

TARANIS AI

Pioneering AI-Driven OSINT

 taranis.ai  [taranis-ai/taranis-ai](https://github.com/taranis-ai/taranis-ai)

What is OSINT?

Open-Source Intelligence (OSINT) refers to the collection and analysis of publicly available information for intelligence purposes.

- Derived from publicly accessible sources (news, social media, forums)
- Common in cybersecurity, journalism, and threat intelligence
- Challenges: data volume, signal-to-noise ratio, source validation

The Analyst Bottleneck

*Thousands of alerts.
Duplicate news articles.
One human analyst.*

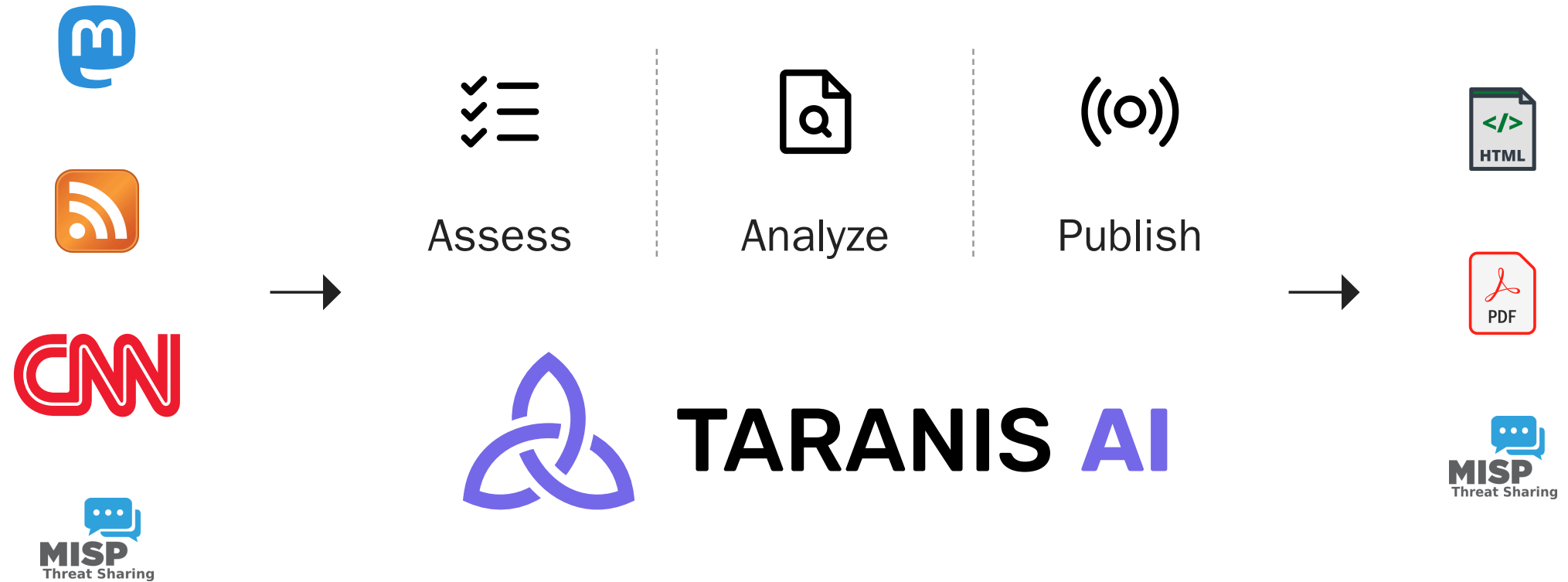
"Do we care about this threat?"

"Have we seen this before?"

"Where did this story originate from?"

Taranis Workflow

Inspired by Taranis3 & Taranis-NG



Features



Named Entity Recognition

Extracts information about people, organizations, locations, etc. from free-form text.



Topic Clustering

Uses topic modelling to find related news items.



Collaboration

Integrates with MISP to streamline threat intelligence collaboration.



Contextual Enrichment

Leverages NLP for automatic creation of summaries and sentiment analysis or Threat Classification

Named Entity Recognition

Lists and Regex - CVEs, APT Groups, Hashes

NER - Person, Location, Organization, Product, Event

Context and source-specific models (IT security or general news)

Published: 2024-10-25 22:22

2024-10-29 14:24

Tags:

Russia-linkedAndroidUkraine'sMeduzaStealerPureStealerUNC5812'sRussia'sTelegramRussian-linkedRussiaSuns spinnerCraxsRATpro-RussianUNC5812UkrainianVisual Basic Script-basedHOMESTEELClickFix-stylePowerShutWindows: CERT-UA

Vote:

00

Article: [darkreading.com](#)

Angreifer nutzten gefälschte AWS-Domains in Phishingkampagne

Angreifer nutzten gefälschte AWS-Domains in Phishingkampagne

AWS hat offenbar zahlreiche gefälschte AWS-Domains vom Netz genommen, die ukrainische Opfer auf Malware-Downloadseiten locken sollten.

- Kathrin Stoll

Sicherheitsforscher des AWS Security Team haben eine Phishing-Kampagne gestoppt, bei der tausende gefälschte AWS-Domains genutzt wurden. Amazon hat seit der Entdeckung der Kampagne massenweise Domains abgeschaltet. Die AWS-Sicherheitsforscher und das Computer Emergency Response Team der Uk ukrainischsprachigen Zielen zu erbeuten.

Ukrainische Ziele im Visier

Die gefälschten AWS-URLs dienten offenbar als Köder. Nachdem die Opfer auf den Link einer solchen URL geklickt hatten, landeten sie auf einer Malware-Downloadseite, die einen sogenannten RDP-Trojaner installiert, der Anmeldedaten von Windows-Systemen stiehlt.

Amazons Chief Information Security Officer CJ Moses schrieb in einem Posting auf LinkedIn, dass Amazon selbst nicht im Visier der Angreifer war. Auch zielten die Angriffe nicht auf Anmeldedaten von AWS-Kunden ab. Stattdessen hatten die Angreifer Ziele mit Verbindungen zu Regierungsbehörden, Unternehmen und enger gefassten Ansatz – dieses Mal seien die Phishingmails an viele Ziele verschickt worden.

Das ukrainische CERT hat ein Advisory mit weiteren Details zu dem Fall veröffentlicht. Cybercrime spielt im Krieg Russlands gegen die Ukraine auf beiden Seiten eine Rolle. Im Juni etwa machten die ukrainischen Behörden Personen dingfest, die sie der Cyberkriminalität verdächtigten, die mutmaßlich im Dienst russisch (kst)

Published: Oct 28, 2024, 21:22:45

Article: [darkreading.com](#)

Author: Becky Bracken, Senior Editor, Dark Reading

Russia Kneecaps Ukraine Army Recruitment With Spoofed 'Civil Defense' App

Russia Kneecaps Ukraine Army Recruitment With Spoofed 'Civil Defense' App

Posing as an application used to locate Ukrainian military recruiters, a Kremlin-backed hacking initiative delivers malware, along with disinformation designed to undermine sign-ups for soldiers in the war against Russia.

October 28, 2024

Ukrainian efforts to recruit new soldiers to serve in its military in the country's war against Russia is under a two-pronged cyberattack by Kremlin-backed threat actors.

Researchers at Google's Threat Intelligence Group (TAG) and Mandiant have tracked down an active campaign that uses a spoofed version of the legitimate Ukrainian-language tool "Civil Defense," a crowdsourced mapping tool used to locate military recruiters. Attackers are using the fake version to perform dual malice The hybrid op, which researchers named UNC5812, uses a Telegram channel to lure perspective recruits to a download the malicious version of "Civil Defense" from a spoofed site, outside of the confines of Google Play. Once downloaded, the application drops Windows and Android malware.

Russian Opp Uses Malware With a Side of Social Engineering

Windows users who make their way to the fake "Civil Defense" site to download the tool will be delivered the Pronsis Loader, which then starts a chain to deliver a malicious mapping application called Sunspinner, as well as an infostealer called Purestealer.

Android users, on the other hand, get a common user backdoor called Craxsrat, in addition to Sunspinner.

"Notably, the Civil Defense website also contains an unconventional form of social engineering designed to preempt user suspicions about APK delivery outside of the App Store and justify the extensive permissions required for the Craxsrat installation," the report noted. "The website's FAQ contains a strained justification accompanying video instructions."

The video also provides instructions on how to disable Google Play Protect.

"While the Civil Defense website also advertises support for macOS and iPhones, only Windows and Android payloads were available at the time of analysis," the report said.

Sunspinner, a decoy graphical user interface (GUI) application written using the Flutter framework, offers functionality aimed to convince victims that the application is legitimate.

"Consistent with the functionality advertised on the [legitimate] Civil Defense website, Sunspinner is capable of displaying crowdsourced markers with the locations of the Ukrainian military recruiters, with an option for users to add their own markers," according to the Google TAG analysis. But the fake map offers only fake inputs. All markers present [were pulled from the attacker's C2 and] were added on the same day by the same user."

Parallel Anti-Mobilization Effort Against Ukrainian Military

In tandem with the espionage effort, the other goal of the Russian fake Civil Defense campaign is to deliver disinformation aimed at suppressing Ukraine's military mobilization effort for the war. The malicious versions of Civil Defense's site and Telegram have pushed out videos with incendiary, anti-Ukrainian-military titles Users who click on the button provided by the Russian hacker-operated site to "Send Material," ostensibly to discredit recruitment efforts, are automatically fed an attacker-controlled chat thread," the report said. "Anti-mobilization content cross-posted to the group's website and Telegram channel appears to be sourced from account."

Russia has consistently used cyberattacks as part of its war strategy against Ukraine, as well as against other governments, including a recent distributed denial-of-service (DDoS) cyberattack campaign against shipping ports in Japan. Russian hackers have also been working feverishly to distribute disinformation ahead uncovered "Civilian Defense" campaign highlights, that's just one of many hacker groups doing the Kremlin's dirty work in cyberspace.

About the Author

You May Also Like

Published: Oct 25, 2024, 22:22:37

Article: [darkreading.com](#)

Author: Nate Nelson, Contributing Writer

Russia's APT29 Mimics AWS Domains to Steal Windows Credentials

Russia's APT29 Mimics AWS Domains to Steal Windows Credentials

Kremlin intelligence carried out a wide-scale phishing campaign in contrast to its usual, more targeted operations.

October 25, 2024

Russia's premiere advanced persistent threat group has been phishing thousands of targets in militaries, public authorities, and enterprises.

APT29 (aka Midnight Blizzard, Nobellum, Cozy Bear) is arguably the world's most notorious threat actor. An arm of the Russian Federation's Foreign Intelligence Service (SVR), it's best known for the historic breaches of SolarWinds and the Democratic National Committee (DNC). Lately, it has breached Microsoft's codebase "APT29 embodies the 'persistent' part of 'advanced persistent threat,'" says Satnam Narang, senior staff research engineer at Tenable. "It has persistently targeted organizations in the United States and Europe for years, utilizing various techniques, including spear-phishing and exploitation of vulnerabilities to gain initial future operations."

Along these same lines, the Computer Emergency Response Team of Ukraine (CERT-UA) recently discovered APT29 phishing Windows credentials from government, military, and private sector targets in Ukraine. And after comparing notes with authorities in other countries, CERT-UA found that the campaign was actually That APT29 would go after sensitive credentials from geopolitically prominent and diverse organizations is no surprise, Narang notes, though he adds that "the one thing that does kind of stray from the path would be its broad targeting, versus [its typical more] narrowly focused attacks."

AWS and Microsoft

The campaign, which dates back to August, was carried out using malicious domain names designed to seem like they were associated with Amazon Web Services (AWS). The emails sent from these domains pretended to advise recipients on how to integrate AWS with Microsoft services, and how to implement zero trust Despite the masquerade, AWS itself reported that the attackers weren't after Amazon, or its customers' AWS credentials.

What APT29 really wanted was revealed in the attachments to those emails: configuration files for Remote Desktop, Microsoft's application for implementing the Remote Desktop Protocol (RDP). RDP is a popular tool that legitimate users and hackers alike use to operate computers remotely.

"Normally, attackers will try to brute force their way into your system or exploit vulnerabilities, then have RDP configured. In this case, they're basically saying: 'We want to establish that connection [upfront].'" Narang says.

Launching one of these malicious attachments would have immediately triggered an outgoing RDP connection to an APT29 server. But that wasn't all: The files also contained a number of other malicious parameters, such that when a connection was made, the attacker was given access to the target computer's storage, Block RDP

APT29 may not have used any legitimate AWS domains, but Amazon still managed to interrupt the campaign by seizing the group's malicious copycats.

For potential victims, CERT-UA recommends strict precautions: not just monitoring network logs for connections to IP addresses tied to APT29 but also analyzing all outgoing connections to all IP addresses on the wider Web through the end of the month. And for organizations at risk in the future, Narang offers simpler advice. "First and foremost, don't allow RDP files to be received. You can block them at your email gateway. That's going to kneecap this whole thing," he says.

AWS declined to provide further comment for this story. Dark Reading has also reached out to Microsoft for its perspective.

About the Author

You May Also Like

Published: Oct 26, 2024, 11:36:00

Article: [thehackernews.com](#)

Author: info@thehackernews.com (The Hacker News)

CERT-UA Identifies Malicious RDP Files in Latest Attack on Ukrainian Entities

The Computer Emergency Response Team of Ukraine (CERT-UA) has detailed a new malicious email campaign targeting government agencies, enterprises, and military entities.

"The messages exploit the appeal of integrating popular services like Amazon or Microsoft and implementing a zero-trust architecture," CERT-UA said. "These emails contain attachments in the form of Remote Desktop Protocol (.rdp) configuration files."

Once executed, the RDP files establish a connection with a remote server, enabling the threat actors to gain remote access to the compromised hosts, steal data, and plant additional malware for follow-on attacks.

Infrastructure preparation for the activity is believed to have been underway since at least August 2024, with the agency stating that it's likely to spill out of Ukraine to target other countries.

CERT-UA has attributed the campaign to a threat actor it tracks as UAC-0215. Amazon Web Service (AWS), in an advisory of its own, linked it to the Russian nation-state hacking group known as APT29.

"Some of the domain names they used tried to trick the targets into believing the domains were AWS domains (they were not), but Amazon wasn't the target, nor was the group after AWS customer credentials," CJ Moses, Amazon's chief information security officer, said. "Rather, APT29 sought its targets' Windows credentials"

The tech giant said it also seized the domains the adversary was using to impersonate AWS in order to neutralize the operation. Some of the domains used by APT29 are listed below -

- ca-west-1.mfa-gov[.]cloud
- central-2-aws.ua-aws[.]army
- us-east-2-aws.ua-gov[.]cloud

TOPIC AND STORY CLUSTERING

- Reduces redundancy from multiple sources
- Identifies stories on the same topic with varied titles and styles
- Visualizes topic trends over time

Collaboration

Integrates with MISP to streamline threat intelligence collaboration.

Taranis → MISP → MISP → Taranis

Issues	Input Filters	Global Actions	Page	API	Bookmarks	★	NSOP	Trans	1	Log out
<div> <input type="text" value=""/> <input type="button" value="Go"/> <input type="button" value="Cancel"/> </div>										
Events	Org Events	Chapters	Tags	ASNs	ASConn	Date	Info			
View	Details	Details	Details	Details	Details	Details	Distribution			
org-0	7	1	77	23	2025-04-29	Security Alerts newsletter Round 513 by Perlagu Paganini - INTERNATIONAL EDITION	Internal evaluation sharing group			
org-9	7	6	95	25	2025-04-29	Cybercriminals target Canadian restaurant chain with Chameleon malware	Internal evaluation sharing group			
org-9	7	7	88	25	2025-04-29	Angreifer nutzen polnische AWS-Domains in Pristingshammen	Internal evaluation sharing group			
org-9	7	9	510	26	2025-04-29	Poland thwarted cyberattacks that were carried out by Russia and Belarus	Internal evaluation sharing group			
org-1	7	10	22	26	2025-04-29	Poland's prime minister says cyberattacks targeted his party as election nears	Internal evaluation sharing group			
org-1	7	11	124	26	2025-04-30	Russian Cable Alerts Threaten To Cut Off World's Internet	Internal evaluation sharing group			
org-1	7	13	93	25	2025-04-30	Sandworm-linked hackers target users of Ukraine's military app in new spying campaign	Internal evaluation sharing group			
org-1	7	14	54	24	2025-04-30	Germany links cyberattacks on research group to Russian state-backed hackers	Internal evaluation sharing group			
org-1	7	15	53	24	2025-04-30	Tageszusammenfassung - 23.04.2025	Internal evaluation sharing group			
org-1	7	16	28	24	2025-04-30	Russia arrests CEO of tech company linked to Doppelgänger disinformation campaign	Internal evaluation sharing group			
org-1	7	17	133	22	2025-04-30	Exclusive: Gen. Paul Nakazono says China is now our biggest cyber threat	Internal evaluation sharing group			
org-1	7	18	64	25	2025-04-30	Cyber Threats Against Energy Sector Surge as Global Tensions Mount	Internal evaluation sharing group			
org-1	7	19	146	25	2025-04-30	Russian crypto exchange Garantex's website taken down in apparent law enforcement operation	Internal evaluation sharing group			
org-2	7	21	99	23	2025-04-30	Hacked buses blast out patriotic pro-Russian anthems in Tallinn, attack government	Internal evaluation sharing group			
org-2	7	22	92	24	2025-04-30	US announces a \$10M reward for Europe's GRU hacker behind attacks on Ukraine	Internal evaluation sharing group			
org-2	7	23	85	24	2025-04-30	French Internet Index Cut in Latest Attack During Olympics	Internal evaluation sharing group			
org-2	7	24	128	25	2025-04-30	Hacktivists Call for Release of Telegram Founder with FreeCyberD DDoS Campaign	Internal evaluation sharing group			
org-2	7	25	247	25	2025-05-06	Quake, HIV/Positive, and Running Out of Medication in Gaza	Internal evaluation sharing group			
org-1	7	26	116	23	2025-05-06	Ukrainian military's anti-drone GPS spoofing suits outlandish 'phones	Internal evaluation sharing group			
org-1	7	27	119	24	2025-05-06	Pro-Russia collective NotAme55(16) launched a new wave of DDoS attacks on Italian sites	Internal evaluation sharing group			
org-2	7	28	133	25	2025-05-07	Beats of video call that are attempts to steal Microsoft 365 access, researchers tell NGOs	Internal evaluation sharing group			
org-2	7	29	224	25	2025-05-07	Lawrence's New Right Rulers in Pan-American Trumpism test	Internal evaluation sharing group			
org-2	7	30	56	22	2025-05-07	Ukraine staff terminals for europeanisches Satelliteninternet selbst her	Internal evaluation sharing group			
org-2	7	31	88	23	2025-05-07	Hackers with Kiev Kremlin ties target Kazakhstan in espionage campaign	Internal evaluation sharing group			
org-1	7	32	33	20	2025-05-07	China-linked APT Musing Panda upgrades tools in its arsenal	Internal evaluation sharing group			
org-1	7	33	22	23	2025-05-07	Top Colleges Are Too Costly Even for Parents Making \$300,000	Internal evaluation sharing group			

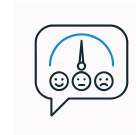
Ingest Incoming Story & Ungroup Local Stories

Contextual Enrichment

→ Summarization

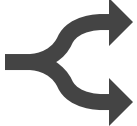


→ Sentiment Analysis



→ Threat Classification








OPEN  Source
Intelligence

Challenges of AI in OSINT

- Training data scarcity for security-specific tasks
- Domain-specific language in cybersecurity reports
- Resource limits in open-source environments

Balanced research  with practical deployment.

Taranis on OpenShift

-  Containerized microservices (Flask, Celery, PostgreSQL)
-  GitOps-ready deployment
-  Optional GPU support for model inference
-  All containers run as non-root, user-only permissions
-  Stateless by design

Demonstration

TARANIS AI

total items: 33 / displayed items: 20

search

Dashboard

Administration

Assess

Analyze

Publish

Assets

search

Items per page

20

Source

Source Group

Source

Filter

day

week

24h

Fist Day

Last Day

Tags

read

important

items in reports

relevant

Sort

published date

relevance

Display

highlight

show charts

compact view

Published: Jun 04, 2024, 10:00 - Jun 04, 2024, 13:00

Tags:

Relevance: 7

Article: [smartcityupdate.com](#)

Genetic Engineering Data Theft by APT81

APT74 involved in sabotaging smart city projects across Europe.

Published: Jun 04, 2024, 10:00 - Jun 04, 2024, 13:00

Tags:

Relevance: 4

Article: [iotsecurityfocus.com](#)

APT73 Exploits Global Shipping Container Systems

APT61 exploits vulnerabilities in IoT devices to create a large-scale botnet.

Published: Jun 04, 2024, 10:00 - Jun 04, 2024, 13:00

Tags:

Relevance: 3

Article: [softwaresecurityfocus.com](#)

Global Mining Espionage by APT67

APT55 launches a series of attacks on software development firms to inject malicious code into widely used applications.

Published: Jun 04, 2024, 10:00 - Jun 04, 2024, 13:00

Tags:

Relevance: 3

Article: [logisticssecuritytoday.com](#)

Patient Data Harvesting by APT60

APT59's new ransomware targets global shipping and logistics, demanding high ransoms.

Published: Jun 04, 2024, 11:00 - Jun 04, 2024, 13:00

Tags:

Relevance: 2

Article: [startupsecurityupdate.com](#)

Advanced Phishing Techniques by APT58

APT57 specializes in the theft of intellectual property from tech startups, threatening innovation.

Published: Jun 04, 2024, 12:00

Tags:

Relevance: 0

Article: [industrialsecuritytoday.com](#)

Industrial Malware Threat by APT54

APT54 develops malware that disrupts industrial control systems, risking severe impacts on national infrastructure.

Published: Jun 04, 2024, 10:00

Tags:

Relevance: 0

Article: [industrialsecuritytoday.com](#)

Bundesinnenministerin Nancy Faeser wird Claudia Plattner zur neuen BSI-Präsidentin berufen

Claudia Plattner wird ab 1. Juli 2023 das Bundesamt für Sicherheit in der Informationstechnik (BSI) leiten






0:00 / 4:41

15 / 19

Try yourself

```
curl -sL $(curl -s https://api.github.com/repos/taranis-ai/taranis-ai/releases/latest |  
jq -r '.assets[] | select(.name=="compose.yml") | .browser_download_url')\  
-o compose.yml  
  
curl -sL $(curl -s https://api.github.com/repos/taranis-ai/taranis-ai/releases/latest |  
jq -r '.assets[] | select(.name=="env.sample") | .browser_download_url')\  
-o .env  
  
podman-compose up -d
```


Taranis on OpenShift

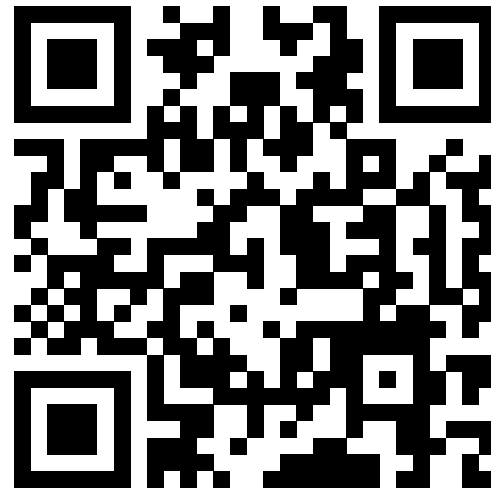
-  Containerized microservices (Flask, Celery, PostgreSQL)
-  GitOps-ready deployment
-  Optional GPU support for model inference
-  All containers run as non-root, user-only permissions
-  Stateless by design

Get Involved!

🌀 Taranis AI is open-source and looking for contributors!

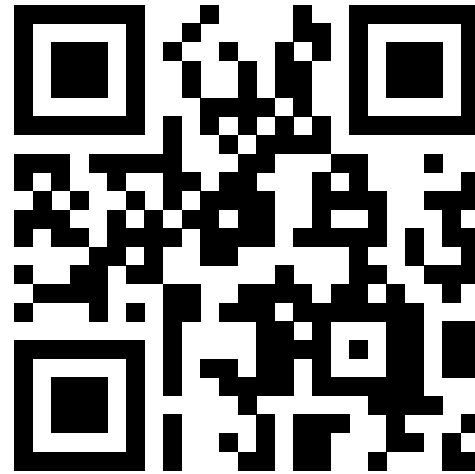
- NLP, machine learning, clustering
- New collector integrations
- Real-world feedback and use cases

 github.com/taranis-ai/taranis-ai



Survey

Help us in only 10 minutes



<https://survey.taranis.ai/>