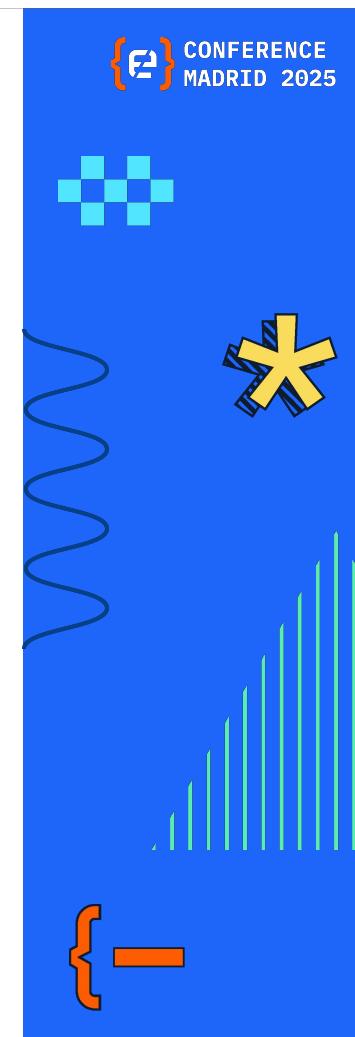
04

Anticipate
attacker behavior

Threat actors follow
patterns; knowing
them helps preempt
attacks.

05

Transforms raw data into Actionable Insight



Crucial Knowledge Areas

Security Concepts & Tools

- Threat Modeling
- Security Controls
- Vulnerability Management
- Penetration Testing



Threat Intelligence

- TTPs
 - (Tactics, Techniques, Procedures)
- Indicators of Compromise
 - (IOCs)
- Threat Actor Profiling

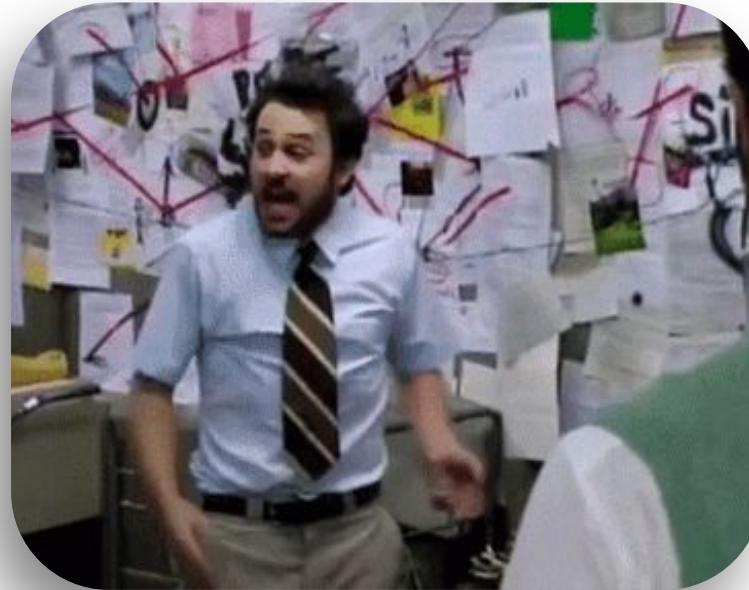


Regulations & Ethics

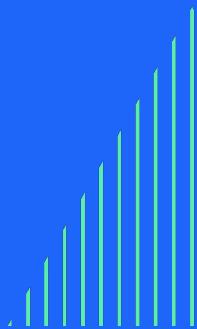
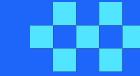
- Compliance Standards
- Security Policies



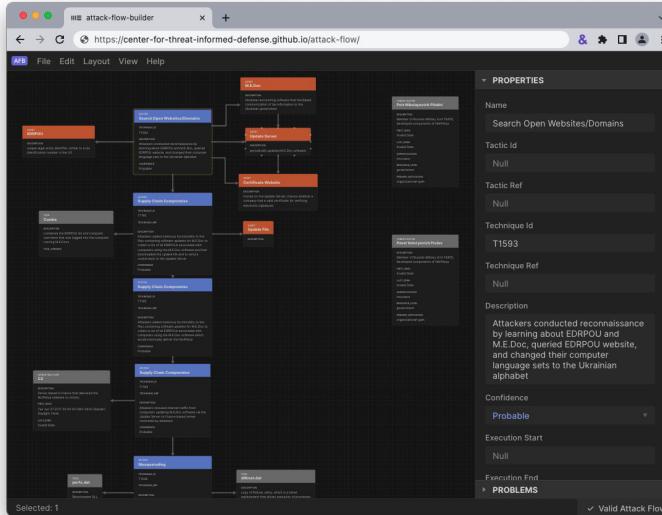
Attack Flow



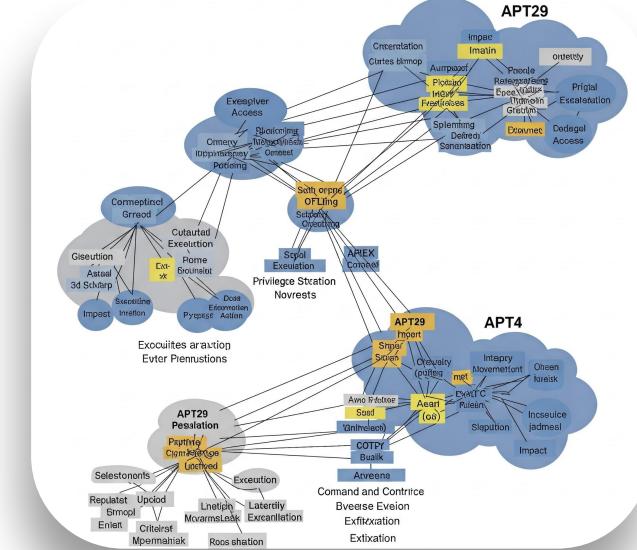
- Powerful concept for a unified cyber framework
- Not just a threat, but a narrative: the how, why, and what.
- They make knowledge usable



Attack Graph vs. MITRE ATT&CK Flow



MITRE | ATT&CK®





NOW WHAT?





State of The Art

- [1] P. Armann, D. Wijesekera and S. Kaushik, "Scalable, Graph-Based Network Vulnerability Analysis," *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 217–224. [Online]. Available: https://www.researchgate.net/publication/3948684_Automated_Generation_and_Analysis_of_Attack_Graphs.
- [2] A. Husari, C. N. Gutierrez, N. Harang and S. Chellappa, "TTPDrill: Automatic and Accurate Extraction of Threat Actions from Unstructured Text of CTI Sources," *Proceedings of the 2017 ACM Workshop on Artificial Intelligence and Security (AISec '17)*, 2017, pp. 59–69. [Online]. Available: <https://dl.acm.org/doi/abs/10.1145/3134600.3134646>.
- [3] N. Soman, "Death to the IOC: What's Next in Threat Intelligence," *Black Hat USA 2019*, [Video and Slides]. [Online]. Available: <https://www.youtube.com/watch?v=MJHSUsS9k7s> and <https://i.blackhat.com/USA-19/Thursday/us-19-Soman-Death-To-The-IOC-Whats-Next-In-Threat-Intelligence.pdf>.
- [4] S. Mittal, A. Joshi and A. Finin, "TIMiner: TTP-based Cyber Threat Intelligence Summarization from Unstructured Text," *Computers & Security*, vol. 96, 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/abs/pii/S0167404820301395>.
- [5] V. Legoy, *rcATT: Mapping Unstructured Cyber Threat Intelligence Reports to the MITRE ATT&CK Framework Using Machine Learning*, Master's Thesis, University of Amsterdam, 2020. [Online]. Available: https://github.com/vlegoy/rcATT/blob/master/MScThesis_rcATT_VLegooy.pdf.
- [6] MITRE Corporation, "Threat Report ATT&CK Mapper (TRAM)," [Online]. Available: <https://ctid.mitre.org/projects/threat-report-attack-mapper-tram>.
- [7] S. Joshi, A. Mittal and A. Joshi, "EXTRACTOR: Extracting Attack Behavior from Threat Reports," *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, Vienna, Austria, 2021, pp. 207–221. [Online]. Available: <https://ieeexplore.ieee.org/document/9581182/>.
- [8] B. Zhang et al., "Looking Beyond IoCs: Automatically Extracting Attack Patterns from External CTI," *arXiv preprint arXiv:2211.01753*, 2022. [Online]. Available: <https://arxiv.org/pdf/2211.01753.pdf>.
- [9] A. Wahab et al., "CTINEXUS: A Framework for Scalable CTI Knowledge Graph Generation with LLM-Augmented Mapping to ATT&CK," *arXiv preprint arXiv:2410.21060*, 2024. [Online]. Available: <https://arxiv.org/pdf/2410.21060.pdf>.
- [10] Y. Liu, "Threats To MITRE(CWD, ATT&CK) AI-LLM Mapper," GitHub Repository, 2024. [Online]. Available: https://github.com/LiuYuancheng/Threats_2_MITRE_AI_Mapper.
- [11] B. Zhang et al., "AttackSeqBench: Benchmarking Sequential Threat Behavior Generation from Large Language Models," *arXiv preprint arXiv:2503.03170*, 2025. [Online]. Available: <https://arxiv.org/pdf/2503.03170v1.pdf>.

- TTPs extraction from text
- Not designed for unstructured text
- Cannot directly parse natural language narratives to extract attack steps or TTPs
- Achieving automation for its input type.
- Limited Training Data and Pattern Recognition
- Lack of Contextual Understanding
- IOC focused
- Traditional ML's attack flow accuracy is limited by its finite labeled data, while LLMs leverage vast knowledge to generate more diverse, novel, and contextually coherent scenarios.
- Automatic and Accurate Extraction of Threat Actions from Unstructured Text of CTI Sources Relies on fixed grammatical patterns (SVOI)
- Limited in capturing semantic nuance, context beyond sentence level, and implicit relationships
- Less adaptable to new or unseen attack descriptions.

DAQ



Feeds



Docs
Storage



Extract

Nearly 400 data feeds are currently being monitored.

NER



Labelling



Classifying

Accurate labeling is essential for effective document classification.

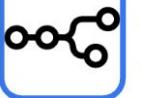
RAG+

Vector
Search



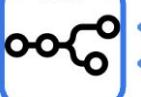
Docs
Related

n8n



LLM
Model

n8n



LLM
Model



Storage

Each candidate document will retrieve *four* additional related documents from the document storage. This enables the system to process documents that were not initially selected as candidates.

OUTPUT

MITRE | ATT&CK®



Attack Flow



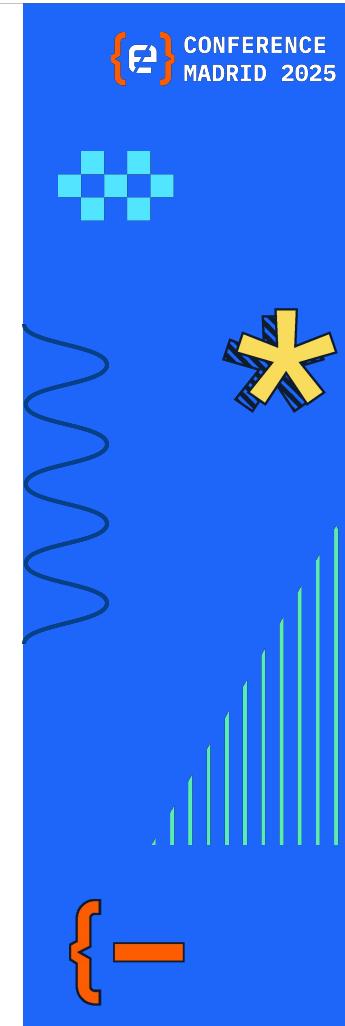
Knowledge
Database

The system will generate an attack flow database compliant with the MITRE ATT&CK Flow standard

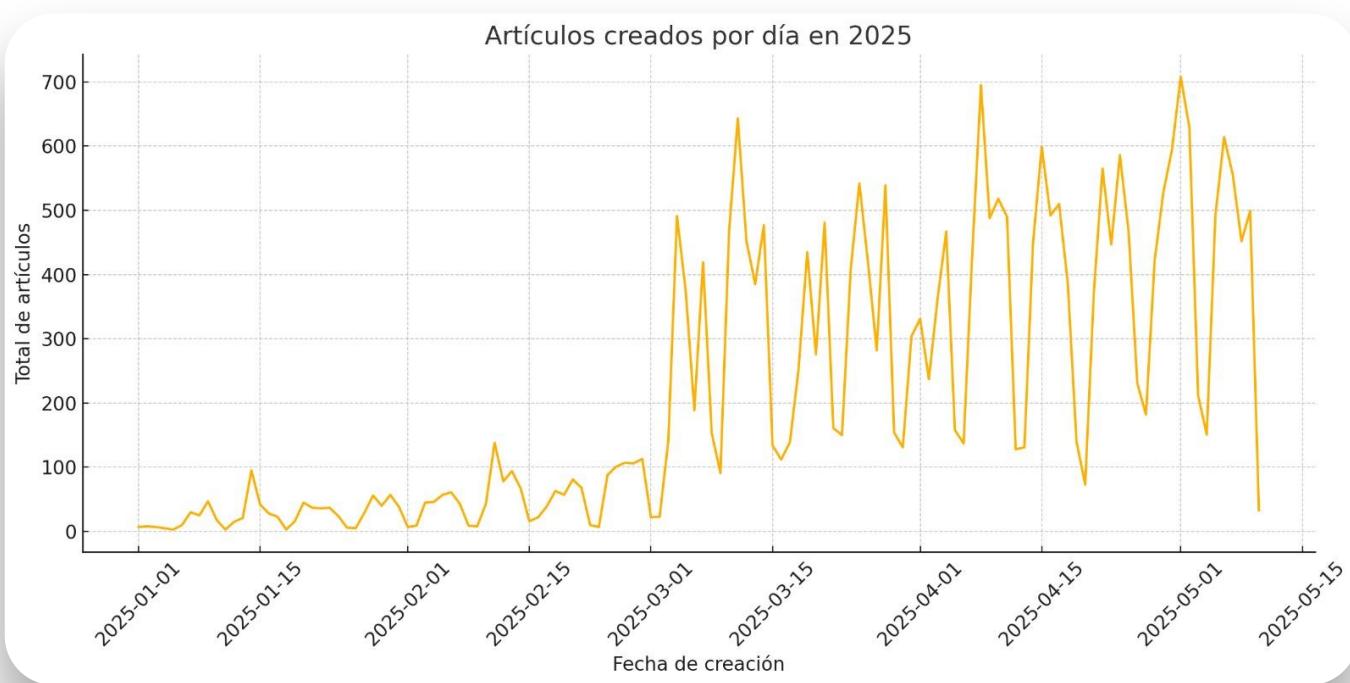
USE CASES



SIEM



Data Acquisition (DAQ): Article Volume



400 new documents per day from almost 400 feeds

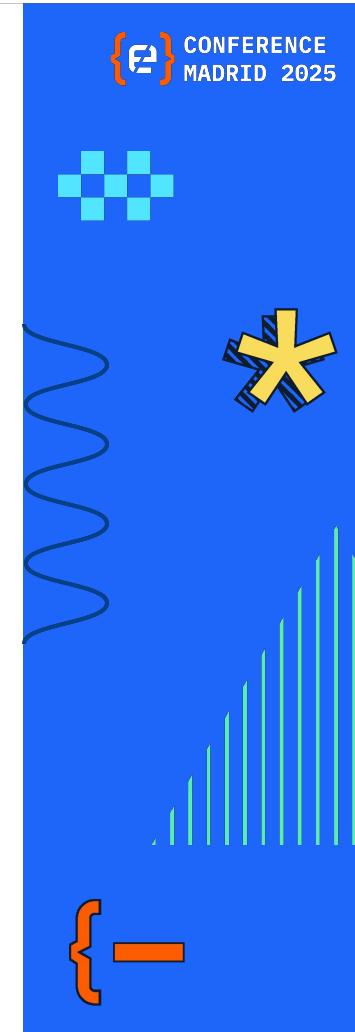
Data Acquisition (DAQ): RSS Feed

```
-zsh — 179x54

This XML file does not appear to have any style information associated with it. The document tree is shown below.

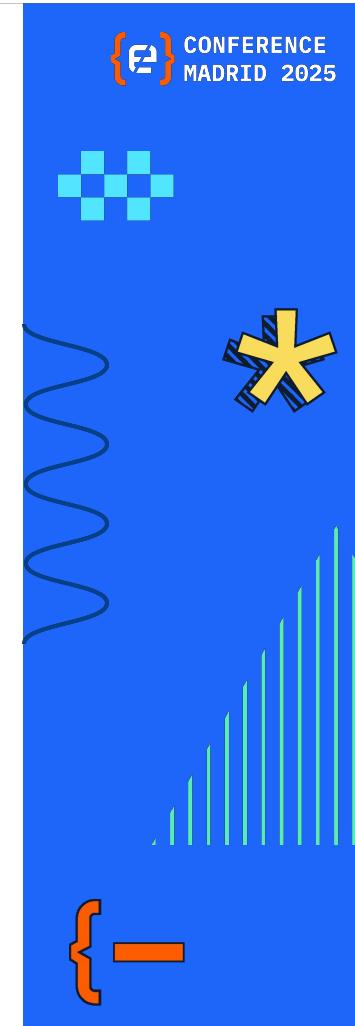
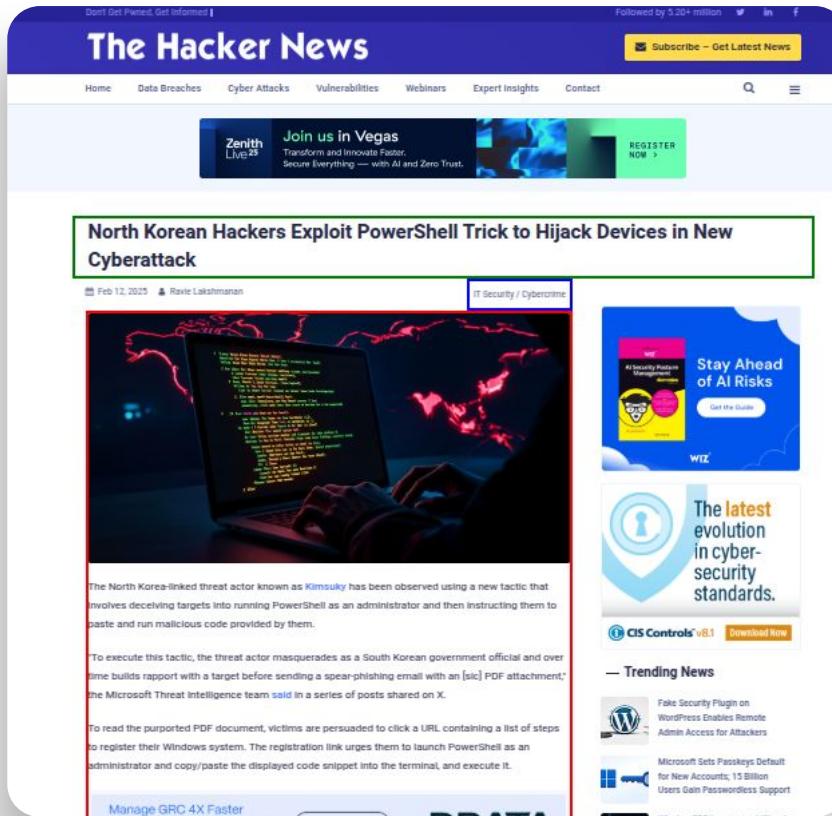
<rss xmlns:atom="http://www.w3.org/2005/Atom" xmlns:content="http://purl.org/rss/1.0/modules/content/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:itunes="http://www.itunes.com/dtds/podcast-1.0.dtd" xmlns:media="http://search.yahoo.com/mrss/" xmlns:stash="http://purl.org/rss/1.0/modules/stash/" xmlns:sy="http://purl.org/rss/1.0/modules/syndication/" xmlns:wf="http://wellformedweb.org/CommentAPI/" version="2.0">
  <channel>
    <title>The Hacker News</title>
    <link>https://thehackernews.com</link>
    <description>Most trusted, widely-read independent cybersecurity news source for everyone; supported by hackers and IT professionals – Send TIPS to authors@thehackernews.com</description>
    <language>en-us</language>
    <lastBuildDate>Fri, 16 May 2025 10:17:34 +0530</lastBuildDate>
    <sy:updatePeriod>hourly</sy:updatePeriod>
    <sy:updateFrequency>1</sy:updateFrequency>
    <atom:link href="https://feeds.feedburner.com/TheHackersNews" rel="self" type="application/rss+xml"/>
  <item>
    <title>Meta to Train AI on E.U. User Data From May 27 Without Consent; Noyb Threatens Lawsuit</title>
    <description>
      <![CDATA[ Austrian privacy non-profit noyb (none of your business) has sent Meta's Irish headquarters a cease-and-desist letter, threatening the company with a class action lawsuit if it proceeds with its plans to train users' data for training its artificial intelligence (AI) models without an explicit opt-in. The move comes weeks after the social media behemoth announced its plans to train its AI models ]]>
    </description>
    <link>https://thehackernews.com/2025/05/meta-to-train-ai-on-eu-user-data-from.html</link>
    <guid isPermaLink="false">https://thehackernews.com/2025/05/meta-to-train-ai-on-eu-user-data-from.html</guid>
    <pubDate>Thu, 15 May 2025 22:15:00 +0530</pubDate>
    <author>info@thehackernews.com (The Hacker News)</author>
    <enclosure length="122216320" type="image/jpeg"
      url="https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjNDV7RaWyoIolFm4g_uLvp282bNtKla2q0k3pBerDV-6vvGffgbodS7o_ZH_Tw7T-Lyx5YbhWRM7Gly549NM7A0hqLxgY9f5tAKbanZx51j1_uoPlm4Bj3um69JfcU4e0x6U7wVnU9cbt2Dfop02BzNxp4QfdobvjaZ_N-b5WfdH3R0JU020p/v/s1600/meta-ai.jpg"/>
  </item>
  <item>
    <title>Coinbase Agents Bribed, Data of ~1% Users Leaked; $20M Extortion Attempt Fails</title>
    <description>
      <![CDATA[ Cryptocurrency exchange Coinbase has disclosed that unknown cyber actors broke into its systems and stole account data for a small subset of its customers. "Criminals targeted our customer support agents overseas," the company said in a statement. "They used cash offers to convince a small group of insiders to copy data in our customer support tools for less than 1% of Coinbase monthly ]]>
    </description>
    <link>https://thehackernews.com/2025/05/coinbase-agents-bribed-data-of-1-users.html</link>
    <guid isPermaLink="false">https://thehackernews.com/2025/05/coinbase-agents-bribed-data-of-1-users.html</guid>
    <pubDate>Thu, 15 May 2025 19:58:00 +0530</pubDate>
    <author>info@thehackernews.com (The Hacker News)</author>
    <enclosure length="122216320" type="image/jpeg"
      url="https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi4Ek9oIDyD8BvB7yeUZ2uDox1AVdtB9p9si2bnY-A04ZgGezyCK5SeGy568cjDz0Ywb-rrnpJiccc2ISGgpb0CMU0jsEOw1QNm7XHXYPuMjdCh-6qDVnAd-arishLdPaN4202h7ooo3Tdq_sUoM9RtBthM3l4hc0s7uxKLjQjmE51w5xE-Z/s1600/coinbase.jpg"/>
  </item>
  <item>
    <title>Pen Testing for Compliance Only? It's Time to Change Your Approach</title>
    <description>
      <![CDATA[ Imagine this: Your organization completed its annual penetration test in January, earning high marks for security compliance. In February, your development team deployed a routine software update. By April, attackers had already exploited a vulnerability introduced in that February update, gaining access to customer data weeks before being finally detected. This situation isn't theoretical: it ]]>
    </description>
  </item>
</channel>
</rss>
```

We pull in RSS feeds—glitches and occasional issues like embedded code—to keep our cybersecurity info fresh.

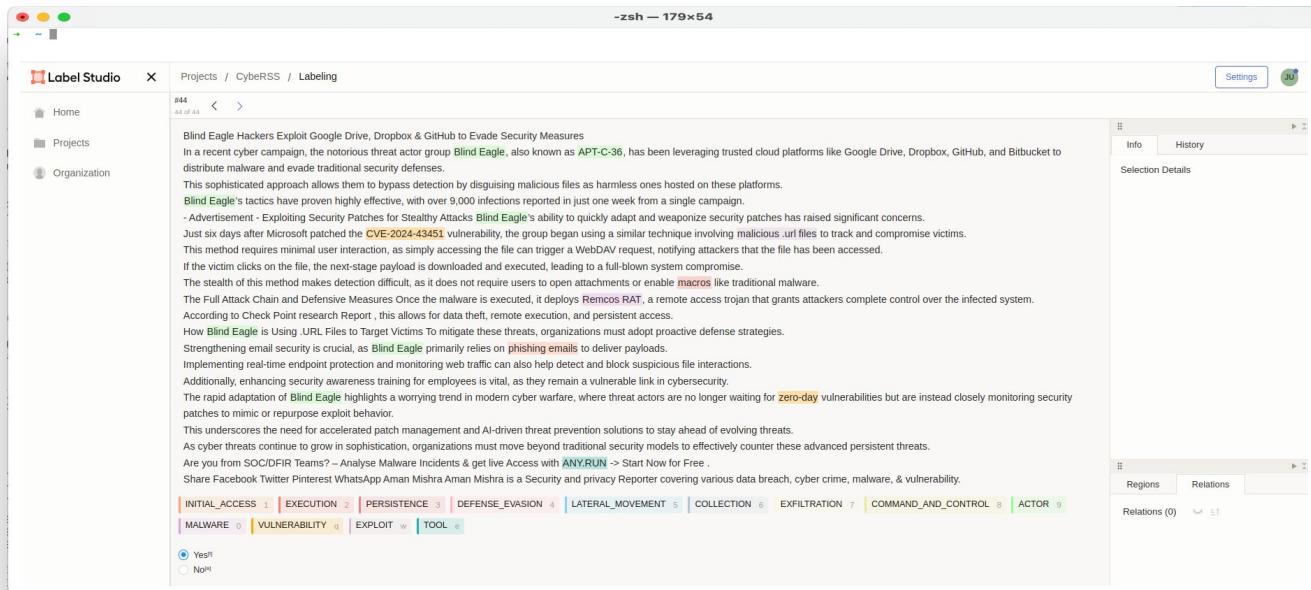


Turning Raw Content into Clean Input

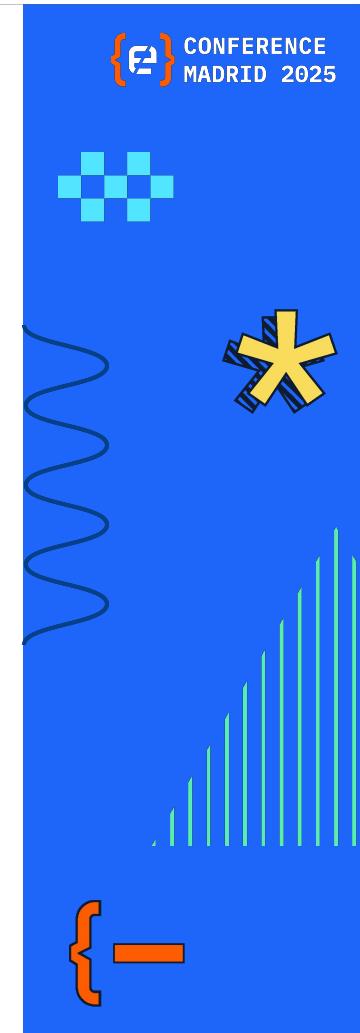
- Extract main content (remove menus, ads, etc.)
- spaCy + NLP models
- Output: clean, structured text ready for analysis



Automatic Structured Annotation



- Using **Label Studio** for automatic entity annotation in CTI texts
- Integrated with models to suggest tags automatically
- Custom NER model detects: **actors**, **vulnerabilities**, **tactics**, **tools**, etc.
- We only need to review the entities suggested by the model



From Text Input to Ranked Results

This post might ring a bell—it changed the game by showing how to represent words as vectors and even do meaningful math with them.

81v3 [cs.CL] 7 Sep 2013

Efficient Estimation of Word Representations in Vector Space

Tomas Mikolov

Google Inc., Mountain View, CA
tmikolov@google.com

Kai Chen

Google Inc., Mountain View, CA
kaichen@google.com

Greg Corrado

Google Inc., Mountain View, CA
gcorrado@google.com

Jeffrey Dean

Google Inc., Mountain View, CA
jeff@google.com

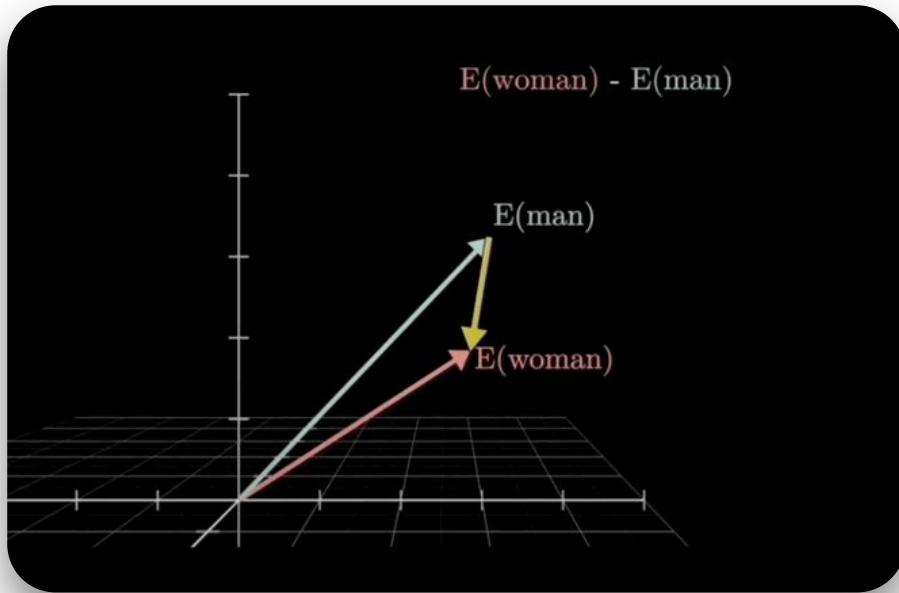
Abstract

We propose two novel model architectures for computing continuous vector representations of words from very large data sets. The quality of these representations is measured in a word similarity task, and the results are compared to the previously best performing techniques based on different types of neural networks. We observe large improvements in accuracy at much lower computational cost, i.e. it takes less than a day to learn high quality word vectors from a 1.6 billion words data set. Furthermore, we show that these vectors provide state-of-the-art performance on our test set for measuring syntactic and semantic word similarities.

<https://arxiv.org/pdf/1301.3781>



From Text Input to Ranked Results



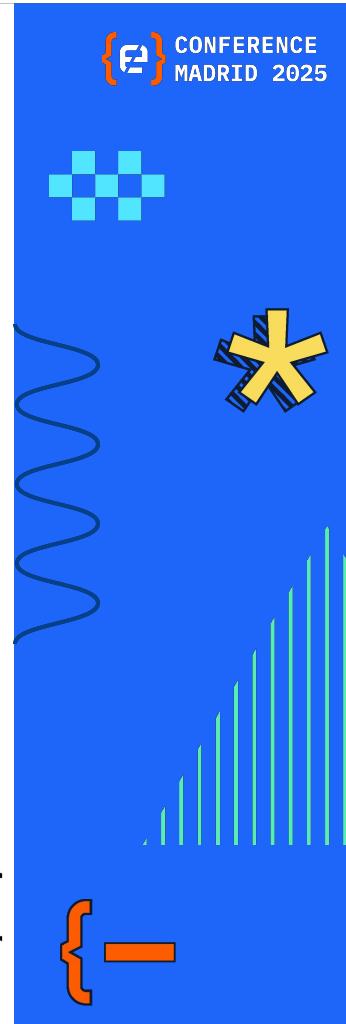
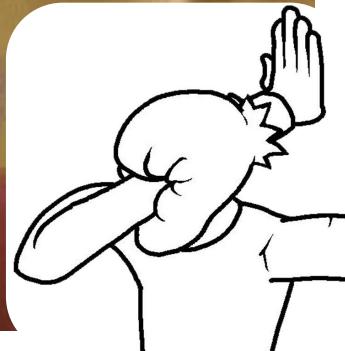
Word2Vec models capture word meanings with math—like how king - man + woman gets you close to queen—revealing not just meanings, but also cultural, geographic, even foodie associations.

From Text Input to Ranked Results

Table 8: Examples of the word pair relationships, using the best word vectors from Table 4 (Skip-gram model trained on 783M words with 300 dimensionality).

Relationship	Example 1	Example 2	Example 3
France - Paris	Italy: Rome	Japan: Tokyo	Florida: Tallahassee
big - bigger	small: larger	cold: colder	quick: quicker
Miami - Florida	Baltimore: Maryland	Dallas: Texas	Kona: Hawaii
Einstein - scientist	Messi: midfielder	Mozart: violinist	Picasso: painter
Sarkozy - France	Berlusconi: Italy	Merkel: Germany	Koizumi: Japan
copper - Cu	zinc: Zn	gold: Au	uranium: plutonium
Berlusconi - Silvio	Sarkozy: Nicolas	Putin: Medvedev	Obama: Barack
Microsoft - Windows	Google: Android	IBM: Linux	Apple: iPhone
Microsoft - Ballmer	Google: Yahoo	IBM: McNealy	Apple: Jobs
Japan - sushi	Germany: bratwurst	France: tapas	USA: pizza

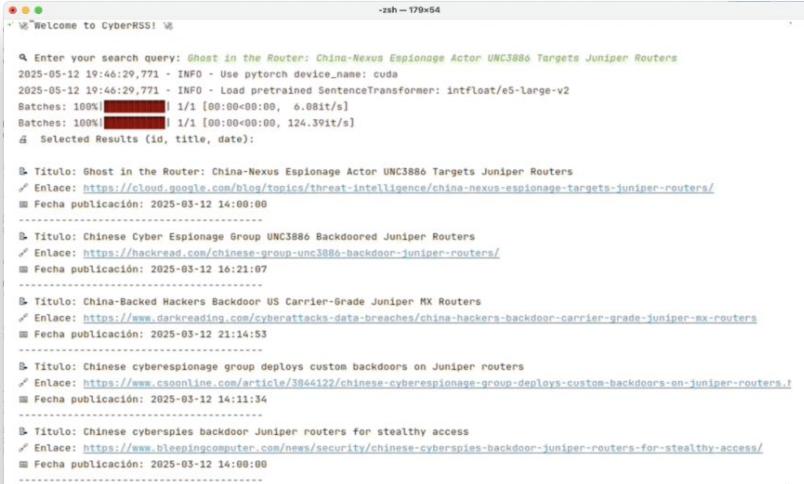
IBM: Linux	Ap
IBM: McNealy	A
France: tapas	U



From Text Input to Ranked Results

It lets us compare texts by meaning, not just matching words—helping us rank articles, spot similarities.

Here, the system turns a headline into a vector and finds semantically similar articles, even if they use different words or angles.



```
-zsh - 179x64

· ⓘ Welcome to CyberRSS! ⓘ

 ⓘ Enter your search query: Ghost in the Router: China-Nexus Espionage Actor UNC3886 Targets Juniper Routers
2025-05-12 19:46:29,771 - INFO - Use pytorch device_name: cuda
2025-05-12 19:46:29,771 - INFO - Load pretrained SentenceTransformer: intfloat/e5-large-v2
Batches: 100% [██████████] 1/1 [00:00<00:00, 6.08bit/s]
Batches: 100% [██████████] 1/1 [00:00<00:00, 124.39it/s]
d Selected Results (id, title, date):
-----
↳ Titulo: Ghost in the Router: China-Nexus Espionage Actor UNC3886 Targets Juniper Routers
↗ Enlace: https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-targets-juniper-routers/
🕒 Fecha publicación: 2025-03-12 14:00:00
-----
↳ Titulo: Chinese Cyber Espionage Group UNC3886 Backdoored Juniper Routers
↗ Enlace: https://hackread.com/chinese-group-unc3886-backdoor-juniper-routers/
🕒 Fecha publicación: 2025-03-12 16:21:07
-----
↳ Titulo: China-Backed Hackers Backdoor US Carrier-Grade Juniper MX Routers
↗ Enlace: https://www.darkreading.com/cyberattacks-data-breaches/china-hackers-backdoor-carrier-grade-juniper-mx-routers
🕒 Fecha publicación: 2025-03-12 21:14:53
-----
↳ Titulo: Chinese cyberespionage group deploys custom backdoors on Juniper routers
↗ Enlace: https://www.csoconline.com/article/3844122/chinese-cyberespionage-group-deploys-custom-backdoors-on-juniper-routers\_1
🕒 Fecha publicación: 2025-03-12 14:11:34
-----
↳ Titulo: Chinese cyberspies backdoor Juniper routers for stealthy access
↗ Enlace: https://www.bleepingcomputer.com/news/security/chinese-cyberspies-backdoor-juniper-routers-for-stealthy-access/
🕒 Fecha publicación: 2025-03-12 14:00:00
```



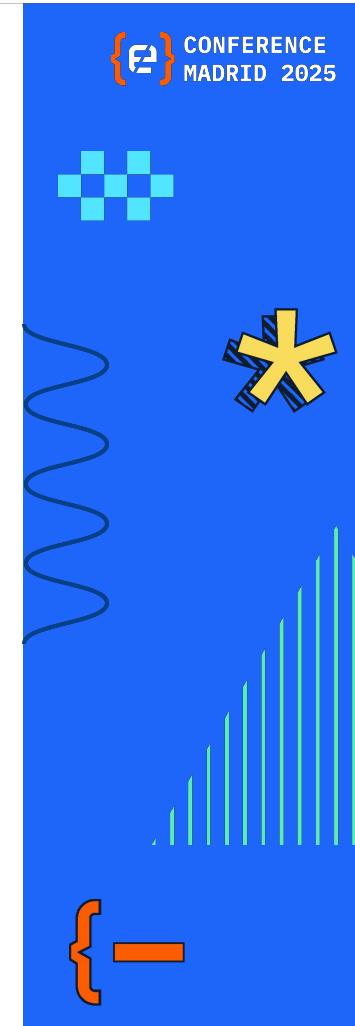
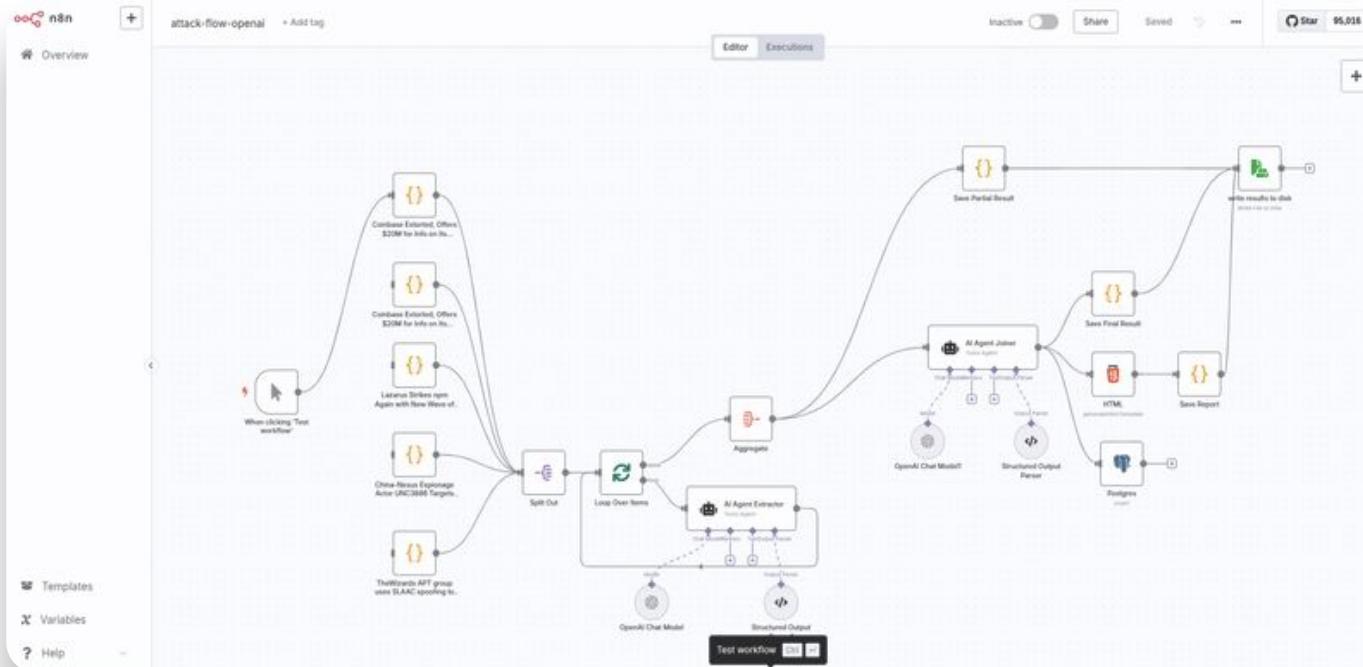
Comparing Embedding Models (MTEB Leaderboard)

Rank	Model	Model Size (GB)	Embedding Dimensions	Max Tokens	Average (56 datasets)	Classification Average (12 datasets)	Clustering Average (11 datasets)	Pair Classification Average (3 datasets)	Retraining Average (4 datasets)	Summary
1	SFT-Embedding-Mistral	14.22	4096	32768	67.56	78.33	51.67	88.54	69.64	59
2	voyage-lite-02-instruct		1024	4096	67.13	79.25	52.42	86.87	58.24	56.6
3	GritiLM-7B	14.48	4096	32768	66.76	79.46	50.61	87.16	60.49	57.41
4	e5-mistral-7b-instruct	14.22	4096	32768	66.63	78.47	50.26	88.34	60.21	56.89
5	GritiLM-8x7B	93.41	4096	32768	65.66	78.53	50.14	84.97	59.8	55.89
6	echo-mistral-7b-instruct-last	14.22	4096	32768	64.68	77.43	46.32	87.34	58.14	55.52
7	mxbai-embed-large-v1	0.67	1024	512	64.68	75.64	46.71	87.2	60.11	54.39
8	UAE-Large-V1	1.34	1024	512	64.64	75.58	46.73	87.25	59.88	54.66
9	text-embedding-3-large		3072	8192	64.59	75.45	49.01	85.72	59.16	55.44
10	voyage-lite-01-instruct		1024	4096	64.49	74.79	47.4	86.57	59.74	55.58
11	Cochere-embed-english-v3.0		1024	512	64.47	76.49	47.43	85.84	58.01	55
12	multilingual-e5-large-instruc	1.12	1024	512	64.41	77.56	47.1	86.19	58.58	52.47

<https://huggingface.co/spaces/mteb/leaderboard>

Benchmarks show models like e5-large and bge excel at semantic search—just what we need to organize and enrich articles.

From article content to structured attack flow



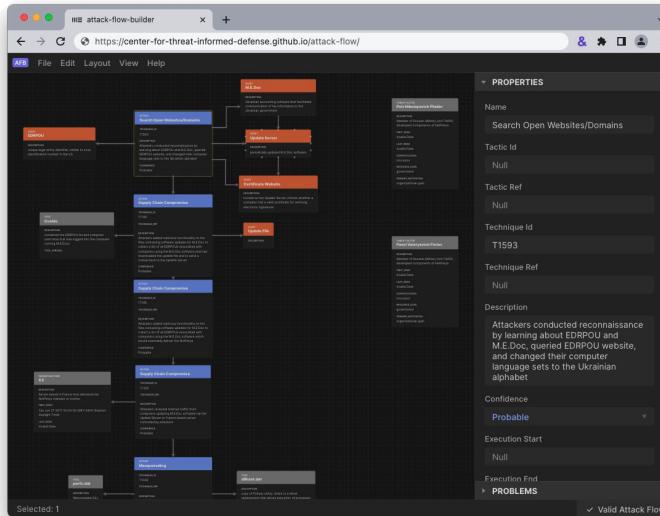
Constructing the Attack Flow

UNC3886 Chinese APT Group Installs Custom Backdoors on Juniper Routers for Persistent Espionage

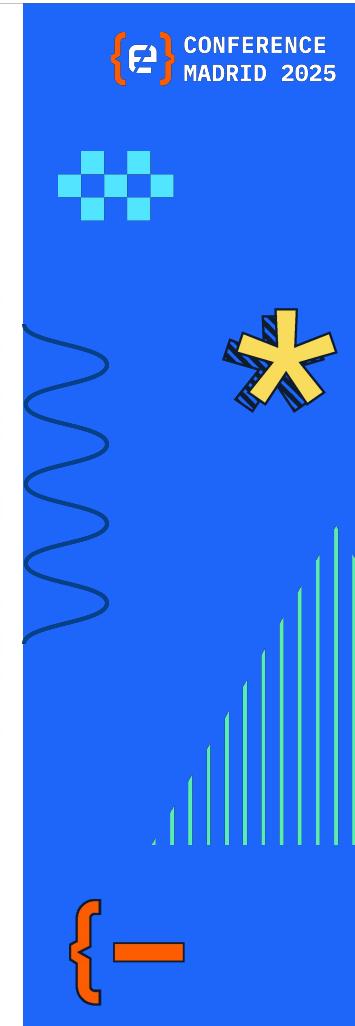
PUBLISHED: 12/03/2025
CATEGORY: APT
SUMMARY: Chinese APT UNC3886 compromised Juniper routers since 2024, using custom backdoors to maintain persistent espionage access to defense, telecom, and ISP networks.

Actor
Actor: UNC3886
Aliases: China-nexus threat group | APT41 (tooling overlap) | UNC3886
Origin: China
Motivation: Cyber espionage targeting defense, technology, telecommunications, and ISPs via persistent access to network devices.
Discovered by: Mandiant

Target Profile
Victim Organizations:
• Juniper Networks



Attack Flow <https://ctid.mitre.org/projects/attack-flow>



Use Cases

What are the potential uses for the knowledge produced?

- Threat Detection & Alert Tuning
- Threat Hunting
- Incident Response & Root Cause Analysis
- Security Content Validation & Adversary Emulation
- SOC Playbook Automation & Enrichment
- Threat Intelligence Enrichment
- AI/ML Model Training for Detection

Use Case	Challenge Addressed	How an Attack Flow Database Helps	Real Life
Threat Detection & Alert Tuning	High alert volume, false positives	Matches alerts with known malicious sequences to prioritize true positives	Triage Re-Rank, Attack Pattern.
Threat Hunting	Lacks context for proactive searches	Provides hypothesis-driven paths based on known TTP sequences. Present and Past.	Hunting for post-exploitation actions. Rollback through known attack flows
Incident Response & Root Cause Analysis	Hard to reconstruct multi-stage attacks	Maps observed evidence to known flows, accelerating investigation	Mapping events to Hafnium attack flow to identify initial access method
Security Content Validation & Adversary Emulation	In some cases detections could fail to detect multi-stage attacks and Simulations are too generic	Simulates real attacks to validate security control effectiveness. Enables red teams to emulate real-world attack chains; helps blue teams test detection/response	Combine with Attack Simulation Solutions
SOC Playbook Automation & Enrichment	Playbooks lack context	Enhances playbooks with dynamic branches based on attack stage and context	Improve Automatic Case Creation and allow for Threat Hunting
Threat Intel & Enrichment	IOCs lack context	Places indicators and TTPs within a larger narrative for better relevance	Context for OSINT/OSTI IOCs
Model Training for Detection	Models need labeled, high-fidelity attack data	Supplies curated attack sequences to train and validate machine learning detection models	Using known flows to build a labeled dataset for behavioral anomaly detection models



Alert Triage Re-Rank

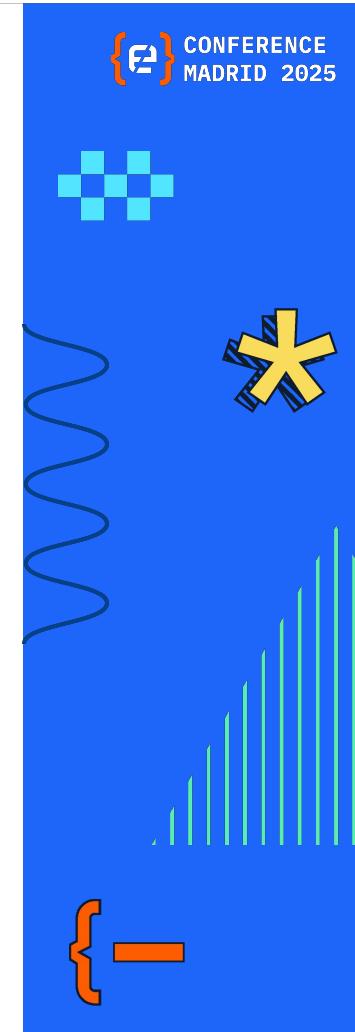
Threat Detection & Alert Tuning

Matches alerts
High alert volume, false positives **with known malicious sequences to prioritize true positives** **Triage Re-Rank, Attack Pattern.**

0 New triggered alerts  Load new since last update

Advanced filter 

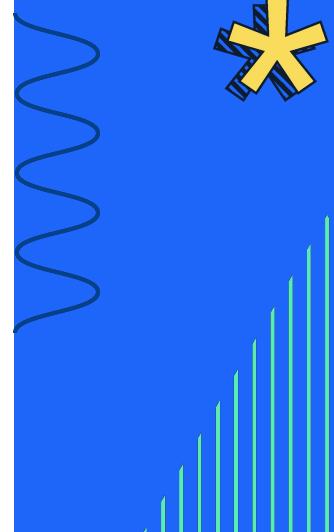
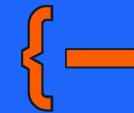
Name	ID	Status
SecOpsWinAdminRemoteLogon	355661767	Unread
SecOpsLinuxMaxSessionsPerUser	355632406	Unread
SecOpsAzureUserLoginSuspiciousRisk	355623215	Unread
SecOpsAzureUserLoginSuspiciousRisk	355623213	Unread
SecOpsAzureUserLoginSuspiciousRisk	355623212	Unread
SecOpsAzureUserLoginSuspiciousRisk	355617314	Unread
SecOpsAzureUserLoginSuspiciousRisk	355617313	Unread
SecOpsAzureUserLoginSuspiciousRisk	355617312	Unread
SecOpsHighVolumeFileDeletion	354964978	Unread
SecOpsPotentialThreatConnectionRansomBe...	354954505	Unread
SecOpsPotentialThreatConnectionRansomBe...	354954504	Unread
SecOpsPotentialThreatConnectionRansomBe...	354954503	Unread
SecOpsPotentialThreatConnectionRansomBe...	354954502	Unread
SecOpsPotentialThreatConnectionRansomBe...	354954501	Unread



SOC Automation & Enrichment

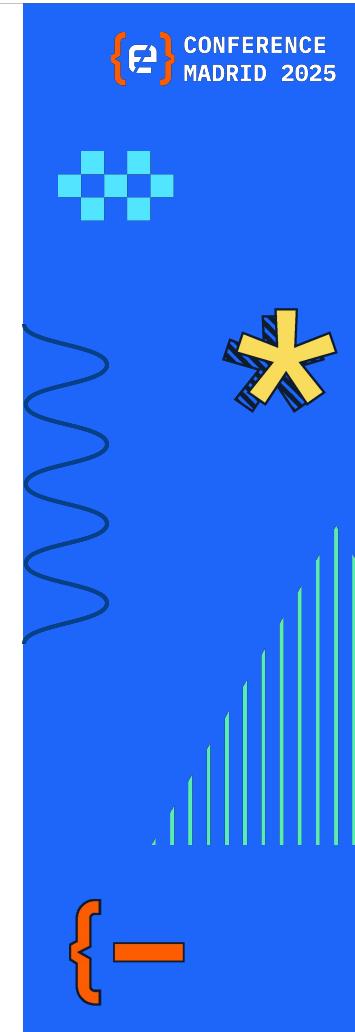
SOC Playbook Automation & Enrichment	Playbooks lack context	Enhances playbooks with dynamic branches based on attack stage and context	Improve Automatic Case Creation and allow for Threat Hunting
--------------------------------------	------------------------	--	--

MITRE | ATT&CK®
Technique Inference Engine
Given a list of observed techniques, infer the next most likely techniques.



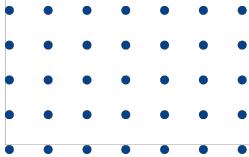
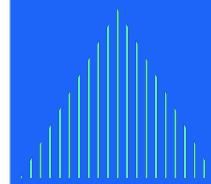
Threat Hunting

Threat Hunting	Lacks context for proactive searches	Provides hypothesis-driven paths based on known TTP sequences. Present and Past.	Hunting for post-exploitation actions. Rollback through known attack flows
----------------	--------------------------------------	--	--





Fails & Future



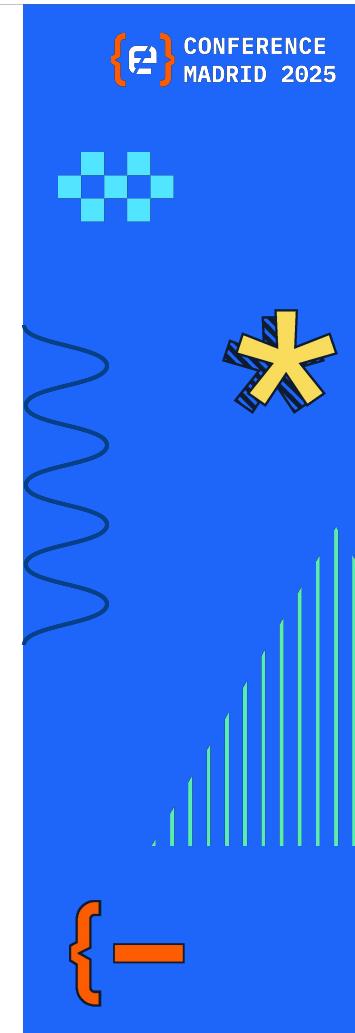
All that glitters is not gold

- Ads
- Vulnerability advisory lack of details

Named Entity Recognition (NER)

Future Uses

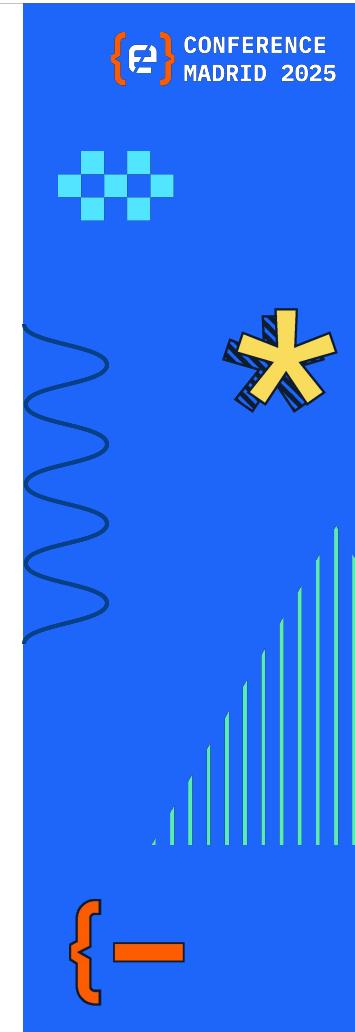
- Automatically filter content based on detected entities
- Enrich the database with structured information
- Automatically map content to **MITRE ATT&CK** tactics and techniques
- Generate training datasets for new models
- Improve prompts



DAQ & SELF-IMPROVEMENT

Future Improvements

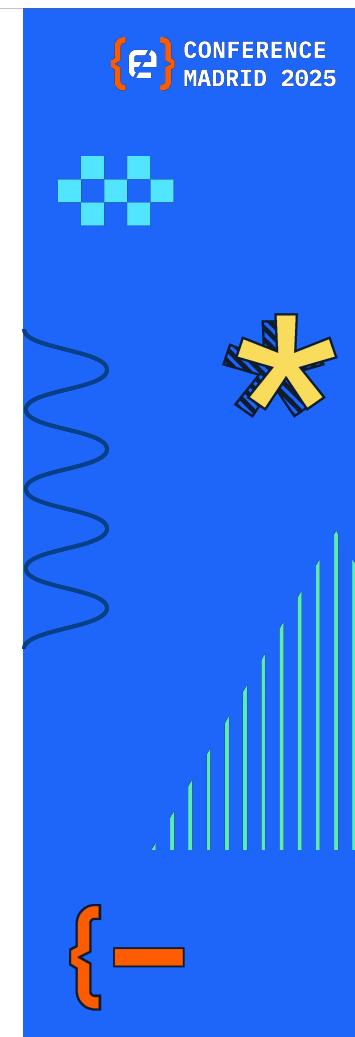
- Result validation
- Auto-discovery of feeds
- Feed ranker and new acquisition
- Attack Pattern prediction



Production Ready

Future Improvements

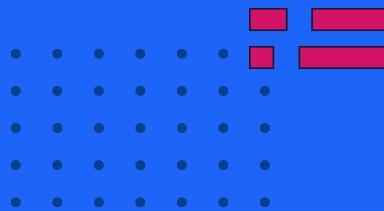
- UI + API
- Self deployment





{codemotion} CONFERENCE MADRID 2025

Don't forget to
rate the talk!





{codemotion} CONFERENCE MADRID 2025

Thanks!

