


DISCOVER THE HIDDEN VULNERABILITY INTELLIGENCE WITHIN CISA'S KEV CATALOG

(CISA IS NOT AFFILIATED WITH THIS TALK, I AM JUST A FAN)

(DATA AS OF JULY 26, 2024)

whoami

employer:  GREYNOISE [www.greynoise.io]

role: Sr. Director of Security Research and Detection Engineering

uptime: 21+ years

offline: Studying weather patterns & SCUBA/🦈 diving

WHAT IS KEV? | "KNOWN EXPLOITED VULNERABILITIES"

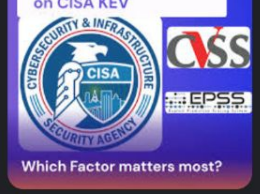
Criteria #1:
Assigned CVE ID

Criteria #2:
Active Exploitation

Criteria #3:
Clear Remediation Guidance

Comprehensive list of security vulnerabilities known to be actively exploited in the wild.
Certain government agencies are required by directive to address these within a set time frame.

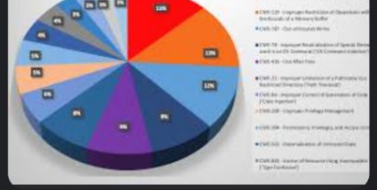
https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities
https://www.cisa.gov/known-exploited-vulnerabilities



Phoenix Security
How can you cross CISA K...

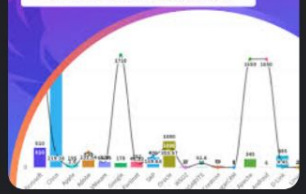
Phoenix Security
CWE and CISA KEV ...

Phoenix Security
The CISA KEV Ransomwar...



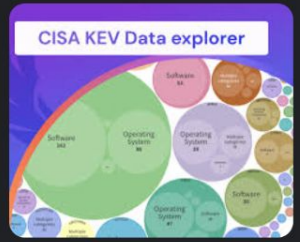
Phoenix Security
CWE and CISA KEV ...

Securin
Exploited Vulnerabilities (KEV) Catalog ...



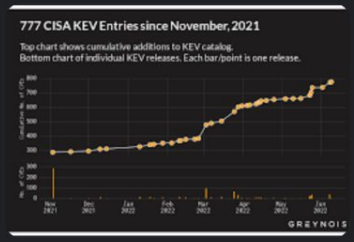
Phoenix Security
Phoenix Security - What is CISA...

Cyber Security Works
Decoding CISA KEV...



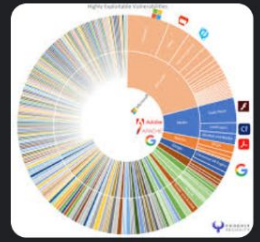
Phoenix Security
Phoenix Security - What is CISA...

Bitsight
Slicing through CISA's KEV Catalog ...



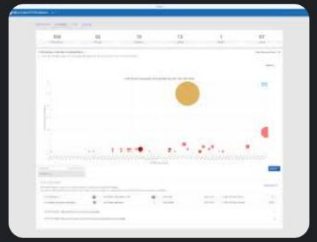
GreyNoise
CISA KEV ...

SOCRadar
2023 Review of the CISA Known Exploite...



Phoenix Security
How can you cross CISA K...

Securin
Known Exploited Vulnera...

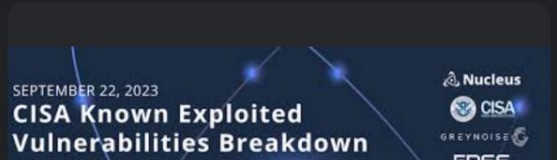


Product Documentation
CISA KEV report

Phoenix Security
The CISA KEV Ransomware Alert ...

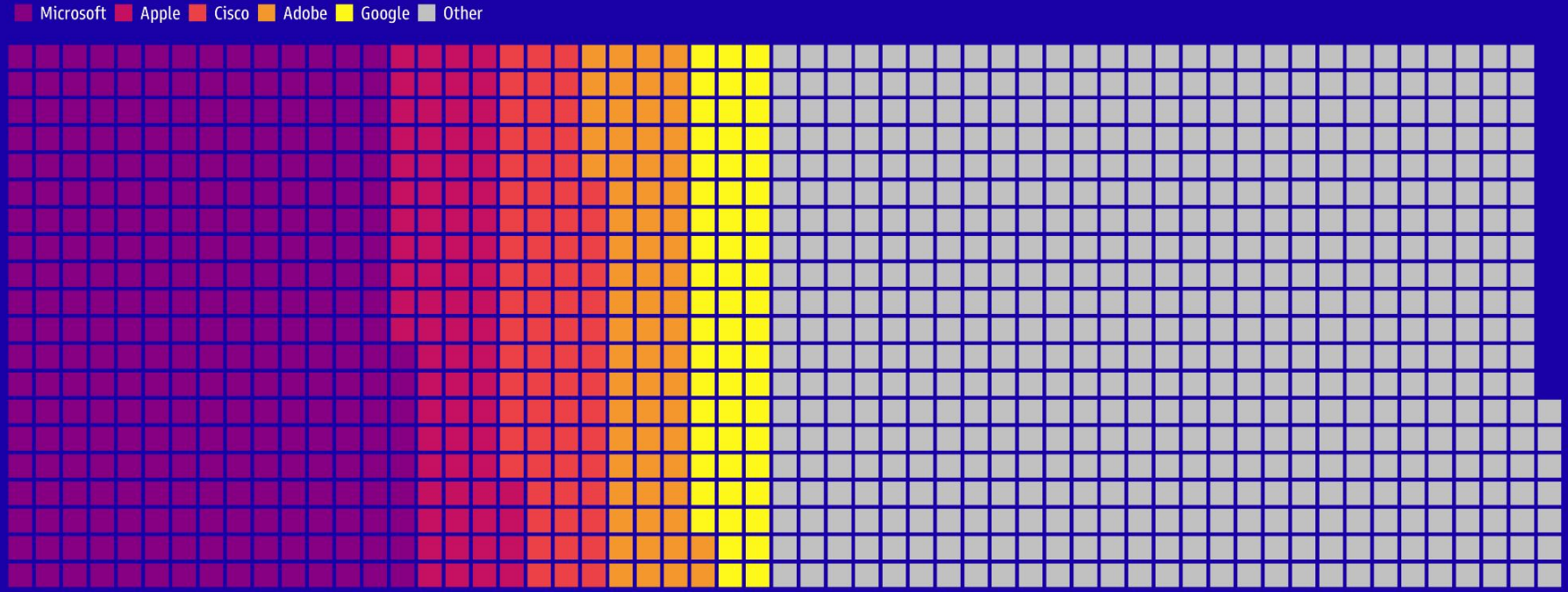
Nucleus Security
A Guide to CISA KEV Enrichment

FOSSA
Using the CISA Kev Catalog - FOSSA



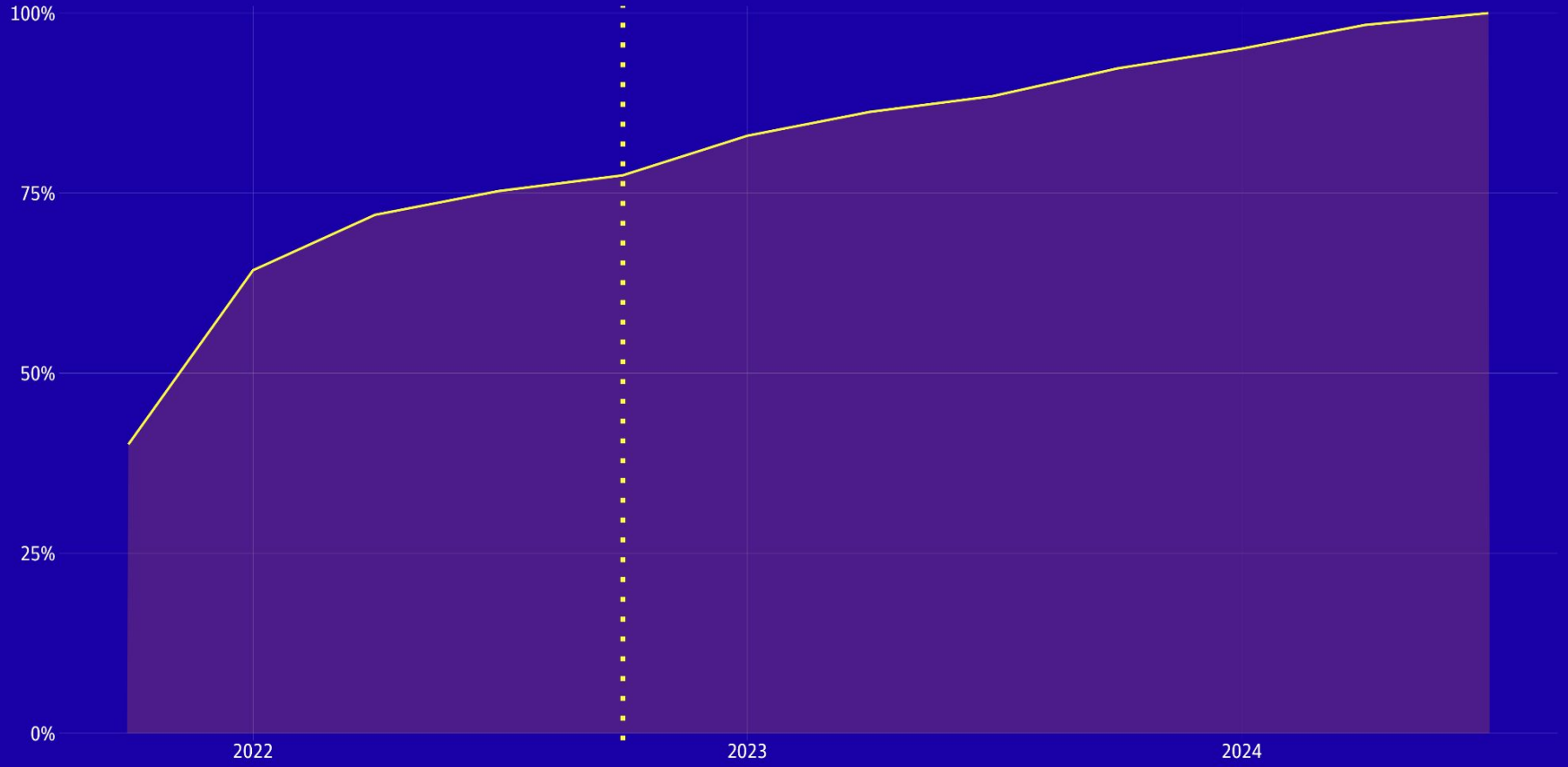
KEV Vendor Rogues Gallery

Five organizations make up just under 50% of KEV CVEs



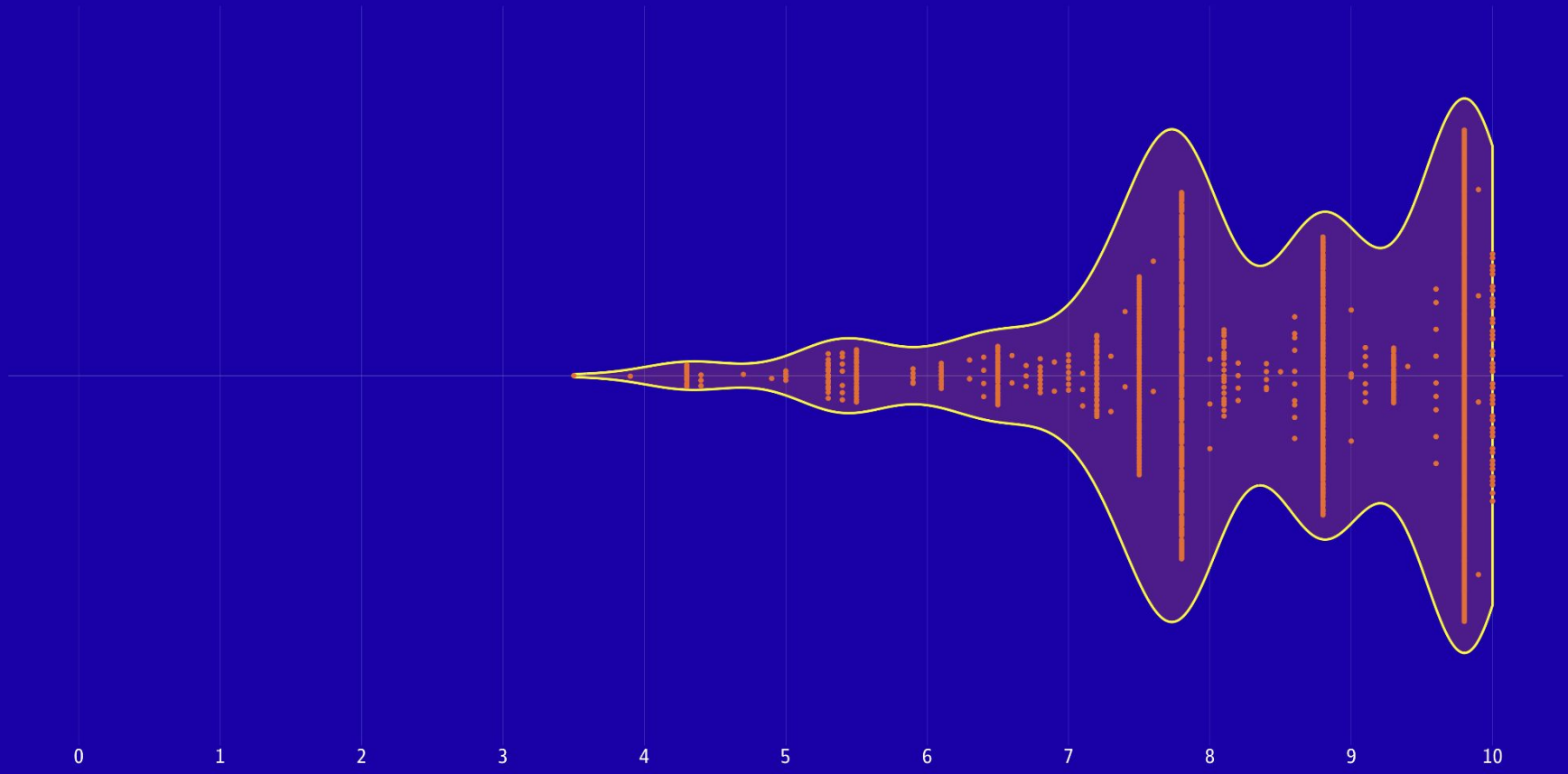
When Were Vendors First Added To KEV?

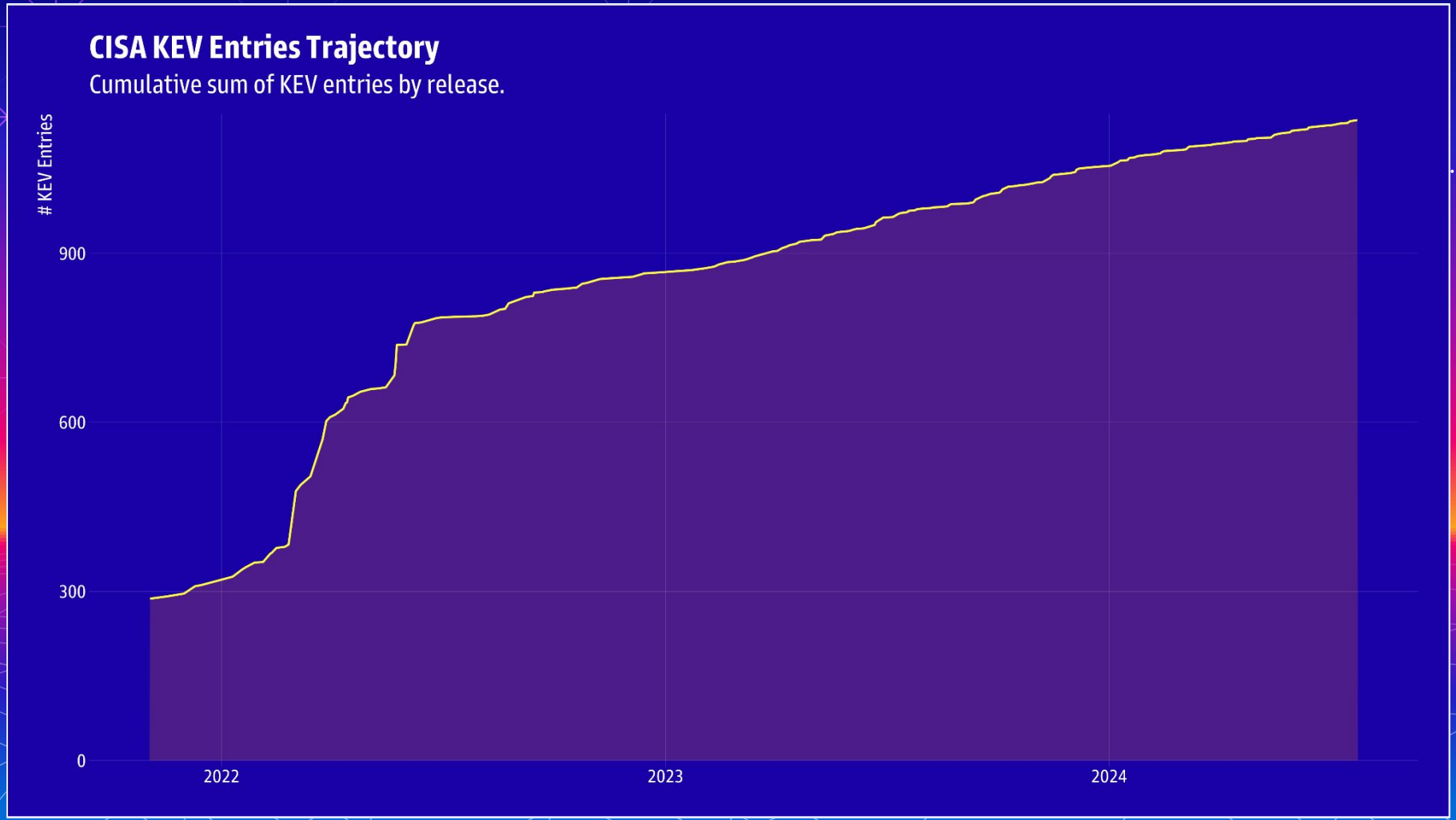
77% of the vendors currently on the list were added in the first 12 months of KEV's life.



CVSS Score Distribution Of KEV

CVSS Score (V2 when no V3 available)




CISA KEV Entries Trajectory
Cumulative sum of KEV entries by release.
KEV Entries
900
600
300
0
2022
2023
2024

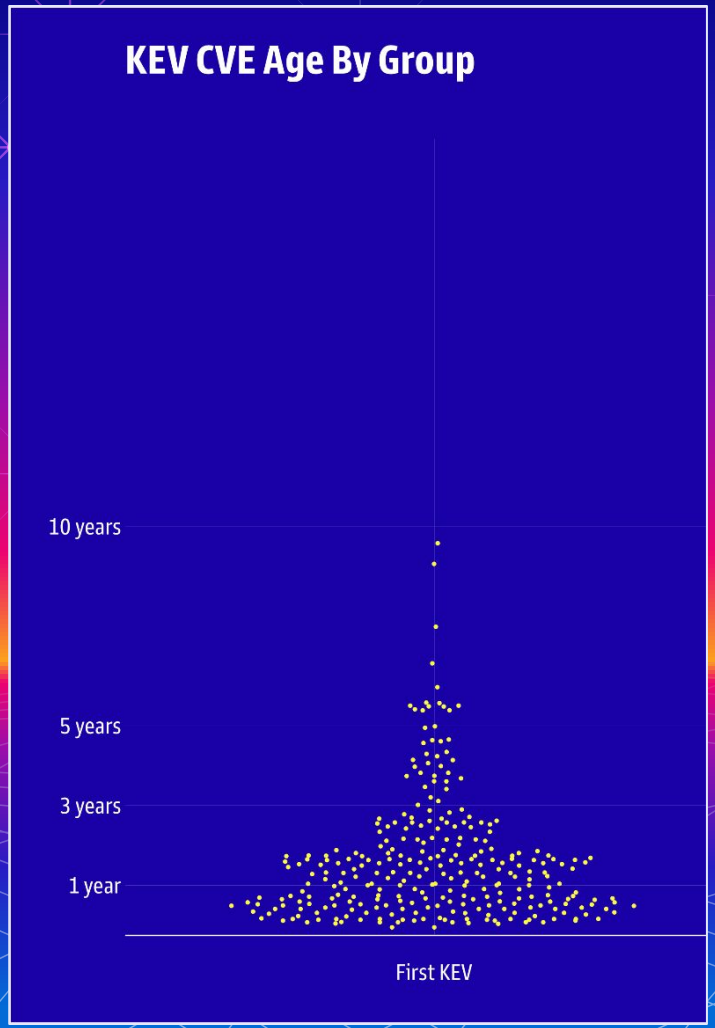
+1,000 DAYS

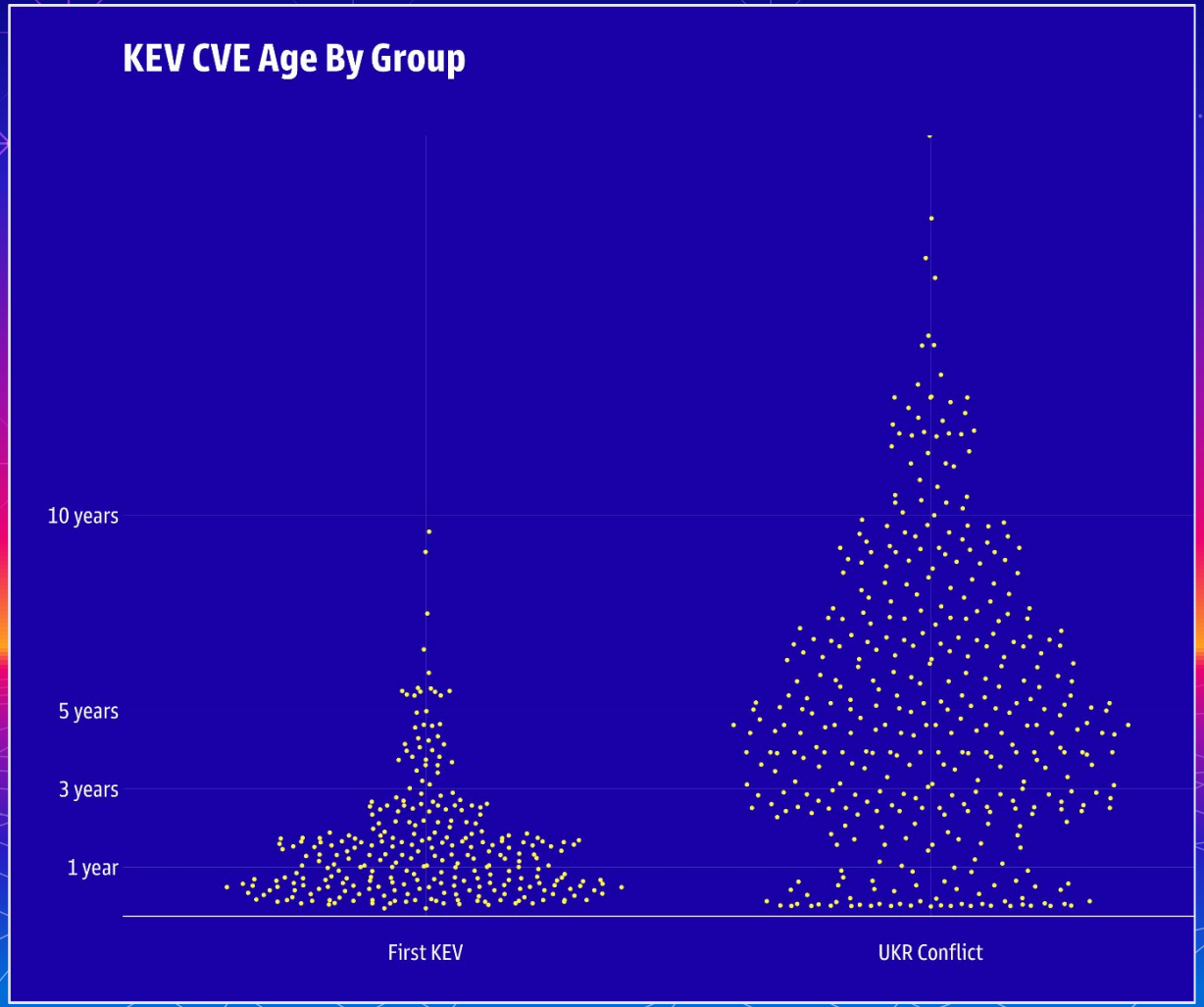
Average CVE Age Across All of KEV

OLDEST THREE ENTRIES

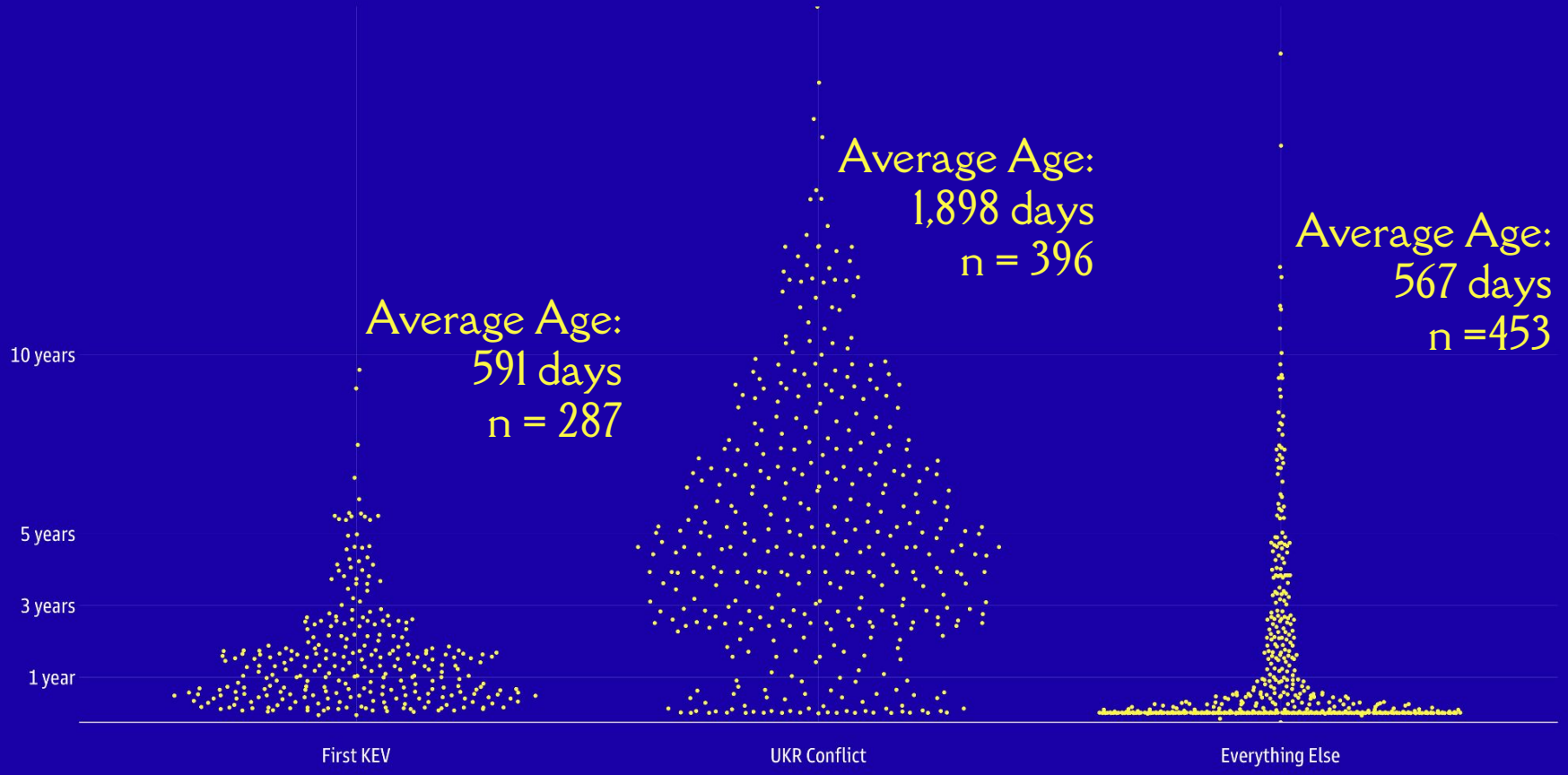
cveID	vendorProject	product	vulnerabilityName	dateAdded
CVE-2002-0367	Microsoft	Windows	Microsoft Windows Privilege Escalation Vulnerability	3/3/2022
CVE-2004-0210	Microsoft	Windows	Microsoft Windows Privilege Escalation Vulnerability	3/3/2022
CVE-2004-1464	Cisco	IOS	Cisco IOS Denial-of-Service Vulnerability	5/19/2023

ACCOMMODATE THE OUTLIERS

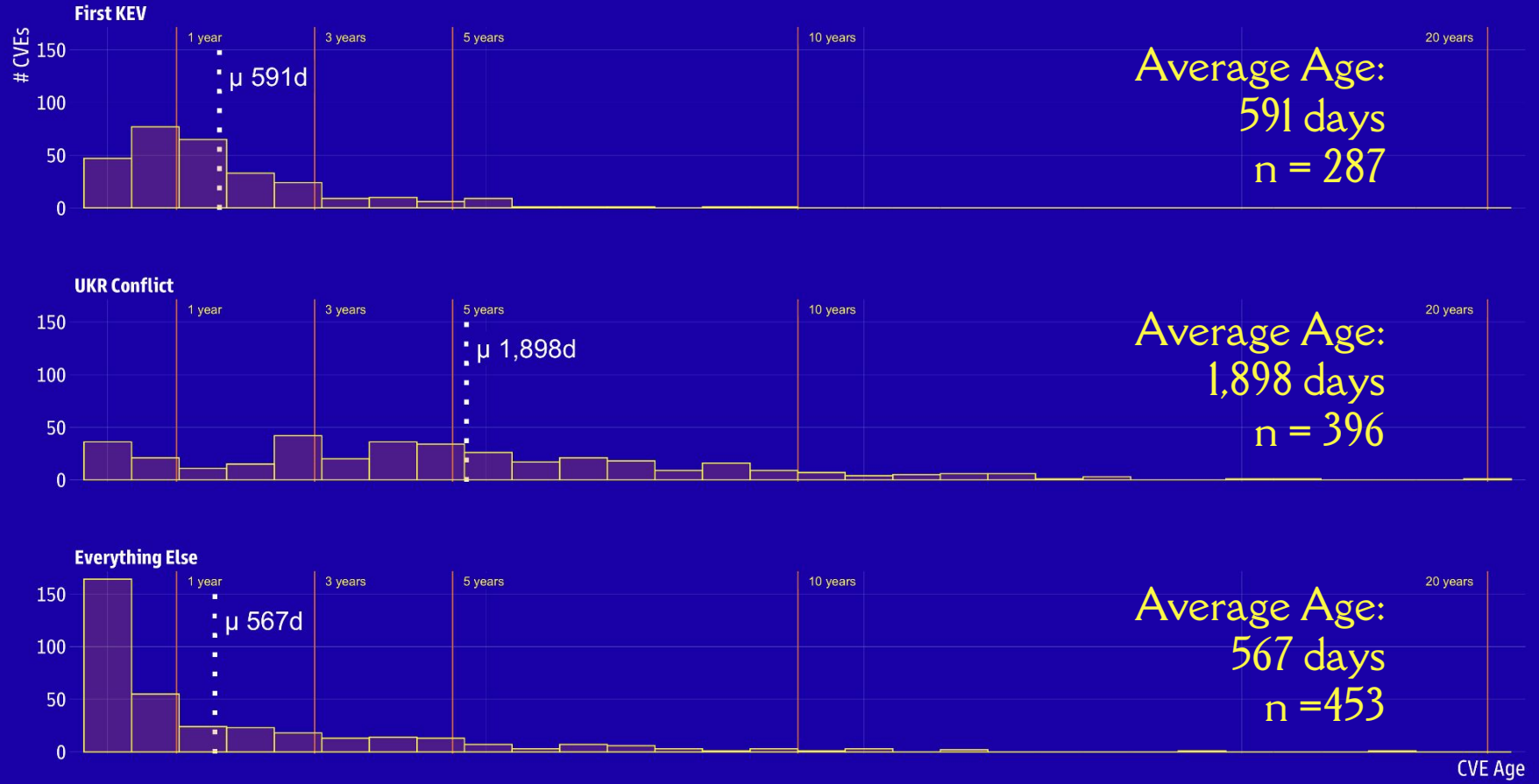

KEV CVE Age By Group
10 years
5 years
3 years
1 year
First KEV

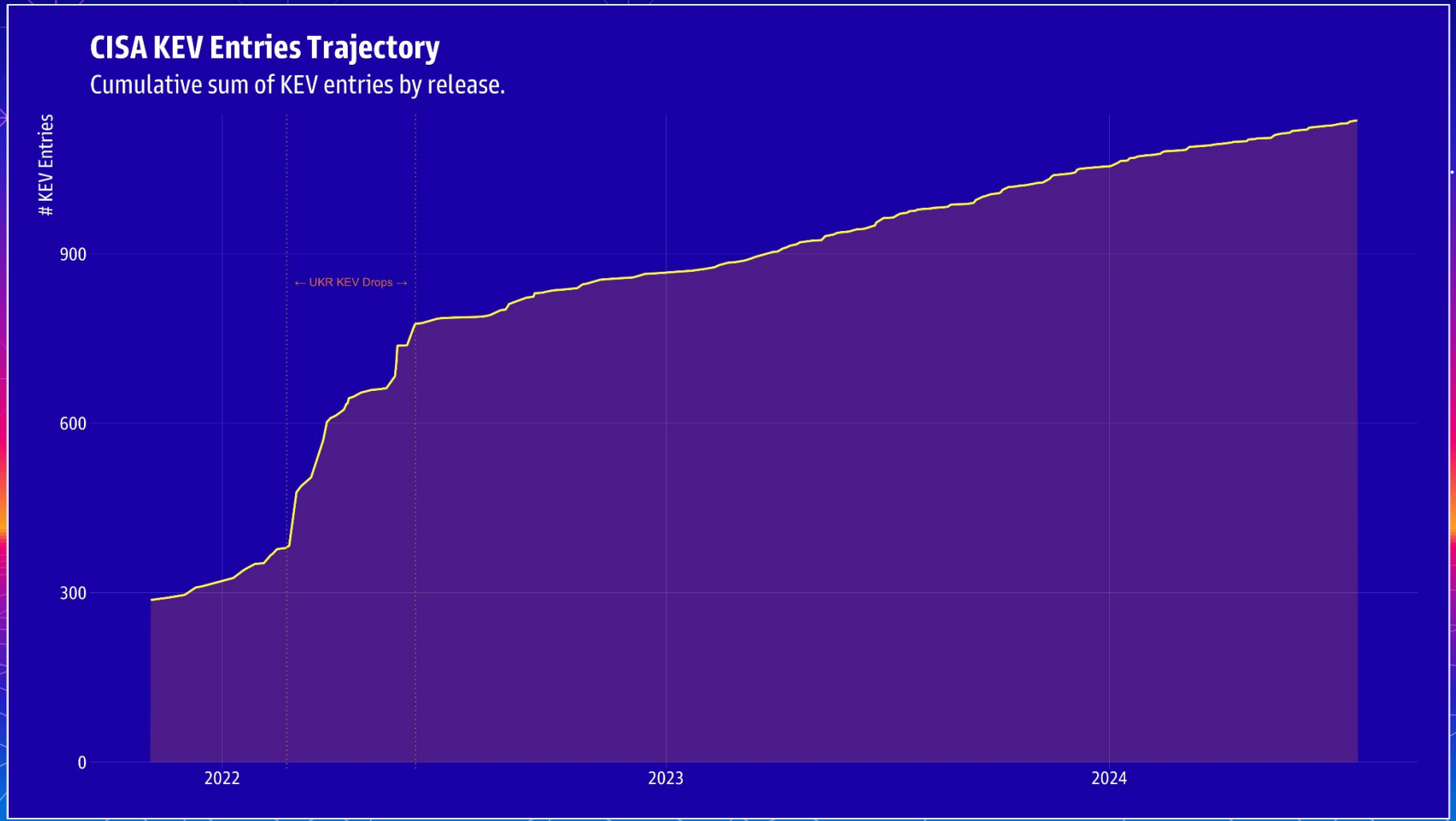

KEV CVE Age By Group
10 years
5 years
3 years
1 year
First KEV
UKR Conflict

KEV CVE Age By Group

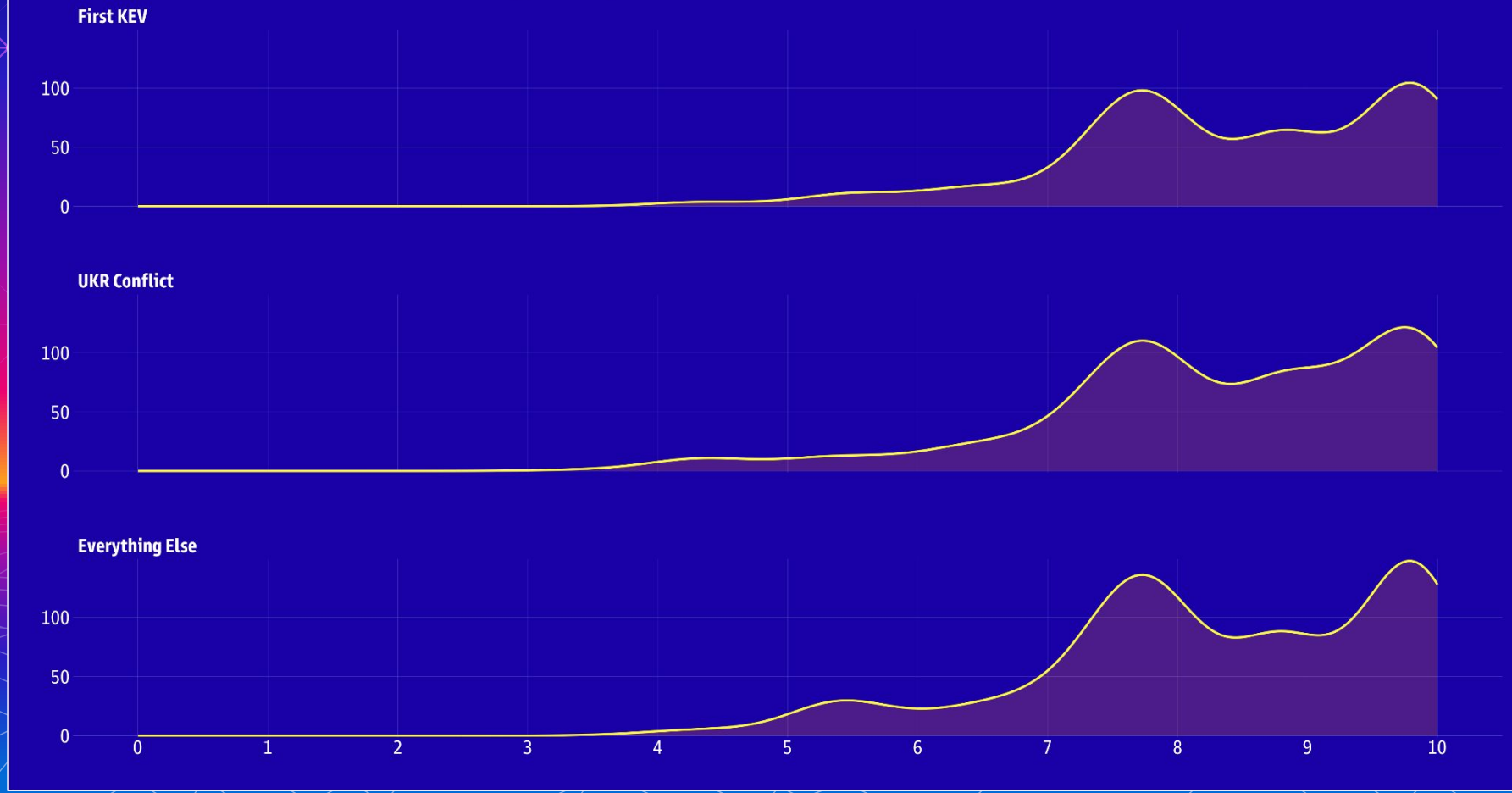


CVE Age Distribution Of KEV By Group

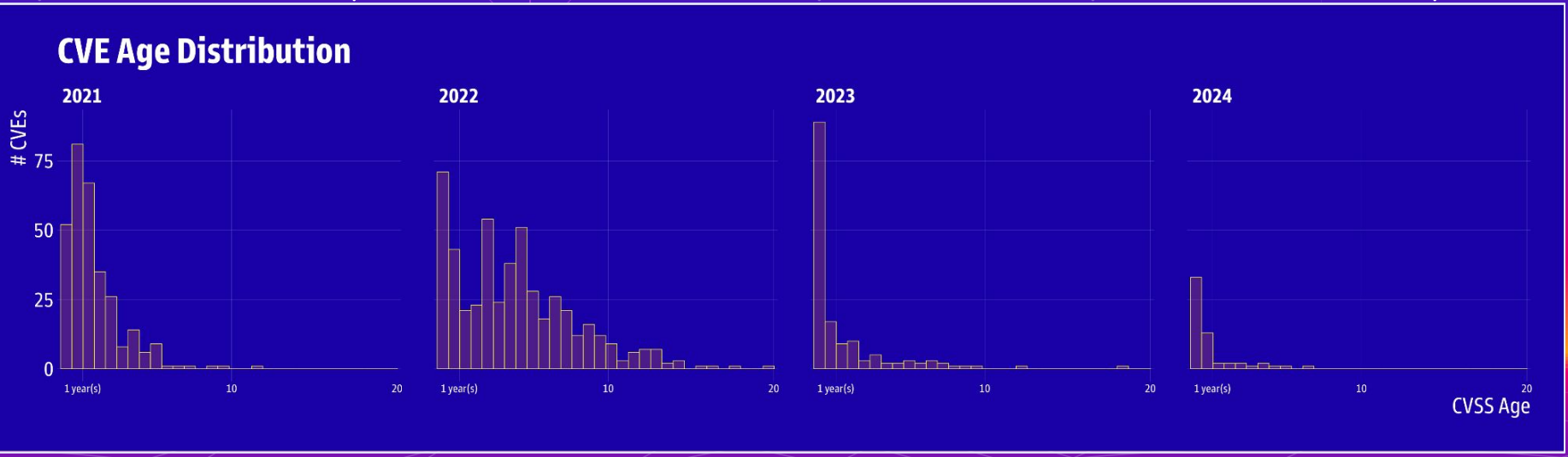



CISA KEV Entries Trajectory
Cumulative sum of KEV entries by release.
KEV Entries
900
600
300
0
← UKR KEV Drops →
2022
2023
2024

CVSS Score Distribution Of KEV By Group



IS THE KEV CVE AGE TRENDING  OR  ?


CVE Age Distribution
2021
2022
2023
2024
CVEs
75
50
25
0
1 year(s)
10
20
CVSS Age

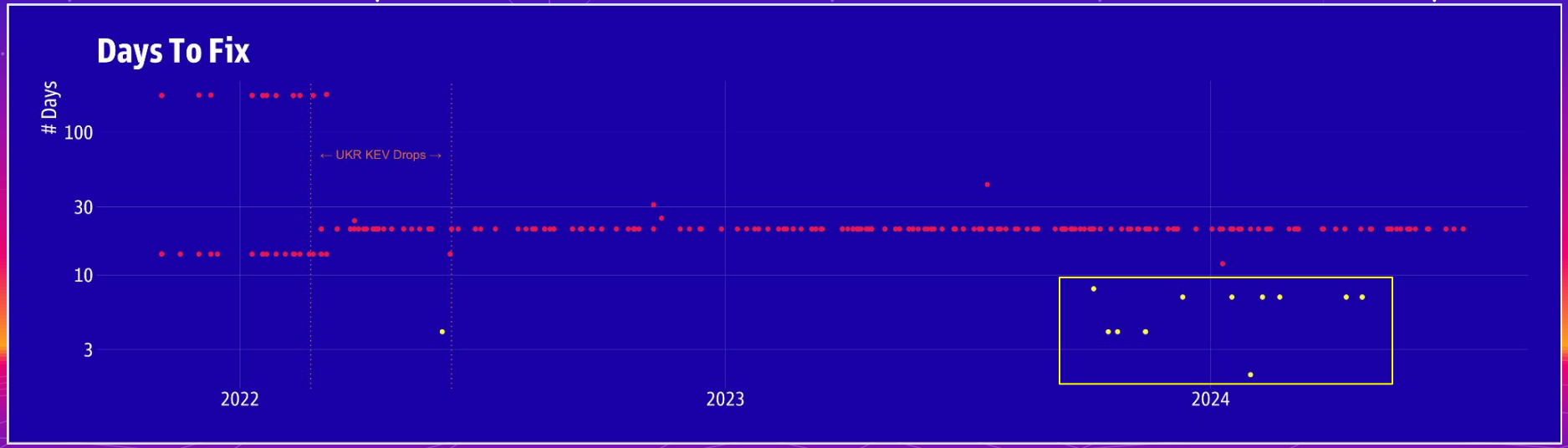
IS THE KEV DATA STATIC?

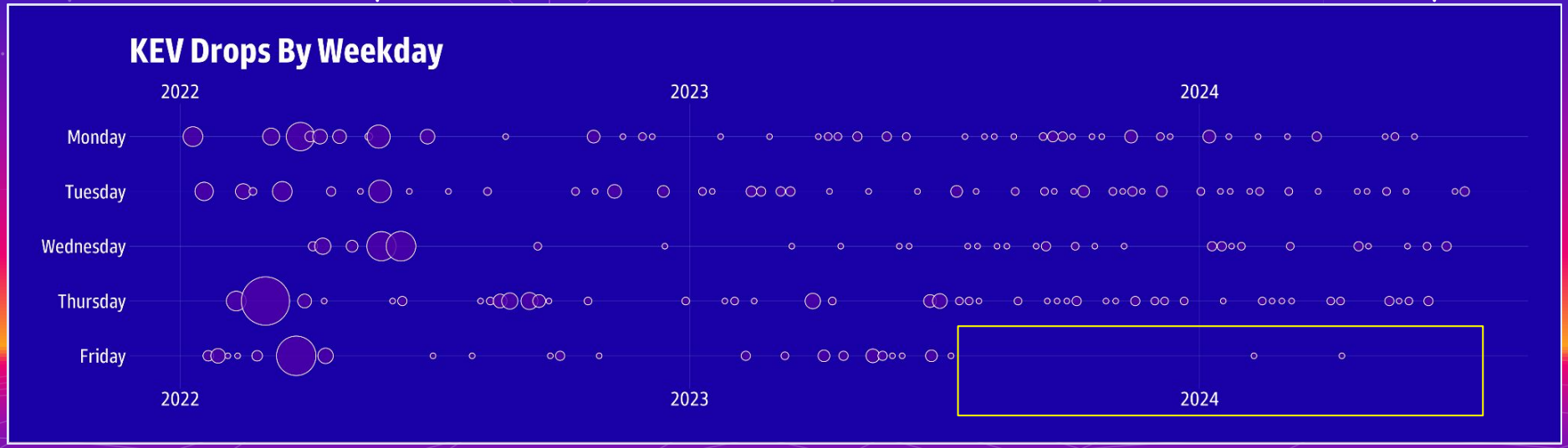
	CVE	KEV'd Date	Unknown Set	Known Set	Days Between Added & Unknown	Days Between Added & Known
1	CVE-2024-1709	2/22/2024	2/22/2024	2/23/2024	1	1
2	CVE-2023-35082	1/18/2024	1/19/2024	1/23/2024	5	4
3	CVE-2023-41265	12/7/2023	12/7/2023	12/12/2023	5	5
4	CVE-2023-41266	12/7/2023	12/7/2023	12/12/2023	5	5
5	CVE-2023-22518	11/7/2023	11/7/2023	11/13/2023	6	6
6	CVE-2023-46604	11/2/2023	11/2/2023	11/13/2023	11	11
7	CVE-2023-24955	3/26/2024	3/26/2024	4/8/2024	13	13
8	CVE-2023-48788	3/25/2024				
9	CVE-2023-22527	1/24/2024				
10	CVE-2013-3993	5/25/2022				
11	CVE-2017-0147	5/24/2022				
12	CVE-2017-11882	11/3/2021				
13	CVE-2017-18362	5/24/2022	10/12/2023	11/13/2023	538	32
14	CVE-2018-13374	9/8/2022	10/12/2023	11/13/2023	431	32
15	CVE-2018-13382	1/10/2022	10/12/2023	11/13/2023	672	32
16	CVE-2018-13383	1/10/2022	10/12/2023	11/13/2023	672	32
17	CVE-2018-19320	10/24/2022	10/12/2023	11/13/2023	385	32
18	CVE-2018-19321	10/24/2022	10/12/2023	11/13/2023	385	32
19	CVE-2018-19322	10/24/2022	10/12/2023	11/13/2023	385	32
20	CVE-2018-19323	10/24/2022	10/12/2023	11/13/2023	385	32
21	CVE-2018-20753	4/13/2022	10/12/2023	11/13/2023	579	32

knownRansomwareCampaignUse has **later** changed to known 41 times

	CVE	KEV'd Date	Unknown Set	Known Set	Days Between Added & Unknown	Days Between Added & Known
22	CVE-2019-11510	11/3/2021	10/12/2023	11/13/2023	740	32
23	CVE-2019-11539	11/3/2021	10/12/2023	11/13/2023	740	32
24	CVE-2021-22893	11/3/2021	10/12/2023	11/13/2023	740	32
25	CVE-2022-1388	5/10/2022	10/12/2023	11/13/2023	552	32
26	CVE-2022-40684	10/11/2022	10/12/2023	11/13/2023	398	32
27	CVE-2022-47986	2/21/2023	10/12/2023	11/13/2023	265	32
28	CVE-2023-0669	2/10/2023	10/12/2023	11/13/2023	276	32
					61	32
					39	32
					83	32
					111	32
					117	32
34	CVE-2023-42793	10/4/2023	10/12/2023	11/13/2023	40	32
35	CVE-2023-4966	10/18/2023	10/18/2023	1/3/2024	77	77
36	CVE-2024-27198	3/7/2024	3/8/2024	5/30/2024	84	83
37	CVE-2023-29357	1/10/2024	1/10/2024	4/8/2024	89	89
38	CVE-2023-38831	8/24/2023	10/12/2023	2/17/2024	177	128
39	CVE-2023-47246	11/13/2023	11/13/2023	4/6/2024	145	145
40	CVE-2021-3129	9/18/2023	10/12/2023	4/10/2024	205	181
41	CVE-2023-38035	8/22/2023	10/12/2023	7/16/2024	329	278

KEV'S SECRET PRIORITIZATION, EXPOSED


Days To Fix
Days
100
30
10
3
← UKR KEV Drops →
2022
2023
2024


KEV Drops By Weekday
2022
2023
2024
Monday
Tuesday
Wednesday
Thursday
Friday
2022
2023
2024

TLDR;

Looking beyond the sums and averages in the KEV catalog, it is a very strong early signal to use for vulnerability prioritization.

The KEV catalog isn't exactly static.

I'd love to see more attention to changes as well as additions.

Weekday of the KEV additions, in addition to the time-to-fix are a way to prioritize within the KEV.

Can't predict the next KEV, so if you must:

Vendor already on list &

AV:N/PR:N/UI:N

SPECIAL THANKS TO

Bob Rudis

Insane data and visualization skills

Feedly*

Their enterprise edition API is so well done it simplified this analysis exponentially

*(can we get a discount now?)

You can find me, this presentation, dataset, and more at:

https://linktr.ee/glennthorp e