

AI POWERED OSINT – TARANIS AI

Peter Leitmann

Center for Digital Safety & Security

Austrian Institute of Technology



AGENDA

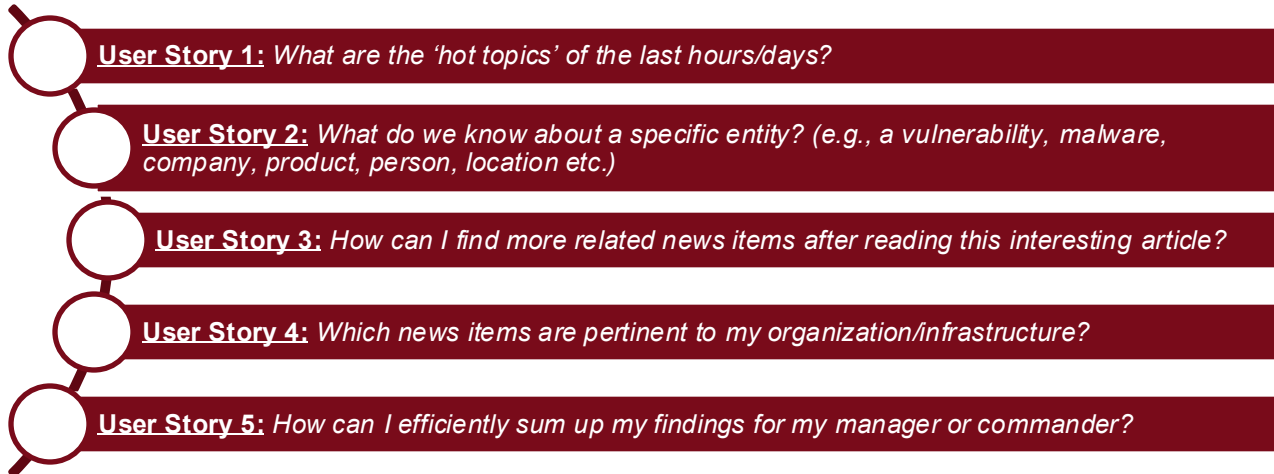
- What is OSINT and Taranis AI
- What are the hard things in OSINT analysis
- Check if more input means more output (intelligence)
- Analysts' workflow
- How AI helps
- Demo
- Q&A

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

TARANIS AI

- Open Source project on GitHub: <https://github.com/taranis-ai/taranis-ai>
- Over 1200 GitHub stars
- Build upon Taranis3 and Taranis NG
- Production-ready OSINT platform
- Connects with MISP



HARD QUESTIONS

- How can an AI model assist without interfering with a human?
- Which actions should remain manual?
- How can independent teams collaborate in a controlled manner?
- Is there one ultimate solution or where should the organisation have a say?

As project evolves, our solutions also keep adjusting

HOW MANY OF YOU HAVE BEEN EVER
OVERWHELMED BY LLM (AI) RESPONSES?
please indicate :)



MORE SIGNALS – MORE INTELLIGENCE?

- More signals do not automatically create more intelligence!
- Security Analysts need to understand:
 - What matters
 - Why it matters
 - What to do next
- This is hard when:
 - Too much arrives (news articles, reports, shared indicators, etc.)
 - Context is fragmented (across systems, sources, organisations)
 - Accountability remains human

WE NEED A BETTER SUPPORTED JUDGEMENT

not more automation



ANALYSTS' WORKFLOW

- **Collect**
 - Selected sources provide newest landscape information
- **Assess**
 - Groups related articles, adds notes/summaries
- **Analyze**
 - Writes the assessment into a structured report
- **Publish**
 - Renders and distributes an intelligence product

WHERE AI HELPS?



REMOVE THE REPETITIVE

- **Create topic clusters – Stories**
- **Summarize**
- **Extract entities and indicators**
- **Classify (sentiment, cybersecurity relevancy, etc.)**

LEADS TO A MORE EFFICIENT WORKFLOW

- **Create topic clusters – Stories**
 - Work with contextualised data
- **Summarize**
 - Relevancy can be decided quicker
- **Extract entities and indicators**
 - Tangible artifacts becomes visible (and machine readable)
- **Classify (sentiment, cybersecurity relevancy, etc.)**
 - Provide more clarity

IMPORTANT: HUMAN DECIDES WHAT MATTERS



HUMAN IN THE LOOP

Automation remains useful. Human validates what matters.

- **Analysts decide what happens**
 - What Stories go to a Report
 - What Stories are automatically shared
 - What Reports go to a Product
 - How and where they share a Product
- Automation is useful when its **boundaries are visible and adjustable**

HOW DO WE KEEP THE SYSTEM UNDER CONTROL?



MODULAR SYSTEM AND SELF-HOSTING

AI mechanisms (Bots) can be enabled individually

- LLM-Bot
 - Summarisation, Named Entity Recognition, Story Clustering, Chat , Sentiment, ...
- Local LLM models
 - Can be deployed with Taranis AI
 - GPU and CPU support
 - Data is retained on your system
- Organisations decide:
 - Where they deploy and how they isolate
 - What LLMs are connected
 - What tasks are automated
 - What Role Based Access, Access Control Lists and Traffic Light Protocol applies

DEMONSTRATION



DASHBOARD



Q Search all...



Administration Dashboard Assess Analyze Publish Assets

Dashboard

Edit Dashboard

Assess

Start analyst review

There are **124** news items

There are **122** stories

This week

124 news items · **122** stories

Top sources

Manual

100.0%

Analyze

0 completed reports

1 reports in progress

This week

1 reports created

Publish

1 products

Prepare products and choose where to publish them.

This week

1 products created

Connectors

0 conflicts need review

Resolve incoming changes before applying them.

Pending conflicts

0 story conflicts · **0** news item conflicts

Recently Active Tags

Seen in the last 7 days; counts show total matching stories.

Cybersecurity

Total stories: 115

ransomware	37
zero-day	28
phishing	28
Data breach	12
Incident response	10

Organization

Total stories: 92

CISA	29
Microsoft	18
Facebook	16
Twitter	15
Google	14

Product

Total stories: 99

PowerShell	15
Windows	14
GitHub	12
Linux	10
machine	8

07/10/2026

ASSESS II. - STORY VIEW

TARANIS AI

Q Search all...

AdministrationDashboardAssessAnalyzePublishAssets

STORY REFERENCE · 3BA7DB12-2416-401F-9744-CF92ABB3F895

✓ Save changes

↶ Return to story

📄 Add to Report

AdvancedSimple

⋮ Actions

How to turn off motion smoothing on your TV (and why it makes such a big difference)

UnreadRelevance 0

FEEDBACKTAP TO VOTE

👍 Like 0👎 Dislike 0

CREATED06. October 2026 23:45

UPDATED06. October 2026 23:47

NEWS ITEMS1

TAGS

Amazon Fire TVTVsmart TVs

LANGUAGES

EN

Editor

Title*How to turn off motion smoothing on your TV (and why it makes such a big difference)

Story TLP override

Inherit from news items

TLP: clear

Summary

Motion smoothing inserts extra frames to make movement look fluid, but can give movies an unnatural "soap opera" effect. The guide explains how to turn the setting off on common TV platforms.

Analyst comments

Analyst note: Non-cybersecurity technology coverage. Keep as a contrast case for classifier review; no security action is indicated by this report.

Attributes

Attributes are stored as key/value pairs. Unsupported keys are preserved as-is.

CYBERSEC_CLASSIFIER_BOT1Remove

NLP_BOT32Remove

cybersecuritynoRemove

sentimentneutralRemove

Add attribute

Story status

Cybersecurity · No

Sentiment · Neutral

AI assisted actions

Kick off automation and keep the panel open while tasks run. Results will refresh automatically when finished.

Generate summary & title

Run sentiment analysis

Cybersecurity classification

MISP auto-update

Push this story after five minutes without further changes.

MISP connectorSelect connector

07/10/2026

21

ASSESS III. - STORY VIEW



Administration Dashboard Assess Analyze Publish Assets

STORY REFERENCE · 11086635-4780-4046-ASD9-81CB510C6A21

Save changes Return to story Add to Report Advanced Simple Actions

Edge Device Intrusions | Related Reporting

Unread Important Relevance 6

FEEDBACK TAP TO VOTE

Like 0 Dislike 0

CREATED 06. October 2026 23:39

UPDATED 06. October 2026 23:46

NEWS ITEMS 3

TAGS

Advanced persistent threat CISa China Cisco Control Systems Hitachi Energy Poland Russia

LANGUAGES

EN

Editor

Title* Edge Device Intrusions | Related Reporting

Story TLP override

Inherit from news items

TLP: clear

Summary

Related reporting links router traffic hijacking, government action to replace unsupported edge devices, and an intrusion at a Polish energy operator associated with exposed VPN access.

Analyst comments

Analyst note: Three reports point to exposure at network boundaries. Compare the named edge and VPN assets with primary advisories, then review externally reachable management and remote-access services.

Attributes

Attributes are stored as key/value pairs. Unsupported keys are preserved as-is.

Add attribute

cybersecurity yes Remove

sentiment negative Remove

CYBERSEC_CLASSIFIER_BOT 1 Remove

report_01a11390-1ebe-739d-ab70-79ba38f Threat Activity Briefing Remove

Story status

Cybersecurity · Yes

Sentiment · Negative

AI assisted actions

Kick off automation and keep the panel open while tasks run. Results will refresh automatically when finished.

Generate summary & title

Run sentiment analysis

Cybersecurity classification

MISP auto-update

Push this story after five minutes without further changes.

ANALYZE – REPORT CREATION VIEW



Search all...

Administration Dashboard Assess Analyze Publish Assets

Update Report - Threat Activity Briefing ID: 01a11390-1ebe-739d-ab70-79ba3888b7ae

Title *

Threat Activity Briefing

Report Type *

OSINT Report

Summary

Summary

Security reporting this week highlights active exploitation of exposed enterprise software. Five linked stories describe vulnerability exploitation and resulting risk to internet-facing services. Prioritize patching, exposure reduction, and log review for affected products.

Sector trends

Enterprise software and network infrastructure appear across the linked reporting, indicating cross-sector exposure where shared platforms are deployed.

Vulnerabilities trends

Multiple reports describe vulnerabilities under active exploitation, including remote code execution and authentication bypass. Confirm affected versions, apply vendor fixes, and review externally reachable management interfaces.

Ransomware trends

The selected stories focus on exploited vulnerabilities rather than a single ransomware group. Monitor for follow-on intrusion activity and ransomware deployment after initial access.

Date published 10/07/2026

Threat level High

Threat level

TLP Level Clear

Ransomware

Ransomware

No ransomware group is identified in the selected reporting; the coverage focuses on exploited vulnerabilities and risk to

Actor

Multiple or unconfirmed actors; the linked reports do not support a single attribution.

Version History (5)

CTI information

Publish

Completed

Incomplete

Split view

Stacked view

Stories

Remove all

Ransomware attackers are exploiting critical SmarterMail vulnerability (CVE-2026-24423)

<https://www.helpnetsecurity.com/2026/02/06/ransomware-smartermail-cve-2026-24423/>

Remove from report

For the third time in two weeks, CISA added a vulnerability (CVE-2026-24423) affecting SmarterTools' SmarterMail email and collaboration server to its Known Exploited Vulnerabilities catalog, and this one is being exploited in ransomware attacks. A glut of SmarterMail vulnerabilities On January 26, the US cybersecurity agency listed CVE-2025-52691 (a unrestricted upload of file with dangerous type vulnerability) and CVE-2026-23760...

Attackers are exploiting critical NGINX vulnerability (CVE-2026-42945)

<https://www.helpnetsecurity.com/2026/05/18/nginx-vulnerability-exploited-cve-2026-42945/>

Remove from report

A critical NGINX vulnerability (CVE-2026-42945) disclosed last week is being exploited by attackers, VulnCheck security researcher Patrick Garrity revealed on Saturday. The vulnerability, dubbed NGINX Rift, can be reliably exploited to trigger a denial-of-service condition and can potentially allow for unauthenticated remote code execution, all achievable by sending a specially crafted HTTP request to a vulnerable NGINX instance.

Attackers are exploiting RCE vulnerability in BIG-IP APM systems (CVE-2025-53521)

<https://www.helpnetsecurity.com/2026/03/28/big-ip-apm-vulnerability-cve-2025-53521-exploited/>

Remove from report

A critical unauthenticated remote code execution vulnerability (CVE-2025-53521) in F5's BIG-IP Access Policy Manager (APM) solution is under active exploitation, the US Cybersecurity and Infrastructure Security Agency warned on Friday. CISA added the flaw to its Known Exploited Vulnerabilities catalog after F5 updated the related security advisory. The advisory was initially published on October 15, 2025, when F5 confirmed a data...

Attackers are exploiting auth bypass vulnerability on FortiGate firewalls (CVE-2025-59718)

<https://www.helpnetsecurity.com/2025/12/17/fortigate-vulnerability-cve-2025-59718-exploited/>

Remove from report

Attackers are exploiting a recently revealed vulnerability (CVE-2025-59718) to bypass authentication on Fortinet's FortiGate firewalls, and are leveraging the achieved access to export their system configuration files, Arctic Wolf researchers warned on Tuesday. Configuration files can expose information about the underlying network and infrastructure, firewall and security policies, encrypted/hashed passwords, and more.

PUBLISH – PRODUCT CREATION

TARANIS AI

Q Search all...

AdministrationDashboardAssessAnalyzePublishAssets

Update Product - Threat Activity Briefing

Create copyDownloadRenderSave

Product Type *

Default html tailwindcss Presenter

Title *

Threat Activity Briefing

Description

Weekly threat briefing on active exploitation affecting enterprise software and network infrastructure.

Report Items

Search...

✓	Id	Title	Created	Completed
✓	01a11390-1ebe-739d-ab70-79ba3888b7ae	Threat Activity Briefing	2026-10-06T23:32:54.645644+00:00	

Items per page: 5< < Page 1 of 1 > >

Last published product

[/reports/01a11390-200b-73b3-8cd7-cce22b42d80d](#)

Publish (manually)

Default Publisher

—

Required only when Autopublish is enabled.

Autopublish

Update Product - Threat Activity Briefing

OSINT INTELLIGENCE REPORT

Threat Activity Briefing

Generated 2026-10-06.

Product ID: 01a11390-200b-73b3-8cd7-cce22b42d80d Presenter: [Html Presenter](#) Coverage: 1 report

NARRATIVES

6

SOURCE ARTICLES

8

LINKED SOURCES

8

SNAPSHOT

REPORT ITEMS

1

TAG SIGNALS

90

UPDATE DATE

2026-10-06

REPORT INDEX

[01 Threat Activity Briefing](#)

REPORT ITEM 1

Threat Activity Briefing

ID 01a11390-1ebe-739d-ab70-79ba3888b7ae Created 2026-10-06T23:32:54.645644+00:00 Updated 2026-10-06T23:32:54.645651+00:00 Status In Progress

STORIES

6

Story count

REPORT METADATA

Ransomware

Actor

Multiple or unconfirmed actors; the linked reports do not support a single attribution.

Comment

Analyst assessment: prioritize patching internet-facing software and network appliances. Attribution and ransomware deployment are unconfirmed in these reports.

Ransomware

OSINT INTELLIGENCE REPORT

Threat Activity Briefing

Generated 2026-10-06.

PRODUCT ID: 01a11390-200b-73b3-8cd7-cce22b42d80d PRESENTER: Html Presenter

COVERAGE: 1 report

SNAPSHOT

REPORT ITEMS

1

TAG SIGNALS

90

UPDATE DATE

2026-10-06

NARRATIVES

6

SOURCE ARTICLES

8

LINKED SOURCES

8

REPORT INDEX

01 Threat Activity Briefing

REPORT ITEM 1

Threat Activity Briefing

ID 01a11390-1ebe-739d-ab70-79ba3888b7ae CREATED 2026-10-06T23:32:54.645644+00:00

UPDATED 2026-10-06T23:32:54.645651+00:00 STATUS In Progress

REPORT METADATA

Ransomware

Summary

ACTOR

DATE PUBLISHED

STORIES

6

Story count

MISP

Edge Device Intrusions | Related Reporting

Event ID	215
UUID	110b6635-4780-4046-a5d9-81cb510c6a21  
Creator org	 ADMIN
Owner org	 ADMIN
Creator user	admin@admin.test
Protected Event (experimental) 	 Event is in unprotected mode. Switch to protected mode
Tags	 
Date	2026-10-07
Threat Level	? Undefined
Analysis	Initial
Distribution	This community only  
Warnings	Contextualisation: Your event has neither tags nor galaxy clusters attached - generating and more accurate filtering, it is highly recommended!
Published	No
#Attributes	56 (4 Objects)
First recorded change	2026-10-07 00:08:22
Last change	2026-10-07 00:08:22
Modification map	.
Sightings	0 (0) - restricted to own organisation only. 

☐ 2026-10-07* afe...2ff 	Object name: taranis-news-item 	title :: text China-Linked DKnife AitM Framework Targets Routers for Traffic Hijacking, Malware Delivery	   
Hide 10 Attributes			
☐ 2026-10-07* 70c...8c4 	Other	title: text China-Linked DKnife AitM Framework Targets Routers for Traffic Hijacking, Malware Delivery	   
☐ 2026-10-07* aaf...503 	External analysis	link: link https://thehackernews.com/2026/02/china-linked-dknife-aitm-framework.html	   
☐ 2026-10-07* a12...9f8 	Other	content: text Cybersecurity researchers have taken the wraps off a gateway-monitoring and adversary-in-the-middle (AitM) framework dubbed DKnife that's operated by China-nexus threat actors since at least 2019. The framework comprises seven Linux-based implants that are designed to perform deep packet inspection, manipulate traffic, and deliver malware via routers and edge devices. Its primary targets seem to be Chinese-speaking users, an assessment based on the presence of credential harvesting phishing page ... Show all	   
☐ 2026-10-07* be5...a91 	Other	author: text info@thehackernews.com (The Hacker News)	   
☐ 2026-10-07* e95...8d6 	Payload delivery	hash: sha256 ea9f79c9f2d45a58ffb9c50dc0e2b3ccb4123964a1ab4e78fc427b5b6513bfb1	   
☐ 2026-10-07* e78...dda 	Other	id: text 5fcb2fc-f6e3-416e-acb5-2c79613e5509	   
☐ 2026-10-07* 790...cbf 	Other	language: text en	   
☐ 2026-10-07* 84d...b3f 	Other	osint_source_id: text 01a1137a-4946-70c7-a394-6f970943835d	   
☐ 2026-10-07* e4f...521 	External analysis	source: https://feeds.feedburner.com/TheHackersNews	   

CHAT FEATURE

New Chat

Find the cybersecurity story ...

Find the cybersecurity story about CVE-2026-24423 and summarize its key risk.

Taranis Chat

The key risk associated with CVE-2026-24423 is that the critical vulnerability in SmarterMail email and collaboration servers is being exploited by ransomware attackers. The vulnerability has been added to CISA's Known Exploited Vulnerabilities catalog.

[View 2 matching stories in Assess](#)

SEARCH & SCOPE help

Q Search stories ctrl+k

Q Search tags

CVE-2026-24423

Filter

Clear time filters

Shift Week 24h

From mm/dd/yyyy, --:-- --

To mm/dd/yyyy, --:-- --

Select sources

Select languages

Ask Taranis...

Read Any

Important Any

In Reports Any

Relevance Any

BOOKMARKS

2 / 2 Stories

PUBLISHED 06. October 2026 23:33

Ransomware attackers are exploiting critical SmarterMail vulnerability (CVE-2026-24423)

<https://www.helpnetsecurity.com/2026/02/06/ransomware-smartermail-cve-2026-24423/>

SOURCE Manual

Unread Important Relevance 6

News Items 1

IN REPORTS

CISA CODE WHITE GmbH CVE-2025-52691 CVE-2026-23760 CVE-2026-24423 +11

For the third time in two weeks, CISA added a vulnerability (CVE-2026-24423) affecting SmarterTools' SmarterMail email and collaboration servers to its Known Exploited Vulnerabilities catalog, and this one is being exploited in ransomware attacks. A glut of SmarterMail vulnerabilities On January 26, the agency CISA warns. Roughly two weeks ago, security researchers raised the alarm about hackers exploiting an authentication bypass vulnerability in SmarterMail (CVE-2025-52691) and CVE-2026-23760...

PUBLISHED 06. October 2026 13:33

Critical SmarterMail Vulnerability Exploited in Ransomware Attacks

<https://www.securityweek.com/critical-smartermail-vulnerability-exploited-in-ransomware-attacks/>

SOURCE Manual

Unread Relevance 0 News Items 1

CISA CVE-2025-11953 CVE-2026-24423 GitHub NIST +5

SmarterTools SmarterMail business email and collaboration servers are targeted in attacks exploiting another recent critical-severity vulnerability. On January 26, the agency CISA warns. Roughly two weeks ago, security researchers raised the alarm about hackers exploiting an authentication bypass vulnerability in SmarterMail (CVE-2025-52691) and CVE-2026-23760...

Showing 1 - 2 of 2

FUTURE PLANS

- Where else is AI's support desired?
- How can we support an efficient collaboration of Analysts?
- Taranis AI Chat – what should the scope be (agentic?)
- Internet History – compare how articles evolve
- Asset Management – how to connect assets with the current landscape well

TALK FUNDING - MIRANDA

- Funded by the European Union under the Horizon Europe Research and Innovation programme (GA no. 101168144 - MIRANDA). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.



QUESTIONS?



THANK YOU!

Peter Leitmann, 7.10.2026



Contact:

Peter.Leitmann@ait.ac.at

Taranis@list.ait.ac.at