AI-Crafted Custom Resources for Threat Intelligence & Hunting

This project:

It's a AI automated Threat Intelligence and hunting that creates custom resources. This will do the collecting and automating for you and provide some AI content which the AI has gone through. This project can be expanded to be scraping on a bigger scale or adding extra things to improve it.

To note:

- This was done by running n8n on my local machine
- This was also using ChatGPT to vibe code JavaScript for each node
- This does take some time to run because it's going to go through more than 10 news and depending that it contains key words
- If it does pass and that it contains key words the ai might output nothing of the "use case" or "query"

Tools used:

- n8n
- thehackernews.com
- ChatGPT
- DeepSeek R1
- Google sheets

API/connections used:

- Jina AI (jina.ai)
- OpenRouter (openrouter.ai)
- Google sheets

Programming and Markup language:

- JavaScript
- HTML

Problems:

- This has only be test for than 20 times but you can come across maybe either false positive (FP) and false negative (FN).
- It only scrapes one page it cannot go to the next page where there are more news article so if a bunch of news came in and there are 2 pages of todays news. It will only scrape the first page
- Sometimes the code node will give blanks in either title, description or MITRE (That's more of the coding end)
- It uses a lot of tokens for this to run. Running it around 3 or 4 times a day should be fine. But if it uses too much tokens the API service will not be able to be used for the next 24 hours (I was using a free version).

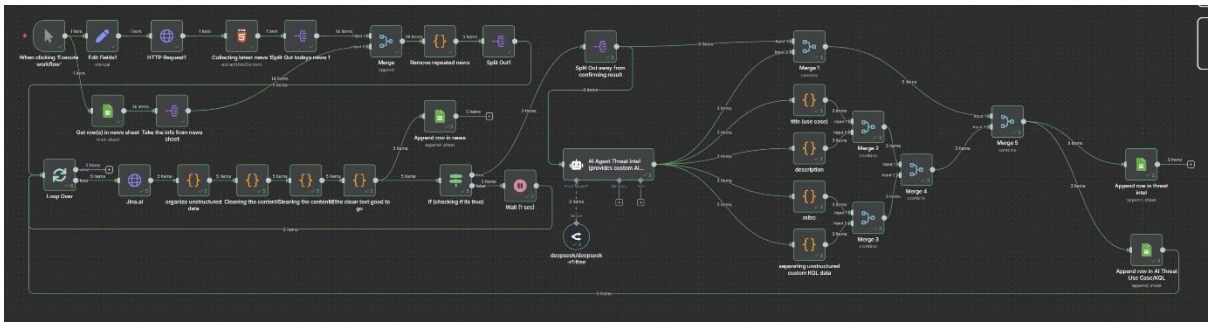
How does it work:

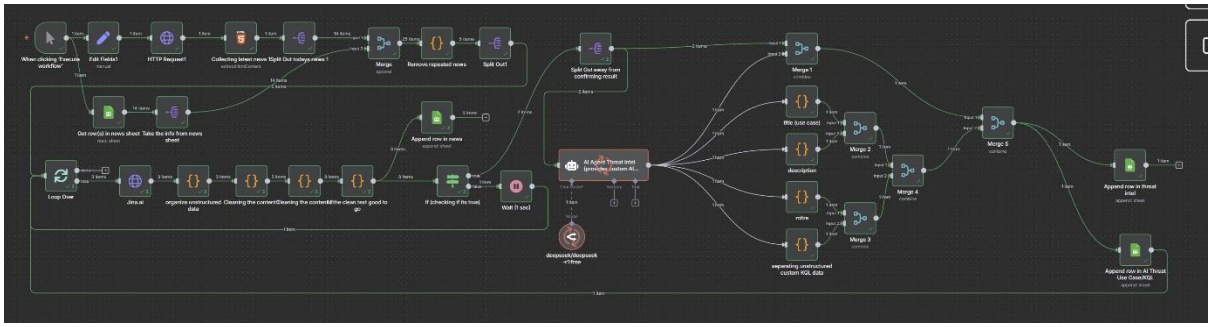
1. This will go through "https://thehackernews.com/" site
2. It will then scrape all the news on the first page of "https://thehackernews.com/"
3. The scraping would be getting the HTML
4. This would be treated as Temporary data
5. This Temporary data contains the URL
6. This Temporary URL will be compare to Permanent URL in the excel sheet
7. If "Temporary URL == Permanent URL" the Temporary URL will not go through, only the ones that are not equal to the Permanent URL will go through
8. It will then go into a Loop which will go through the number of URL there are
9. Each URL news will go in one at a time
10. Jina AI will extract the content from the URL
11. That content will go through a cleaning process
12. The cleaning process (the code) will get rid as much of the unnecessary stuff as possible
13. It will then go through the new content and look for key words
14. Once its finished find or not find the keyword it will append the excel sheet

15. It appends the sheet for the reason that if this is run again you will not get 2 of the same information
16. Back to find the key word, once found or not it will be put through a IF statement
17. If a key word was found in the content it will give a true value and move the content to the AI agent
18. If it was false, it will loop back again and start doing the next URL
19. Once the ai is finished with the content it output the “AI content”
20. The AI content will go through 4 codes that each one will do either getting the title, description, MITRE ATT&CK, and KQL Queries.
21. The KQL Queries is for **Microsoft Sentinel**
22. They will all be merge together one by one
23. Once finished it will be append to the excel sheets
24. To note that all JavaScript code was vibe code

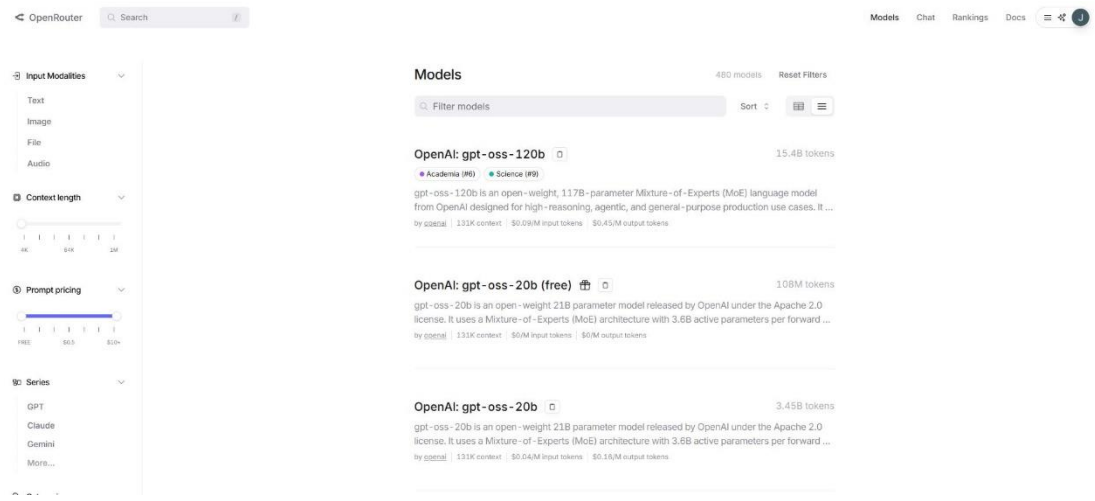
The Process:

This is the workflow:

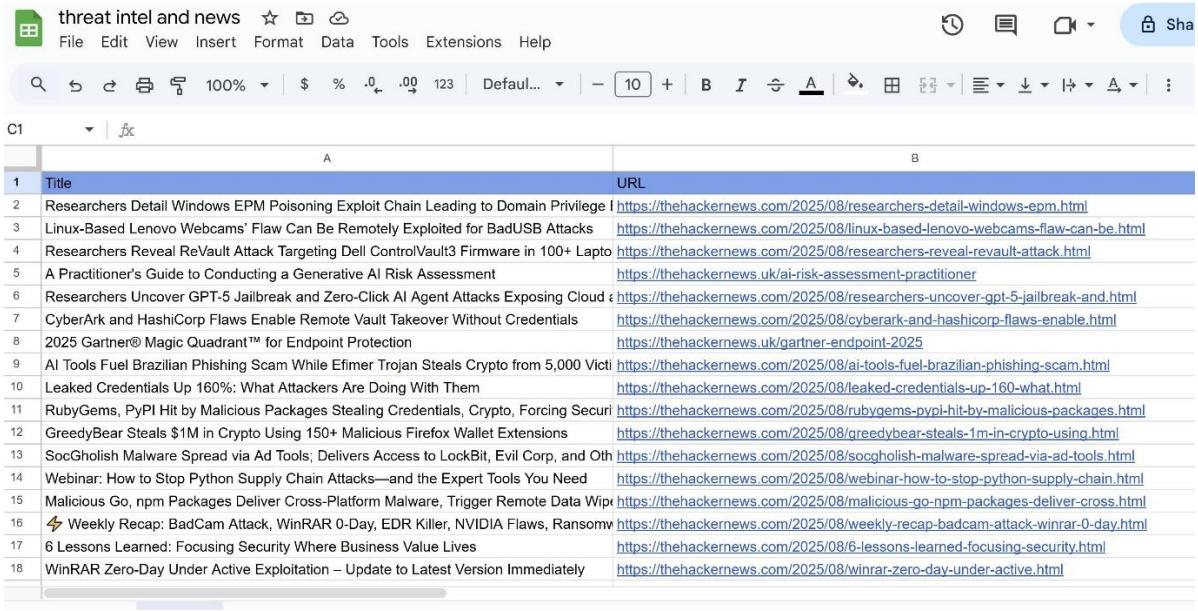




These are the 2 sites where I got my API from. (jina ai and openrouter):



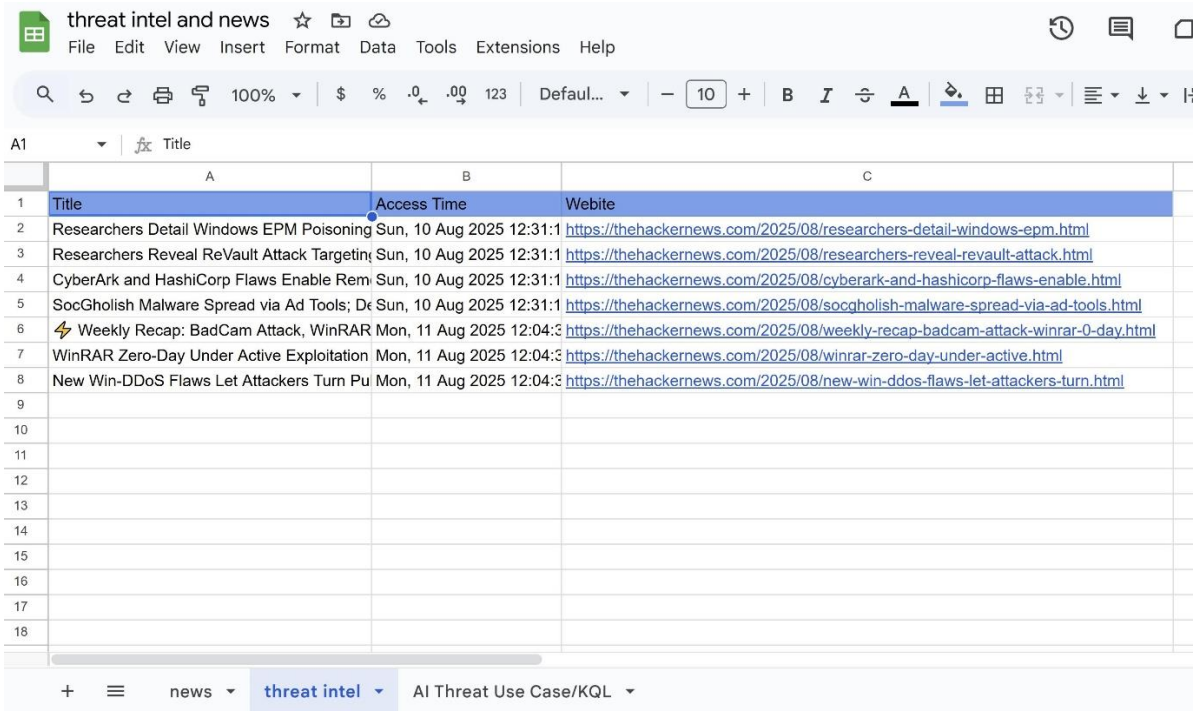
This is my google sheets result:

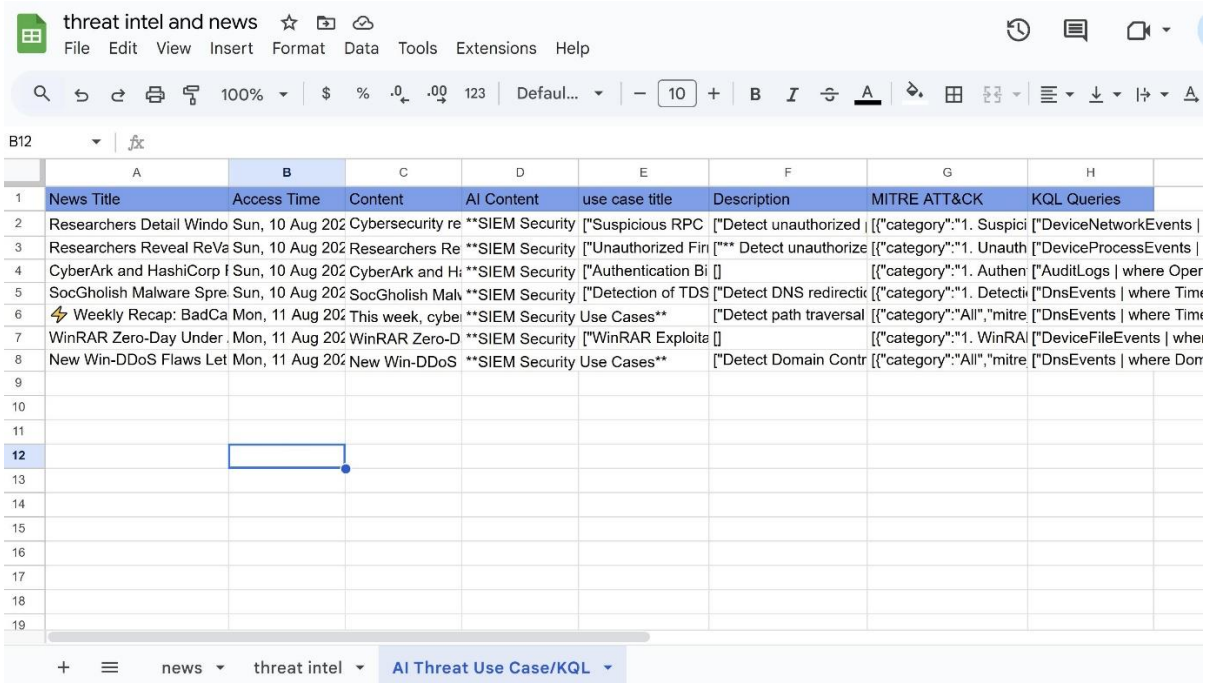

threat intel and news

File Edit View Insert Format Data Tools Extensions Help

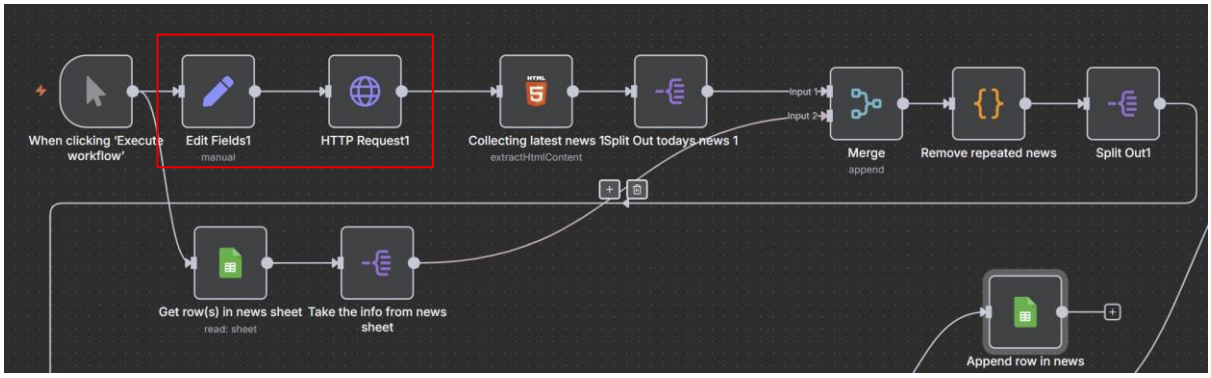
C1

	A	B
1	Title	URL
2	Researchers Detail Windows EPM Poisoning Exploit Chain Leading to Domain Privilege I	https://thehackernews.com/2025/08/researchers-detail-windows-epm.html
3	Linux-Based Lenovo Webcams' Flaw Can Be Remotely Exploited for BadUSB Attacks	https://thehackernews.com/2025/08/linux-based-lenovo-webcams-flaw-can-be.html
4	Researchers Reveal ReVault Attack Targeting Dell ControlVault3 Firmware in 100+ Lapto	https://thehackernews.com/2025/08/researchers-reveal-revault-attack.html
5	A Practitioner's Guide to Conducting a Generative AI Risk Assessment	https://thehackernews.uk/ai-risk-assessment-practitioner
6	Researchers Uncover GPT-5 Jailbreak and Zero-Click AI Agent Attacks Exposing Cloud a	https://thehackernews.com/2025/08/researchers-uncover-gpt-5-jailbreak-and.html
7	CyberArk and HashiCorp Flaws Enable Remote Vault Takeover Without Credentials	https://thehackernews.com/2025/08/cyberark-and-hashicorp-flaws-enable.html
8	2025 Gartner® Magic Quadrant™ for Endpoint Protection	https://thehackernews.uk/gartner-endpoint-2025
9	AI Tools Fuel Brazilian Phishing Scam While Efimer Trojan Steals Crypto from 5,000 Victi	https://thehackernews.com/2025/08/ai-tools-fuel-brazilian-phishing-scam.html
10	Leaked Credentials Up 160%: What Attackers Are Doing With Them	https://thehackernews.com/2025/08/leaked-credentials-up-160-what.html
11	RubyGems, PyPI Hit by Malicious Packages Stealing Credentials, Crypto, Forcing Securi	https://thehackernews.com/2025/08/rubygems-pypi-hit-by-malicious-packages.html
12	GreedyBear Steals $1M in Crypto Using 150+ Malicious Firefox Wallet Extensions	https://thehackernews.com/2025/08/greedybear-steals-1m-in-crypto-using.html
13	SocGholish Malware Spread via Ad Tools; Delivers Access to LockBit, Evil Corp, and Oth	https://thehackernews.com/2025/08/socgholish-malware-spread-via-ad-tools.html
14	Webinar: How to Stop Python Supply Chain Attacks—and the Expert Tools You Need	https://thehackernews.com/2025/08/webinar-how-to-stop-python-supply-chain.html
15	Malicious Go, npm Packages Deliver Cross-Platform Malware, Trigger Remote Data Wipe	https://thehackernews.com/2025/08/malicious-go-npm-packages-deliver-cross.html
16	⚡ Weekly Recap: BadCam Attack, WinRAR 0-Day, EDR Killer, NVIDIA Flaws, Ransomw	https://thehackernews.com/2025/08/weekly-recap-badcam-attack-winrar-0-day.html
17	6 Lessons Learned: Focusing Security Where Business Value Lives	https://thehackernews.com/2025/08/6-lessons-learned-focusing-security.html
18	WinRAR Zero-Day Under Active Exploitation – Update to Latest Version Immediately	https://thehackernews.com/2025/08/winrar-zero-day-under-active.html

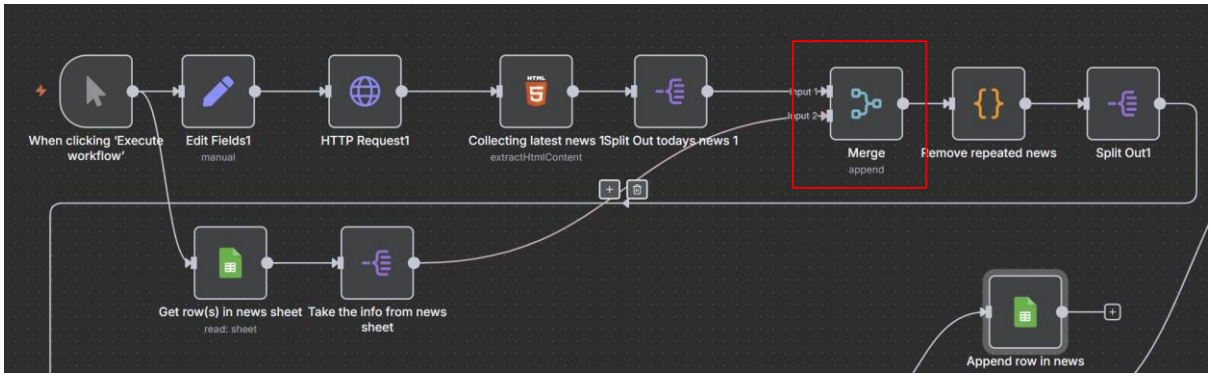




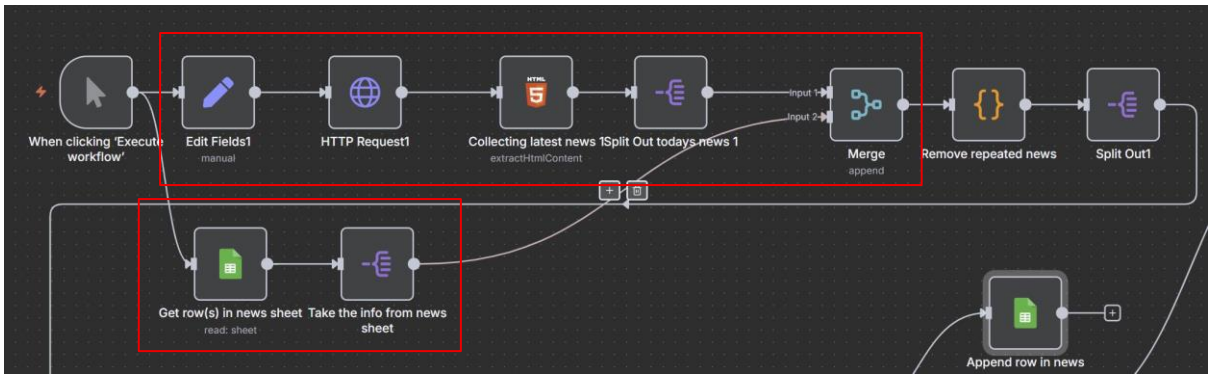
This contains the URL of “https://thehackernews.com/”:



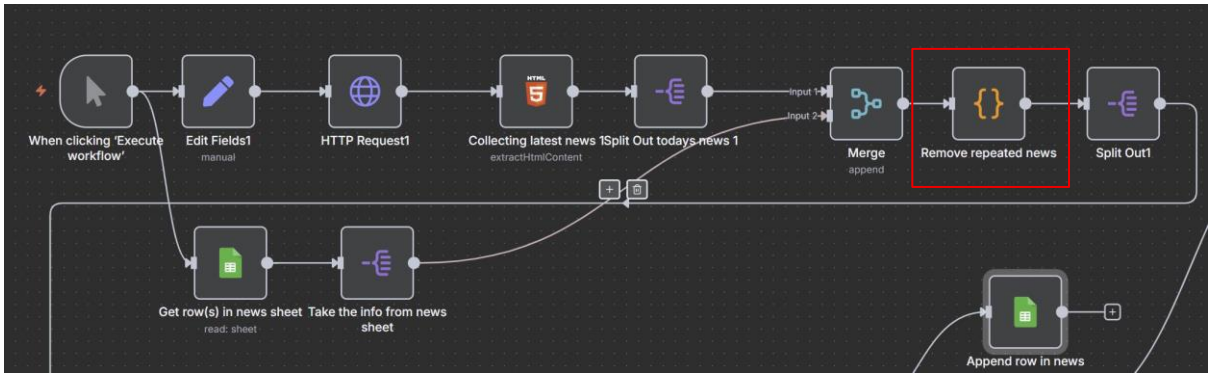
This extract the HTML content of the website only for “https://thehackernews.com/” which then gets to the merge node:



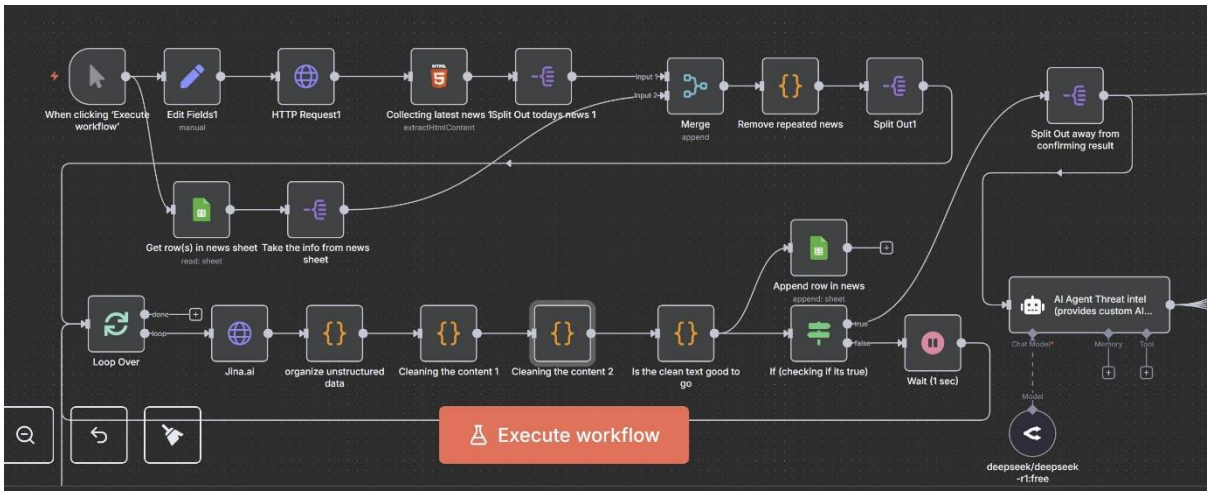
Same for the google sheet that its just getting the URL and having Temporary URL and Permeant URL:



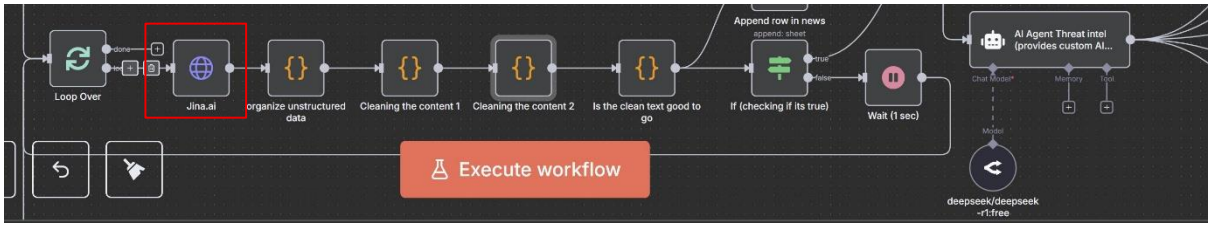
Then it gets pushed in a code node (JavaScript) where it outputs the URL that are not equal to each other :



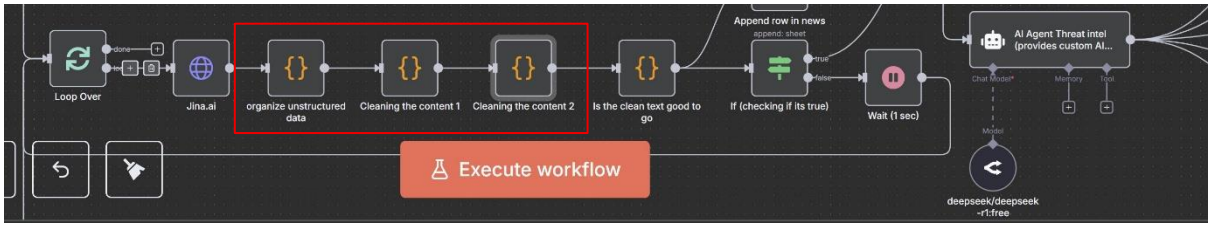
The list will of URL will go through a Loop:



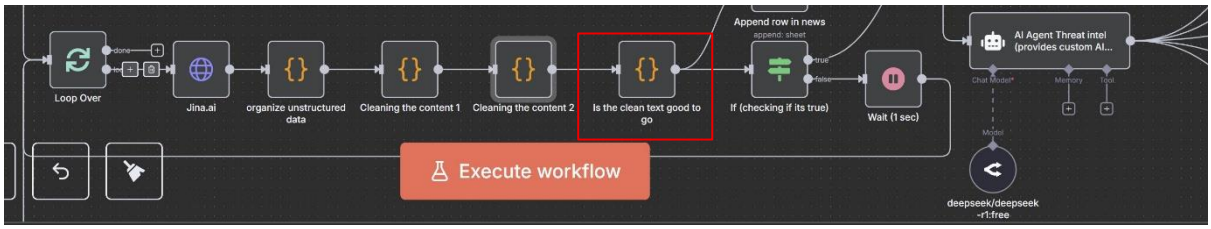
This will go into AI scrape called Jina AI which the node and AI is setup in a way that it will go through each news one at a time:



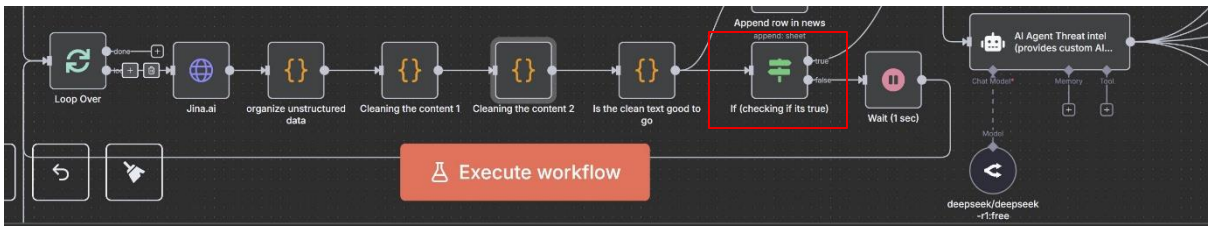
It then goes through 3 code nodes (JavaScript) which the 1st nodes separates the content from everything else. The 2nd and 3rd is trying to get as much of the tiny detail because this content will be pushed into the AI agent.



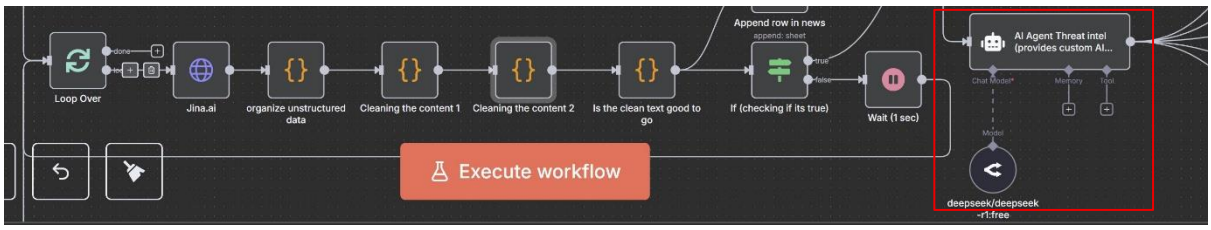
The Last node will check in the cleaned content any key words which could be domains, URL or CVE. If contains any of the threat hunting keywords then it will give a true, if not false:



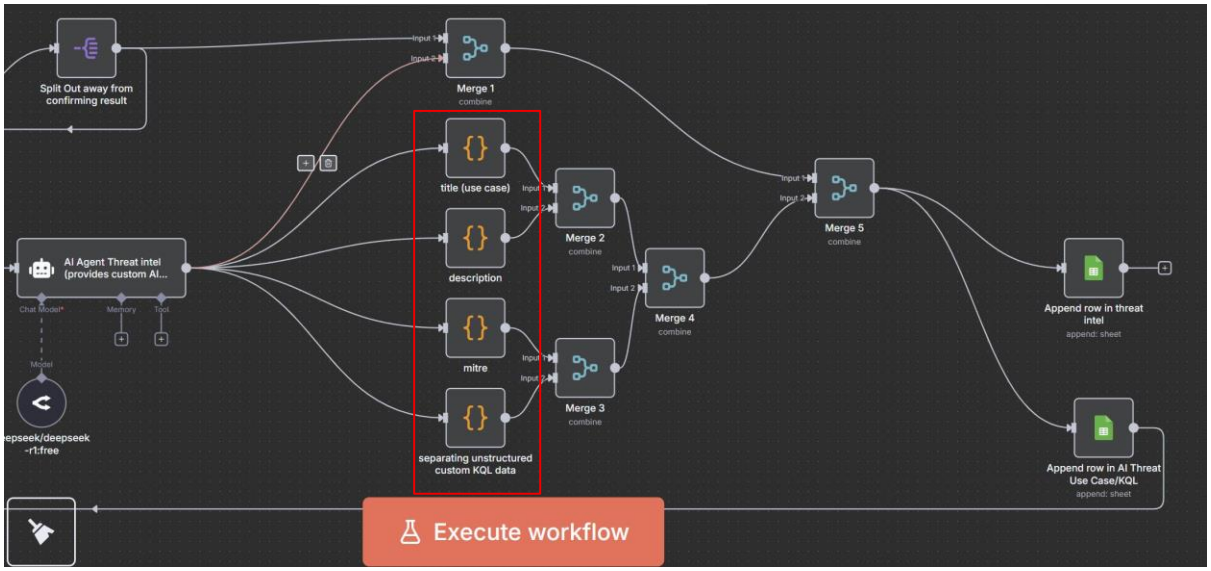
This then gets append into a google sheet which become the database where this will help the 1st google sheet if there are any duplicates in the future. It can filter out the URLs.



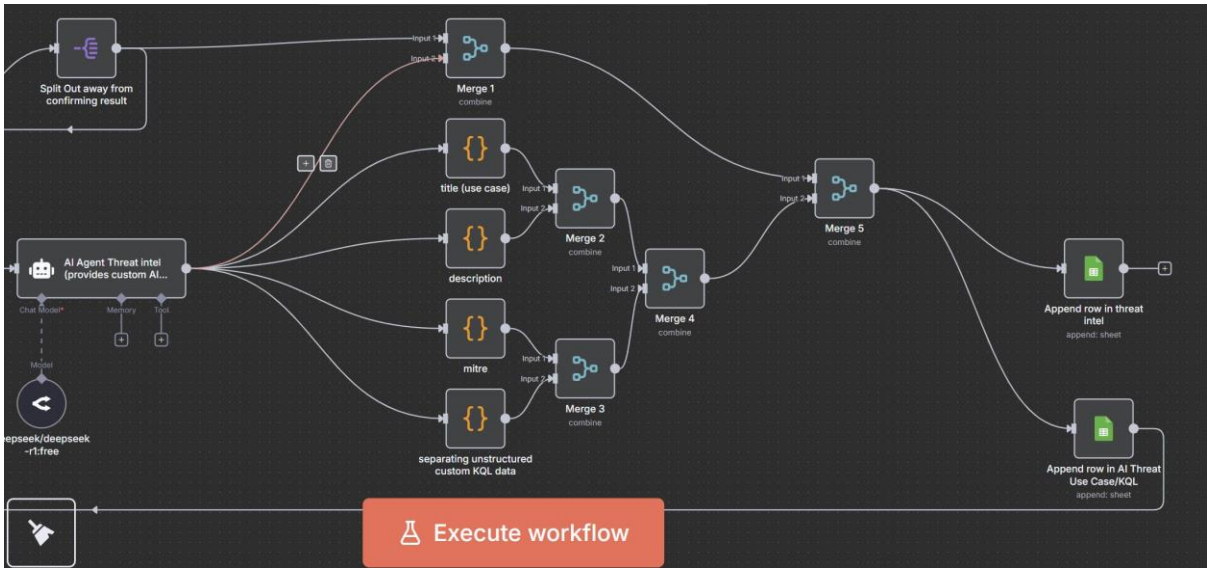
The IF statement checks if it's true or false. If true get the content pushed to the AI Agent. If false move onto the next URL.



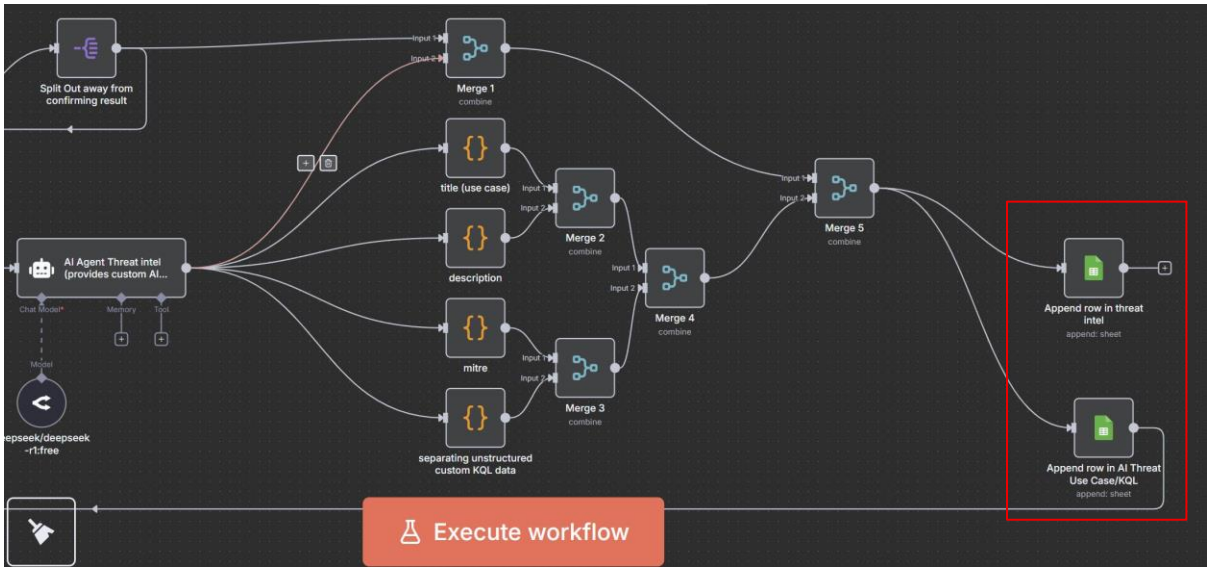
It gets pass to the AI agent to analyse the content and produce the AI content, title, description, MITRE ATT&CK, and KQL queries:



Once everything is done, everything gets put into 1 row. The reason there is not just 1 merge node is that it will not create 1 row but multiple which a lot with give “[undefined]”:



Once its all in one row it gets append into the excel sheets



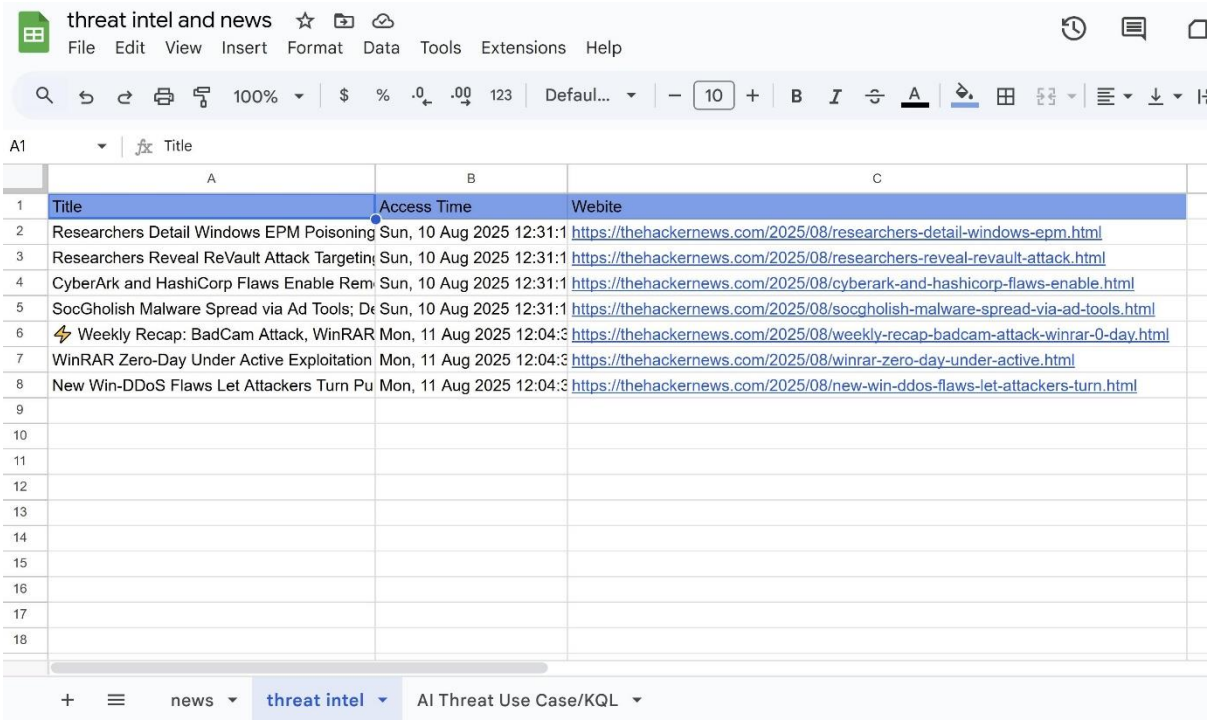
This was the first excel to get append information which just keeps all the news. It does not matter if it was pass by ai or not:

threat intel and news

File Edit View Insert Format Data Tools Extensions Help

	A	B
1	Title	URL
2	Researchers Detail Windows EPM Poisoning Exploit Chain Leading to Domain Privilege I	https://thehackernews.com/2025/08/researchers-detail-windows-epm.html
3	Linux-Based Lenovo Webcams' Flaw Can Be Remotely Exploited for BadUSB Attacks	https://thehackernews.com/2025/08/linux-based-lenovo-webcams-flaw-can-be.html
4	Researchers Reveal ReVault Attack Targeting Dell ControlVault3 Firmware in 100+ Lapto	https://thehackernews.com/2025/08/researchers-reveal-revault-attack.html
5	A Practitioner's Guide to Conducting a Generative AI Risk Assessment	https://thehackernews.uk/ai-risk-assessment-practitioner
6	Researchers Uncover GPT-5 Jailbreak and Zero-Click AI Agent Attacks Exposing Cloud a	https://thehackernews.com/2025/08/researchers-uncover-gpt-5-jailbreak-and.html
7	CyberArk and HashiCorp Flaws Enable Remote Vault Takeover Without Credentials	https://thehackernews.com/2025/08/cyberark-and-hashicorp-flaws-enable.html
8	2025 Gartner® Magic Quadrant™ for Endpoint Protection	https://thehackernews.uk/gartner-endpoint-2025
9	AI Tools Fuel Brazilian Phishing Scam While Efimer Trojan Steals Crypto from 5,000 Victi	https://thehackernews.com/2025/08/ai-tools-fuel-brazilian-phishing-scam.html
10	Leaked Credentials Up 160%: What Attackers Are Doing With Them	https://thehackernews.com/2025/08/leaked-credentials-up-160-what.html
11	RubyGems, PyPI Hit by Malicious Packages Stealing Credentials, Crypto, Forcing Securi	https://thehackernews.com/2025/08/rubygems-pypi-hit-by-malicious-packages.html
12	GreedyBear Steals $1M in Crypto Using 150+ Malicious Firefox Wallet Extensions	https://thehackernews.com/2025/08/greedybear-steals-1m-in-crypto-using.html
13	SocGholish Malware Spread via Ad Tools; Delivers Access to LockBit, Evil Corp, and Oth	https://thehackernews.com/2025/08/socgholish-malware-spread-via-ad-tools.html
14	Webinar: How to Stop Python Supply Chain Attacks—and the Expert Tools You Need	https://thehackernews.com/2025/08/webinar-how-to-stop-python-supply-chain.html
15	Malicious Go, npm Packages Deliver Cross-Platform Malware, Trigger Remote Data Wipe	https://thehackernews.com/2025/08/malicious-go-npm-packages-deliver-cross.html
16	Weekly Recap: BadCam Attack, WinRAR 0-Day, EDR Killer, NVIDIA Flaws, Ransomw	https://thehackernews.com/2025/08/weekly-recap-badcam-attack-winrar-0-day.html
17	6 Lessons Learned: Focusing Security Where Business Value Lives	https://thehackernews.com/2025/08/6-lessons-learned-focusing-security.html
18	WinRAR Zero-Day Under Active Exploitation – Update to Latest Version Immediately	https://thehackernews.com/2025/08/winrar-zero-day-under-active.html

This sheet is for the ones that have been pass through the AI agent:

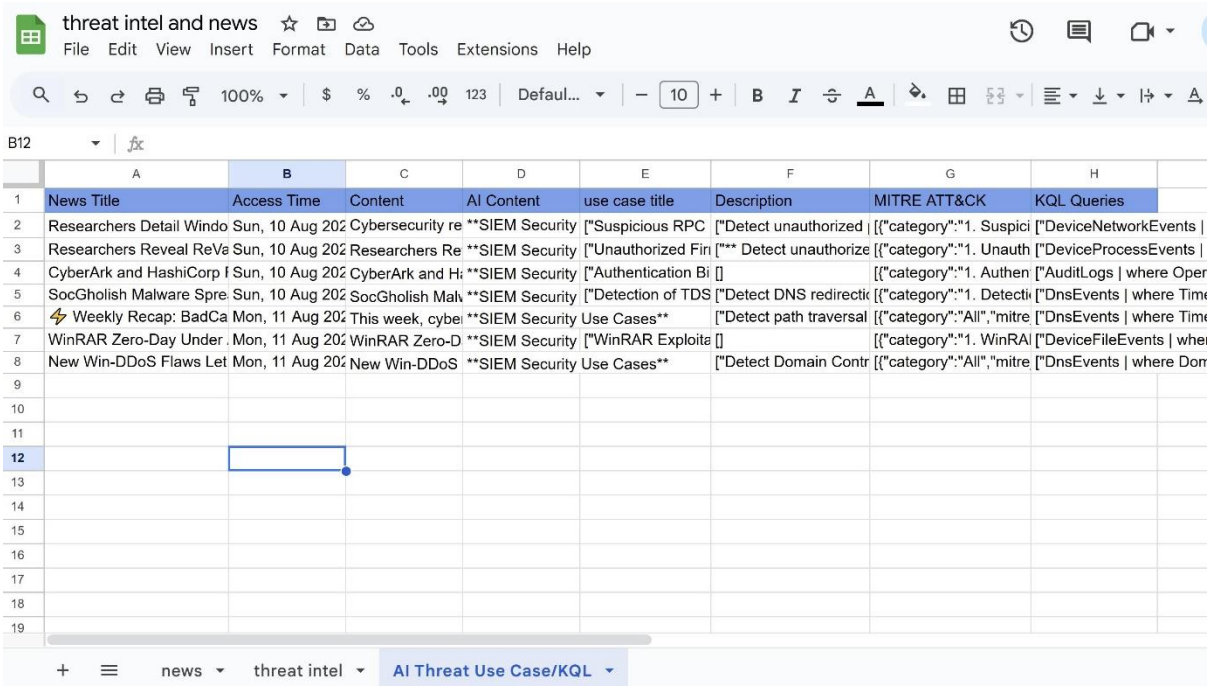

threat intel and news

File Edit View Insert Format Data Tools Extensions Help

A1 Title

	A	B	C
1	Title	Access Time	Webite
2	Researchers Detail Windows EPM Poisoning	Sun, 10 Aug 2025 12:31:1	https://thehackernews.com/2025/08/researchers-detail-windows-epm.html
3	Researchers Reveal ReVault Attack Targetin	Sun, 10 Aug 2025 12:31:1	https://thehackernews.com/2025/08/researchers-reveal-revault-attack.html
4	CyberArk and HashiCorp Flaws Enable Rem	Sun, 10 Aug 2025 12:31:1	https://thehackernews.com/2025/08/cyberark-and-hashicorp-flaws-enable.html
5	SocGholish Malware Spread via Ad Tools; De	Sun, 10 Aug 2025 12:31:1	https://thehackernews.com/2025/08/socgholish-malware-spread-via-ad-tools.html
6	⚡ Weekly Recap: BadCam Attack, WinRAR	Mon, 11 Aug 2025 12:04:3	https://thehackernews.com/2025/08/weekly-recap-badcam-attack-winrar-0-day.html
7	WinRAR Zero-Day Under Active Exploitation	Mon, 11 Aug 2025 12:04:3	https://thehackernews.com/2025/08/winrar-zero-day-under-active.html
8	New Win-DDoS Flaws Let Attackers Turn Pu	Mon, 11 Aug 2025 12:04:3	https://thehackernews.com/2025/08/new-win-ddos-flaws-let-attackers-turn.html
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			

news | threat intel | AI Threat Use Case/KQL


threat intel and news

File Edit View Insert Format Data Tools Extensions Help

B12

	A	B	C	D	E	F	G	H
1	News Title	Access Time	Content	AI Content	use case title	Description	MITRE ATT&CK	KQL Queries
2	Researchers Detail Windo	Sun, 10 Aug 202	Cybersecurity re	**SIEM Security	["Suspicious RPC	["Detect unauthorized	[{"category":"1. Suspici	["DeviceNetworkEvents |
3	Researchers Reveal ReVa	Sun, 10 Aug 202	Researchers Re	**SIEM Security	["Unauthorized Firi	["** Detect unauthorize	[{"category":"1. Unauth	["DeviceProcessEvents |
4	CyberArk and HashiCorp I	Sun, 10 Aug 202	CyberArk and Hi	**SIEM Security	["Authentication Bi	[]	[{"category":"1. Authen	["AuditLogs | where Oper
5	SocGholish Malware Spre	Sun, 10 Aug 202	SocGholish Mal	**SIEM Security	["Detection of TDS	["Detect DNS redirecti	[{"category":"1. Detecti	["DnsEvents | where Time
6	⚡ Weekly Recap: BadCa	Mon, 11 Aug 202	This week, cybe	**SIEM Security	Use Cases**	["Detect path traversal	[{"category":"All","mitre	["DnsEvents | where Time
7	WinRAR Zero-Day Under	Mon, 11 Aug 202	WinRAR Zero-D	**SIEM Security	["WinRAR Exploita	[]	[{"category":"1. WinRA	["DeviceFileEvents | whe
8	New Win-DDoS Flaws Let	Mon, 11 Aug 202	New Win-DDoS	**SIEM Security	Use Cases**	["Detect Domain Contr	[{"category":"All","mitre	["DnsEvents | where Dom
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								

news | threat intel | AI Threat Use Case/KQL