STORM WATCH

CYBERSECURITY NEWS

Dateline: 2024-03-19

LIKE

SUBSCRIBE

Storm ⚡ Watch by GreyNoise Intelligence

GreyNoise Intelligence

TECHNOLOGY · UPDATED WEEKLY

GreyNoise Storm ⚡ Watch is a weekly podcast and livestream hosted by GreyNoise Intelligence (https://www.greynoise.io), a cybersecurity company that focuses on understanding internet noise. The show features hosts b MORE

https://StormWatch.ing

LEAVE A COMMENT

SHARE

STORM WATCH

CYBERSECURITY NEWS

CYBERSIDE CHAT

https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-university-oxford-promise-and

News

All News

Blogs

Photo Galleries

Podcasts

Press Releases

SPEECH

Deputy Attorney General Lisa O. Monaco Delivers Remarks at the University of Oxford on the Promise and Peril of AI

Wednesday, February 14, 2024

Every new technology is a double-edged sword, but AI may be the sharpest blade yet. It has the potential to be an indispensable tool to help identify, disrupt, and deter criminals, terrorists, and hostile nation-states from doing us harm.

So far, we've just scratched the surface of how AI can strengthen the Justice Department's work. But we've already deployed AI:

- To classify and trace the source of opioids and other drugs.
- To help us triage and understand the more than one million tips submitted to the FBI by the public every year.
- And to synthesize huge volumes of evidence collected in some of our most significant cases, including January 6.

Yet for all the promise it offers, AI is also accelerating risks to our collective security.

We know it has the potential to amplify existing biases and discriminatory practices.

It can expedite the creation of harmful content, including child sexual abuse material.

It can arm nation-states with tools to pursue digital authoritarianism, accelerating the spread of disinformation and repression.

And we've already seen that AI can lower the barriers to entry for criminals and embolden our adversaries. It's changing how crimes are committed and who commits them — creating new opportunities for wanna-be hackers and supercharging the threat posed by the most sophisticated cybercriminals.

Election security is an area where I'm particularly focused on the potential risks posed by AI.

The upcoming elections crack open a window for foreign adversaries and bad actors to divide and mislead us.

- They can radicalize users on social media with incendiary content created with generative AI — accelerating online harassment, hate, and disinformation.
- They can misinform voters by impersonating trusted sources and spreading deepfakes — easy to create, and often hard to rapidly detect.
- And with chatbots, fake images and even cloned voices spreading falsehoods about elections, they can deny people their most fundamental of rights — to have their voices heard as voters.

We've already seen the misuse of AI play out in elections from Chicago and New Hampshire to Slovakia. And I fear it's just the start.

Left without guardrails, AI poses immense challenges for democracies around the world.

So, we're at an inflection point with AI. We have to move quickly to identify, leverage, and govern its positive uses while taking measures to minimize its risks.

Time (h)

Download : Download high-res image (180KB)

Download : Download full-size image

https://www.sciencedirect.com/science/article/abs/pii/S2468023024002402

Certainly, here is a possible introduction for your topic:Lithium-metal batteries are promising candidates for high-energy-density rechargeable batteries due to their low electrode potentials and high theoretical capacities [1], [2]. However, during the cycle, dendrites forming on the lithium metal anode can cause a short circuit, which can affect the safety and life of the battery [3], [4], [5], [6], [7], [8], [9]. Therefore, researchers are indeed focusing on various aspects such as negative electrode structure [10], electrolyte additives [11], [12], SEI film construction [13], [14], and collector modification [15] to inhibit the formation of lithium dendrites. However, using a separator with high mechanical strength and chemical stability is another promising approach to prevent dendrites from infiltrating the cathode. By incorporating a separator with high mechanical strength, it can act as a physical barrier to impede the growth of dendrites. This barrier can withstand the mechanical stress exerted by the dendrites during battery operation, preventing them from reaching the cathode and causing short circuits or other safety issues. Moreover, chemical stability of the separator is equally important as it ensures that the separator remains intact and does not react or degrade in the presence of the electrolyte or other battery components. A chemically stable separator helps to

Science of Science
@MishaTeplitskiy

Lots of people in CS are (almost surely) GPT-ing their peer reviews

https://arxiv.org/abs/2403.07183

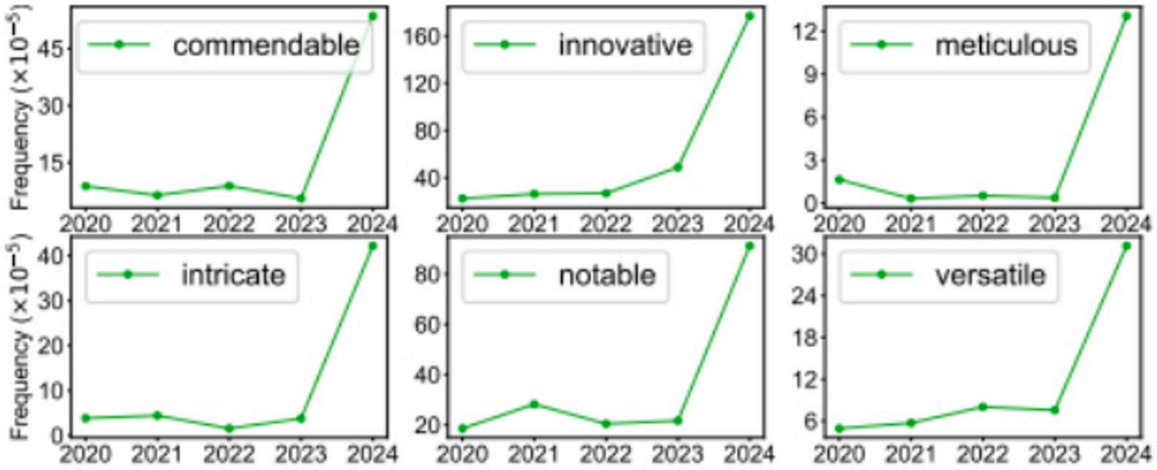


Figure 1: **Shift in Adjective Frequency in *ICLR* 2024 Peer Reviews.** We find a significant shift in the frequency of certain tokens in *ICLR* 2024, with adjectives such as "commendable", "meticulous", and "intricate" showing 9.8, 34.7, and 11.2-fold increases in probability of occurring in a sentence. We find a similar trend in *NeurIPS* but not in *Nature Portfolio* journals. Supp. Table 2 and Supp. Figure 12 in the Appendix provide a visualization of the top 100 adjectives produced disproportionately by AI.

2:38 PM · Mar 17, 2024 · **128.1K** Views

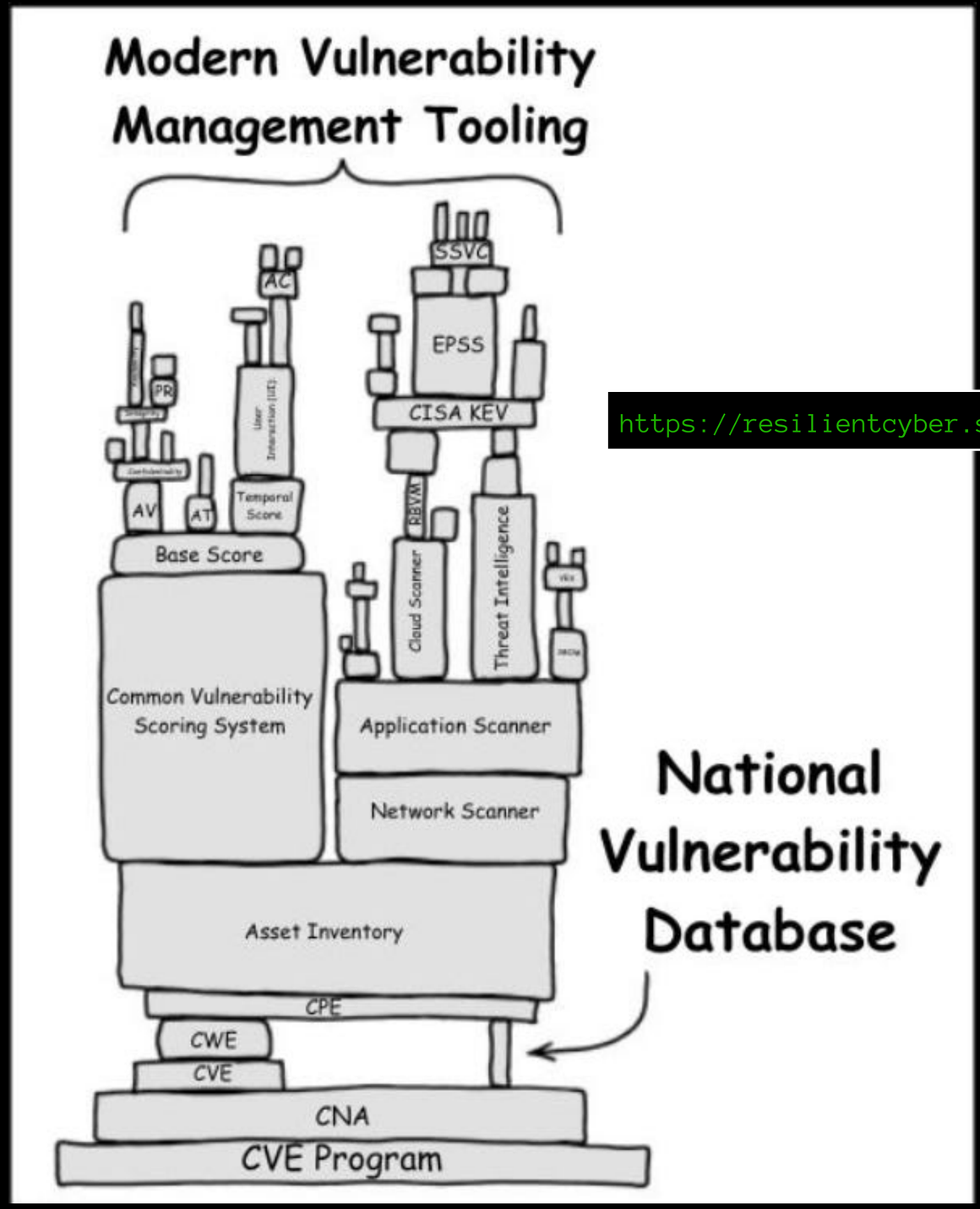
STORM WATCH

CYBERSECURITY NEWS

CYBER SPOTLIGHT


NIST
NATIONAL VULNERABILITY
DATABASE
NVD


NVD



https://resilientcyber.substack.com/p/death-knell-of-the-nvd

https://www.linkedin.com/posts/jgamblin_vulnerabilitymanagement-cve-nvd-activity-7172701454816669696-nw00/

Jerry Gamblin • 1st

Principal Engineer at Cisco Threat Detection & Respo...

1w •

This afternoon, I looked into the delays in processing vulnerabilities at the National Vulnerability Database (NVD). Currently, there's a significant backlog. They have yet to address nearly 2,500 Common Vulnerabilities and Exposures (CVEs), accounting for about 40% of all CVEs released this year. If we focus on the period starting from February 15th, when the NVD posted a notice about the issue, the situation appears more critical. Since that date, they've only managed to process 59 CVEs. This means there's an outstanding backlog of over 2,150 CVEs, making up more than 90% of all the CVEs published in that timeframe.

#vulnerabilitymanagement #CVE #nvd

https://nvd.nist.gov/vuln/data-feeds

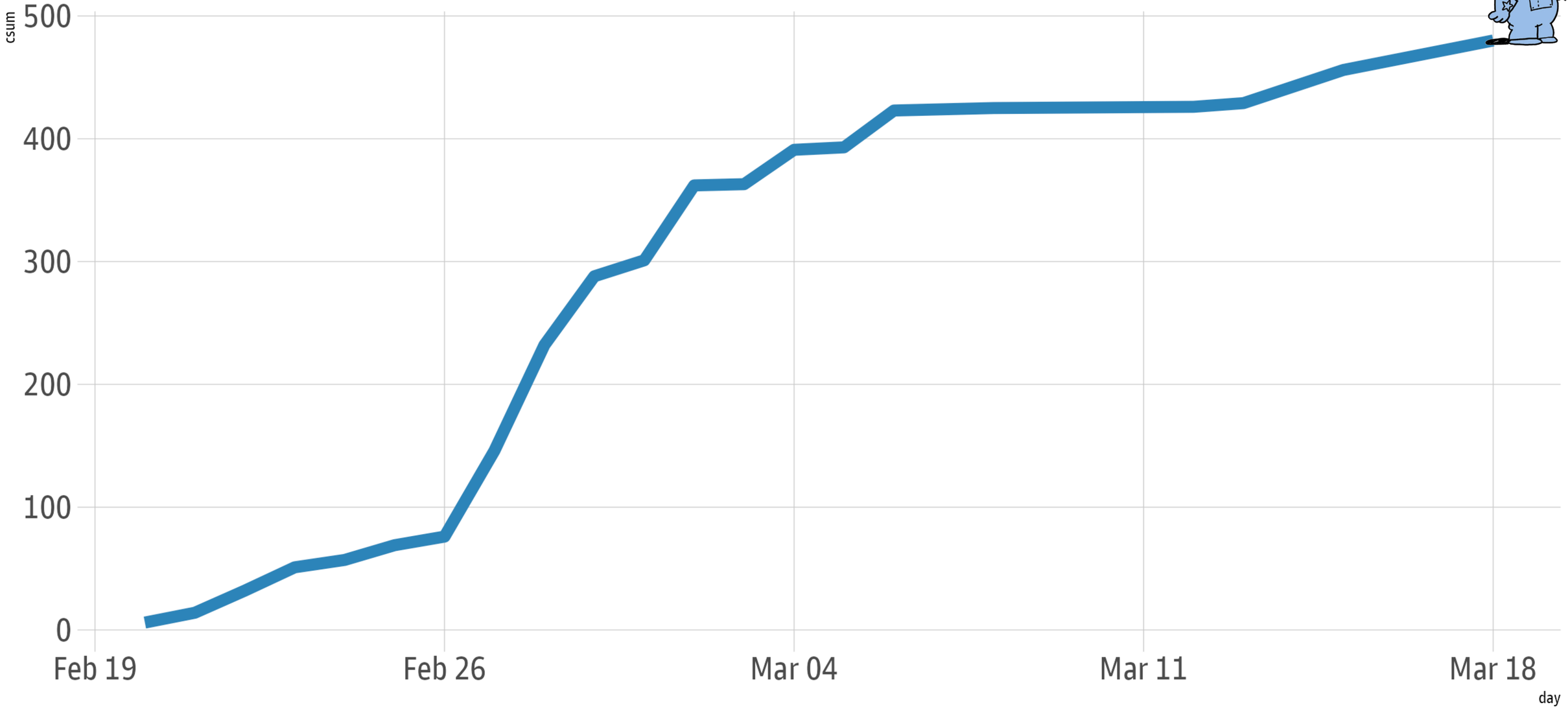
NOTICE

NIST is currently working to establish a consortium to address challenges in the NVD program and develop improved tools and methods. You will temporarily see delays in analysis efforts during this transition. We apologize for the inconvenience and ask for your patience as we work to improve the NVD program.

https://nvd.nist.gov/vuln/data-feeds

The NVD plans to retire all legacy data feeds while guiding any remaining data feed users to updated application-programming interfaces (APIs). APIs have many benefits over data feeds and have been the proven and preferred approach to web-based automation for over a decade. For additional information on the NVD API, please visit the developers pages. Click here for more information on the retirement timeline.

Linux Kernel CVE Submissions Since February 20, 2024



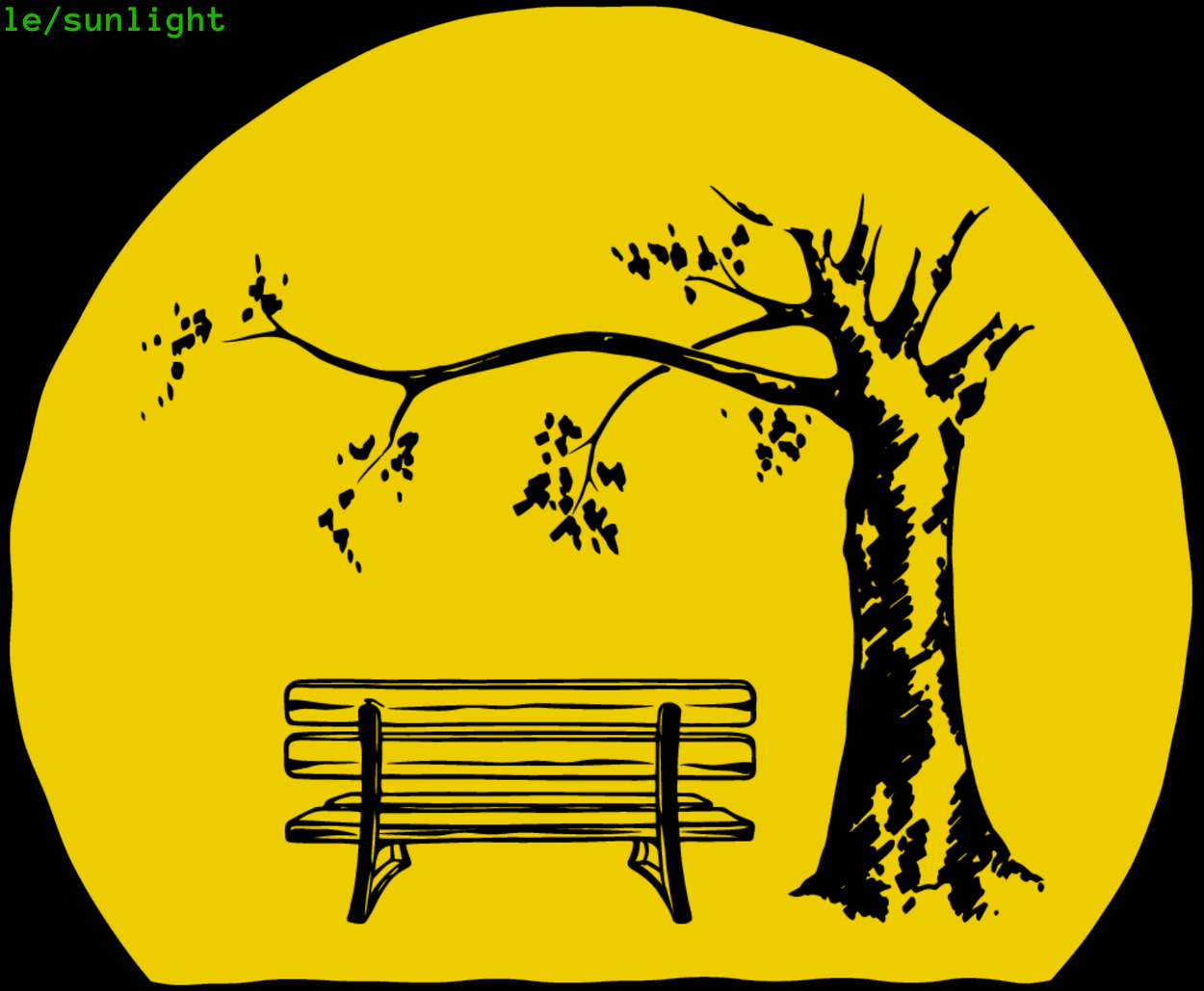
STORM WATCH

CYBERSECURITY NEWS

TOOL TIME

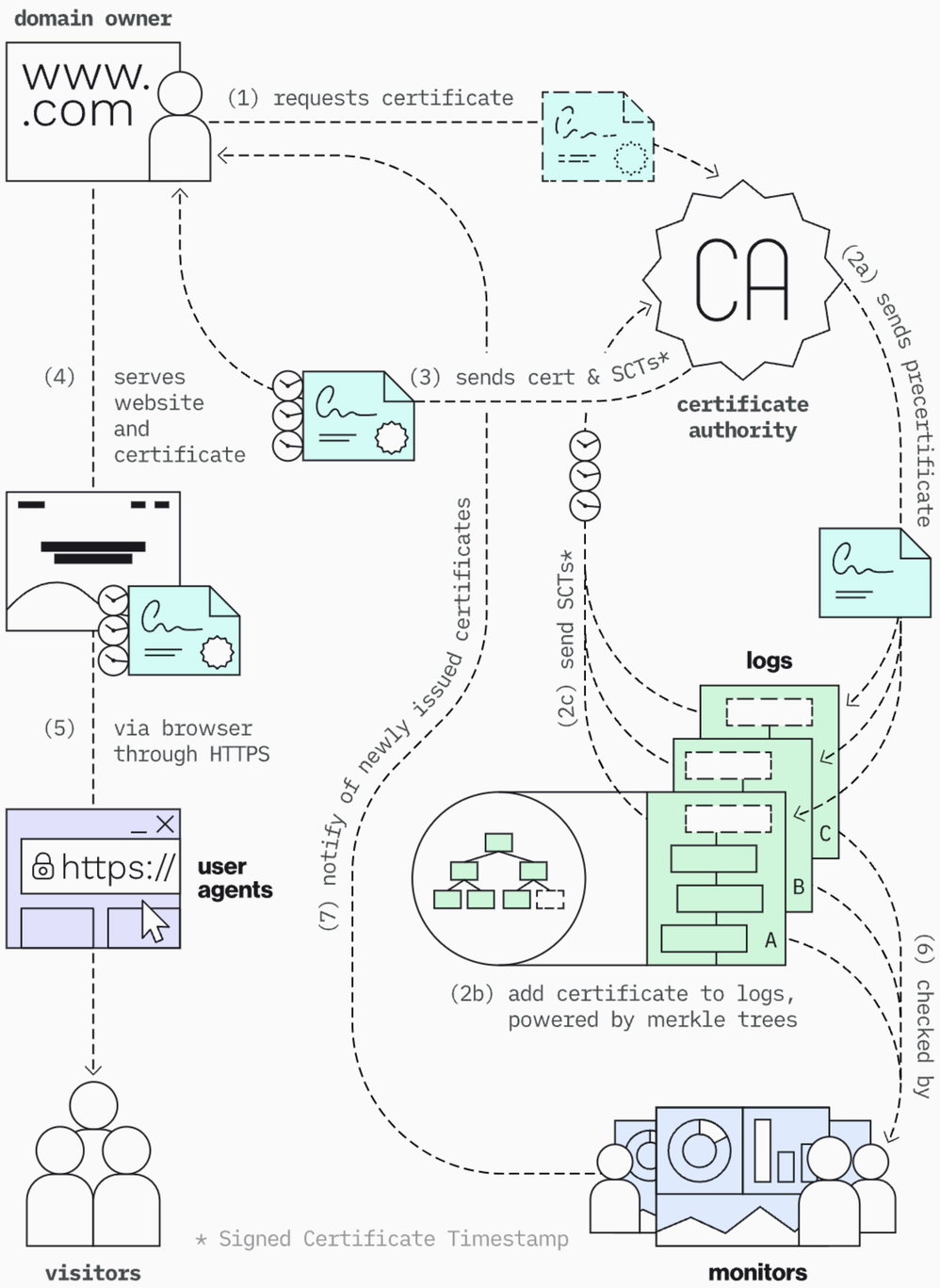
https://github.com/FiloSottile/sunlight

https://sunlight.dev/



SUNLIGHT

https://letsencrypt.org/2024/03/14/introducing-sunlight.html



- Website owner requests a certificate from the Certificate Authority (CA)
- CA issues a precertificate
- CA sends precertificates to logs
- Precertificates are added to the logs
- Logs return SCTs to the CA
- CAs send the certificate to the domain owner
- Browsers and user agents help keep the web secure
- Logs are cryptographically monitored

Previous Scaling Method

- Utilized a relational database for storage.
- Employed temporal sharding, splitting each year's data into separate databases.
- Later reduced shard sizes to six-month periods to manage growth.

New Method with Sunlight

- Abandons relational databases for storage in favor of static, easily cached tiles.
- Tiles contain 256 elements each, either as hashes at a certain tree height or certificates at the leaf level.
- Enables horizontal scaling by serving tiles directly from cloud object storage like S3, reducing costs and complexity.

- Google ‘Argon2023’ log (https://ct.googleapis.com/logs/argon2023/)
- Google ‘Argon2024’ log (https://ct.googleapis.com/logs/us1/argon2024/)
- Google ‘Xenon2023’ log (https://ct.googleapis.com/logs/xenon2023/)
- Google ‘Xenon2024’ log (https://ct.googleapis.com/logs/eu1/xenon2024/)
- Cloudflare ‘Nimbus2023’ Log (https://ct.cloudflare.com/logs/nimbus2023/)
- Cloudflare ‘Nimbus2024’ Log (https://ct.cloudflare.com/logs/nimbus2024/)
- DigiCert Yeti2024 Log (https://yeti2024.ct.digicert.com/log/)
- DigiCert Yeti2025 Log (https://yeti2025.ct.digicert.com/log/)
- DigiCert Nessie2023 Log (https://nessie2023.ct.digicert.com/log/)
- DigiCert Nessie2024 Log (https://nessie2024.ct.digicert.com/log/)
- DigiCert Nessie2025 Log (https://nessie2025.ct.digicert.com/log/)
- Sectigo ‘Sabre’ CT log (https://sabre.ct.comodo.com/)
- Let’s Encrypt ‘Oak2023’ log (https://oak.ct.letsencrypt.org/2023/)
- Let’s Encrypt ‘Oak2024H1’ log (https://oak.ct.letsencrypt.org/2024h1/)
- Let’s Encrypt ‘Oak2024H2’ log (https://oak.ct.letsencrypt.org/2024h2/)
- Trust Asia Log2023 (https://ct.trustasia.com/log2023/)
- Trust Asia Log2024-2 (https://ct2024.trustasia.com/log2024/)

https://source.chromium.org/chromium/chromium/src/+/main:components/certificate_transparency/data/log_list.json

STORM WATCH

CYBERSECURITY NEWS

SHAMELESS SELF-PROMOTION

censys

Products Solutions Federal Resources Company Censys Search Request a Demo

BLOGS

Key Insights from The 2024 State of Threat Hunting Report

https://censys.com/key-insights-from-the-2024-state-of-threat-hunting-report/

https://www.greynoise.io/blog/where-are-they-now-starring-atlassians-confluence-cve-2023-22527

LABS VULNERABILITIES

Where are they now? Starring: Atlassian's Confluence CVE-2023-22527

Ron Bowes | March 13, 2024

STORM WATCH

CYBERSECURITY NEWS

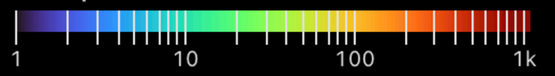
TAG ROUND-UP

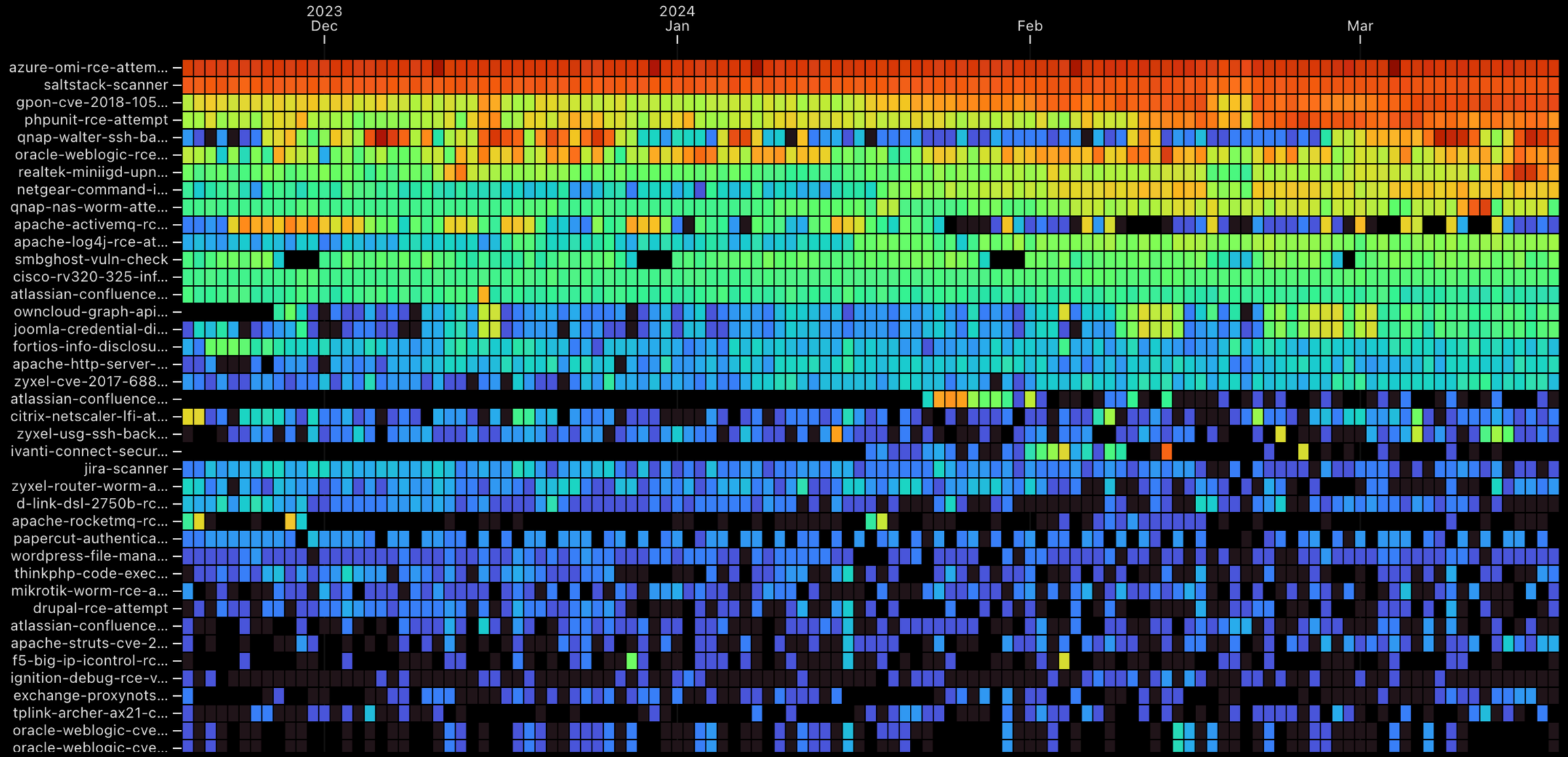
- Cisco ASA CVE-2020-3259 Information Disclosure Attempt (CVE-2020-3259)
- Hongfan OA ioAssistance.asmx RCE Attempt
- Ecology OA validate.jsp SQL Injection Attempt
- PhpMyAdmin setup.php Remote Command Execution Check (CVE-2009-1151)
- FortiNet FortiClientEMS CVE-2023-48788 SQL Injection Attempt
- Oracle BI Publisher CVE-2019-2588 Directory Traversal Attempt
- ECOA BAS Controller CVE-2021-41293 Path Traversal Attempt
- WP-22.php Malware Scanner
- Hikvision IP Cameras CVE-2013-4975 Privilege Escalation Check

https://viz.greynoise.io/trends?view=recent

KEV Tag Activity Heatmap

There are 81 KEV Tags With NO Activity





WE NEED

TO TALK

ABOUT

KEV


KEV

THIS
PAGE
INTENTIONALLY
LEFT
BLANK


DairyPak
MISSING
MILK!
2% Reduced Fat
Milk
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
HAVE YOU SEEN ME?